WASHINGTON
LEGISLATIVE OFFICE


June 11, 2010

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

**Re: Docket No. 100402174-0175-01 Information Privacy and Innovation in the Internet Economy**

**AMERICAN CIVIL LIBERTIES UNION**
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
*DIRECTOR*

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500



Dear Sir/Madam:

The American Civil Liberties Union (ACLU) submits the following comments to the Department of Commerce regarding proposed review 100402174-0175-01, published in the Federal Register on April 23, 2010. The ACLU has over half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. Throughout our history, we have been one of the nation's foremost protectors of individual privacy.

As the Privacy and Innovation Initiative works to identify policies that enhance transparency, strengthen public confidence and support fundamental democratic values we urge them to focus on updating the Electronic Communication's Privacy Act (ECPA). ECPA was written in 1986, before the Web was even invented, yet remains the main statutory protection for the privacy of electronic communications. Communications technology has not only advanced tremendously since 1986, it has also become an essential part of our lives. It impacts how we learn, share, shop and connect. However, in order for Americans to feel comfortable utilizing these new technologies they must be assured their privacy will be protected. We believe that in order to best promote innovation in the information economy we need an updated ECPA to match our modern online world. As part of the review process, we urge the Department to adopt the principles set forth herein and to use all its resources to urge Congress to build such principles into a reform and modernization of ECPA.

The Founding Fathers recognized that citizens in a democracy need privacy for their "persons, houses, papers, and effects." That remains as true as ever. But our privacy laws have not kept up as technology has changed the way we hold information. Thomas Jefferson knew the papers and effects he stored in his office at Monticello would remain private. Today's citizens

deserve no less protection just because their "papers and effects" might be stored electronically.

**Americans Have Embraced Technology**

Technology has changed immensely since ECPA was written in 1986—and Americans have adopted these changes into their lives:

- Over 50% of American adults use the Internet on a typical day.[1]
- 62% of online adults watch videos on video-sharing sites, [2] including 89% of those aged 18–29.[3]
- 69% of online adults use "cloud computing" [4] services to create, send and receive, or store documents and communications online.[5]
- Over 70% of online teens and young adults[6] and 35% of online adults have a profile on a social networking site. [7]
- 83% of Americans own a cell phone and 35% of cell phone owners have accessed the Internet via their phone.[8]

Companies continue to innovate and create new ways for Americans to merge technology with daily activities. Google has spent the last five years building a new online book service and sales of digital books and devices have been climbing.[9] Americans increasingly turn to online video

---

[1] Common daily activities include sending or receiving email (40+% of all American adults do so on a typical day), using a search engine (35+%), reading news (25+%), using a social networking site (10+%), banking online (15+%), and watching a video (10+%). Pew Internet & American Life Project, *Daily Internet Activities, 2000–2009*, http://www.pewinternet.org/Trend-Data/Daily-Internet-Activities-20002009.aspx.

[2] A "video-sharing site" or "video hosting site" is a website that allow users to upload videos for other users to view (and, often, comment on or recommend to others). Wikipedia, *Video Hosting Service*, http://en.wikipedia.org/wiki/Video_sharing (as of May 1, 2010, 04:21 GMT). YouTube is the most common video-sharing site today.

[3] Pew Internet & American Life Project, *Your Other Tube: Audience for Video-Sharing Sites Soars*, July 29, 2009, http://pewresearch.org/pubs/1294/online-video-sharing-sites-use

[4] The term "cloud computing" has many definitions, but generally refers to services that offer applications or data storage accessible via the web. Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx.

[5] Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 2008 [hereinafter Pew Cloud Report], http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx . 56% of Internet users use webmail services, 34% store photos online, and 29% use online applications such as Google Docs or Adobe Photoshop to create or edit documents.

[6] Pew Internet & American Life Project, *Social Media & Young Adults*, Feb. 3, 2010, http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[7] "Social networking sites" allow users to construct a "semi-public" profile, connect with other users of the service, and navigate these connections to view and interact with the profiles of other users. danah m. boyd & Nicole B. Ellison, *Social Networking Sites: Definition, History, and Scholarship,* 13 J. of Comp.-Mediated Comm. 1 (2007); Pew Internet & American Life Project, *Adults & Social Network Sites*, Jan. 14, 2009, http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx.

[8] Pew Internet & American Life Project, *Internet, Broadband, and Cell Phone Statistics*, Jan. 5, 2010, http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.

[9] *See generally* ACLU of Northern California, *Digital Books: A New Chapter for Reader Privacy*, Mar. 2010, *available at* http://www.dotrights.org/digital-books-new-chapter-reader-privacy.

sites to learn about everything from current news to politics to health.[10] Location-based services[11] are a burgeoning market.[12]

These services provide many benefits, but they also have the ability to collect and retain detailed information about individuals: their interests, concerns, movements, and associations. This information can be linked together, allowing a user's Internet searches, emails, cloud computing documents, photos, social networking activities, and book and video consumption to be collected into a single profile.[13]

**Americans Still Expect Privacy**

This rapid adoption of new technology has not eliminated Americans' expectations of privacy. To the contrary, Americans still expect and desire that their online activities will remain private, and express a desire for laws that will protect that privacy.

- 69% of Internet users want the legal right to know everything that a Web site knows about them.[14]
- 92% want the right to require websites to delete information about them.[15]
- A large percentage of users of cloud computing are "very concerned" about how their personal information may be used and disclosed to law enforcement and third parties.[16]

When user privacy is not protected innovation is hindered because users are hesitant to adopt new technology. A recent poll revealed that 50% of Americans polled have little or no interest in using cloud computing and that 81% of these respondents are reluctant, at least in part, because they are concerned about the security of their information in the cloud.[17] For a complete analysis

---

[10] "More Americans are watching online video each and every month than watch the Super Bowl once a year.." Greg Jarboe, *125.5Million Americans Watched 10.3 Billion YouTube Videos in September*, SEARCHENGINEWATCH.COM, Oct. 31, 2009, http://blog.searchenginewatch.com/091031-110343.

[11] "Location-based services" is an information service utilizing the user's physical location (which may be automatically generated or manually defined by the user) to provide services. Wikipedia, *Location-Based Service*, http://en.wikipedia.org/wiki/Location-based_service (as of May 1, 2010, 04:35 GMT).

[12] Recent location-based service Foursquare built a base of 500,000 users in its first year of operation. Ben Parr, *The Rise of Foursquare in Numbers [STATS]*, MASHABLE, Mar. 12, 2010, http://mashable.com/2010/03/12/foursquare-stats/.

[13] *See* ACLU of Northern California, *Digital Books*, *supra* note 9 ("[I]f a reader has logged in to other Google services such as Gmail at the time he searches for a book, Google can link reading data to the reader's unique Google Account [and] retains the right to combine all this information with information gleaned from its DoubleClick ad service, which tracks users across the Internet.") More information is available at the ACLU's Demand Your dotRights campaign website. Demand Your dotRights, http://dotRights.org.

[14] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[15] *Id.*

[16] Cloud computing users are "very concerned" about law enforcement access to data (49%); services retaining files after users delete them (63%); services using personal data for targeted advertisements (68%) or marketing (80%); services selling files or data to third parties (90%). See Pew Cloud Report, *supra* note 5, at 11.

[17] Harris Interactive, *Cloud Computing: Are Americans Ready?*, Apr. 21, 2010, http://news.harrisinteractive.com/profiles/investor/ResLibraryView.asp?BzID=1963&ResLibraryID=37539&Category=1777

of the state of privacy in the cloud see the ACLU of Northern California's report, Cloud Computing: Storm Warning for Privacy, attached as Appendix A.

Americans want and need legal protections for privacy that reflect the technology they use every day. The time has come to modernize ECPA to reflect our 21st century digital world.

**ECPA Rules Are Confusing and Outdated**

In the face of rapid technological change and Americans' continuing expectation of privacy, ECPA has fallen behind. Distinctions in ECPA have become increasingly confusing and arbitrary, based on an understanding of technology that is a generation behind that which we use today.[18] Many new technologies, particularly those dealing with location information, are not addressed by ECPA. These failures not only leave holes in the privacy protections in place for individuals, but pose a threat to continuing innovation and business development. We need to update ECPA to encompass all of the ways that Americans use technology today.

E-mail exemplifies the gap between the language of ECPA and today's technology. In 1986, e-mail was typically downloaded to a recipient's computer upon receipt and immediately deleted from the e-mail provider's storage. ECPA was written with this behavior in mind: it requires a search warrant to retrieve a message from an e-mail provider's storage only if the message is less than 180 days old, and provides for lower standards if the email is left on the server for more than 180 days.[19] Today, however, e-mail is often both stored on and accessed from remote servers belonging to the e-mail provider, and many people "archive" their e-mail on their provider's server rather than deleting old messages. Basing legal protection on how long an e-mail has been stored is incongruous with current e-mail use. Instead, ECPA should provide full protection for all online documents and communications and dispose of these artificial and outdated distinctions.

Similarly, the state of technology in 1986 resulted in more legal protection in ECPA for the content of communication—the body of an e-mail or the contents of a letter or phone conversation—than for the transactional information. Historically, transactional information was easy to distinguish from content: the number dialed on a telephone as opposed to the voice call itself, or writing on the outside of an envelope as opposed to the message within. The digital world, however, blurs the line between content and transactional data. Internet search terms, browser history, e-mail subject lines and location information do not fit neatly into either category and can reveal sensitive data like political and religious affiliations. Most people consider such information to be private. The law should match these expectations and require a warrant for disclosure.

In addition to the difficulty in anticipating modern uses of technologies existing in that era, lawmakers in 1986 could not predict technological innovations. Mobile phones provide a glaring

---

[18] *See Steve Jackson Games v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) (The Wiretap Act, as amended by ECPA, is "famous (if not infamous) for its lack of clarity.").

[19] Even this limited protection is in doubt. The Department of Justice has argued that, once email is opened, it is no longer in "electronic storage" and thus no longer subject to a warrant requirement under ECPA even if it is less than 180 days old. *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), D. Colo., No. 09-80.*

example, along with the location information gleaned from them. Modern cell phones have become, in essence, portable tracking devices. Technologies including GPS[20] and cell tower triangulation[21] allow mobile phone providers to determine our physical locations in real time—and these providers can retain records of this location information for various purposes. The legal standard for access to these records is currently being litigated, and Congress has never weighed in on what the appropriate standard should be.[22] In the meantime, litigants regularly demand these sensitive records in government investigations and civil suits. A company employee recently admitted that Sprint received a staggering eight million requests for mobile phone location information from law enforcement in just over a year.[23]

Outdated digital privacy law is a threat to individual privacy as well as innovation. User perception of inadequate privacy is one threat that companies face. For example, Microsoft recently announced that its future lies in online cloud computing services, but its own poll found that more than 90 percent of the general population is "concerned about the security, access, and privacy of personal data" stored online,[24] leading the company to explicitly ask Congress for better online privacy protection to promote cloud computing.[25]

Companies are also affected when they receive demands to turn over the personal information of users. Google just released data that it received over 3,500 demands from law enforcement involving criminal investigations in the last six months of 2009.[26] If Google is receiving thousands of demands digging into the intimate details of individual lives that are captured in emails, search histories, reading and viewing logs, and the like, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day? And how can companies hope to respond to these requests without improperly over- or under-disclosing information when faced with outdated, confusing laws with questionable applicability to their products or services?

---

[20] GPS, or Global Positioning System, is a satellite-based navigation system that allows a GPS receiver to determine its own location. *Global Positioning System*, http://gps.gov.

[21] Cell tower triangulation allows the location of a mobile device to be determined by "triangulation" based on its calculated distance from two or more cell towers within the phone's range. *See* Chris Silver Smith, *Cell Phone Triangulation Accuracy Is All Over the Map*, SearchEngineLand.com, Sep. 22, 2008, http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790.

[22] *See, e.g., In re Application of the United States for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government*, No. 08-4227 (3d. Cir. oral argument heard Feb. 12, 2010).

[23] Kim Zetter, *Feds 'Pinged' Sprint GPS Data 8 Million Times Over a Year*, WIRED, Dec. 1, 2009.

[24] Microsoft News Center, *Cloud Computing Flash Poll—Fact Sheet* , http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc. More information is available at http://www.microsoft.com/presspass/presskits/cloudpolicy/materials.aspx.

[25] Microsoft News Center, *Press Release: Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud*, Jan. 20, 2010, *available at* http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.

[26] Government Requests Tool, http://www.google.com/governmentrequests. Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

**Key Principles for Updating ECPA**

Because these inadequate legal standards create difficulties for Internet users and businesses alike, a coalition of privacy advocates and businesses—from the American Civil Liberties Union to Google and AT&T—has formed to urge Congress to update electronic privacy law to provide clear rules and better protection for electronic data. The coalition believes that just as the law recognized that storing information in digital form on a computer hard drive should have the same probable cause warrant protection as information stored in paper form in a filing cabinet, the time has come to ensure that these same privacy protections apply to digital information stored in the cloud.

The ACLU believes the efforts being urged by the coalition to update ECPA are critical first steps but believes a full review of ECPA should involved all of the following issues:

1. Robustly Protect All Personal Electronic Information.
2. Safeguard Location Information.
3. Institute Appropriate Oversight and Reporting Requirements.
4. Require a Suppression Remedy.
5. Craft Reasonable Exceptions.

*Robustly Protect All Personal Electronic Information.*

In the modern world, just as in Jefferson's time, our personal, private information—whether paper documents and correspondence or records of what we search and read online—reveals a tremendous amount about us. Our right to privacy and our rights to free expression and free association require that this information be protected from disclosure to the government without notice and without a warrant based on probable cause. Changing technology must not erode these protections. Our e-mail, online spreadsheets and photos, and other digital documents need strong legal protections regardless of how, where, or how long they are stored.

Congress has long-recognized the privacy interests in the transactional records of users of expressive material. The Video Privacy Protection Act prohibits disclosure of video viewing records without a warrant or court order, requires notice prior to any disclosure of personally identifiable information to a law enforcement agency, and requires the destruction of personally identifiable information one year after it becomes unnecessary.[27] The Cable Communications Policy Act similarly prohibits disclosure of cable records absent a court order.[28] Similarly, to safeguard autonomy, privacy, and intellectual freedom, our laws extend protection to library and book records.[29] We need the same protection for digital records that implicate our First Amendment freedoms by recording our expressive actions and choices.

---

[27] 18 U.S.C. § 2710(b)(2)(B), (b)(3),(e) (2009).
[28] 47 U.S.C. § 551(c) (2008).
[29] 48 states protect library reading records by statute, *see, e.g.*, N.Y. C.P.L.R. § 4509; Cal. Gov. Code §§ 6267, 6254(j), and federal and state courts have also often frowned upon attempts by the government or civil litigants to gain access to such records, *see, e.g.*, *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (quashing a government subpoena seeking the identities of 120 book buyers because "it is an unsettling and un-American scenario to envision federal agents nosing through the reading lists of law-abiding citizens while

Current loopholes in our privacy laws need to be closed to protect electronic information without regard to its age, whether it is "content" or "transactional" in nature, or whether companies or individuals can use this information for other purposes. ECPA must be modernized to provide robust protection for all personal electronic information and require a probable cause warrant and notice prior to disclosure.

*Safeguard Location Information.*

The vast majority of Americans own cell phones. The location information transmitted by these phones every minute of every day reveals not only where we go but often what we are doing and who we are talking to. Americans take cell phones everywhere: to gun rallies, to mental health clinics, to church, and everywhere else we go. Ubiquitous tracking is a reality in the United States. We must protect this sensitive information from inappropriate government access. Location information, whether current or historical, is clearly personal information. The law should require government officials to obtain a warrant based on probable cause before allowing access.

*Institute Appropriate Oversight and Reporting Requirements.*

Electronic recordkeeping enables easy collection and aggregation of records, and the insufficient and outdated standards applied by ECPA provide little barrier should the government wish to engage in a "shopping spree" through the treasure trove of personal information held by private companies. In addition to updating the standards for access to electronic information, ECPA should ensure adequate oversight by Congress and adequate transparency to the public by extending existing reporting requirements for wiretap orders to all types of law enforcement surveillance requests.

The House Judiciary Committee recognized this need when it passed HR 5018 (106th Congress) by a vote of 20-1.[30] The proposed bill would have required reporting on all orders, warrants, or subpoenas issued by government entities seeking electronic communications records or content information. Current efforts to modernize ECPA should include this requirement as well.

*Require a Suppression Remedy.*

Both the Fourth Amendment and the Wiretap Act provide for an exclusionary remedy: if a law enforcement official obtains information in violation of a defendant's constitutional privacy rights or the Act, that information usually cannot be used in a court of law.[31] The same rule, however, does not apply to electronic information obtained in violation of ECPA. Without an exclusionary rule, there is a lack of deterrence for government overreaching. Unlawfully

---

hunting for evidence against somebody else."); *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (First Amendment requires government to "demonstrate a compelling interest in the information sought . . . [and] a sufficient connection between the information sought and the grand jury investigation" prior to obtaining book records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1059 (Colo., 2002) (government access to book records only passes muster under Colorado Constitution if "warrant plus" standard is met by the government—i.e, prior notice, adversarial hearing, and showing of a compelling need).

[30] H.R. Rep. No. 106-932 to accompany H.R. 5018 (2000) at 23.

[31] 18 U.S.C. 2515.

obtained electronic information should be barred from use in court proceedings. A suppression remedy provision passed the House Judiciary Committee in 2000 as part of HR 5018 and should be included in any current Congressional language to modernize ECPA.[32]

*Craft Reasonable Exceptions.*

Overbroad exceptions and the abuse of "voluntary disclosure" procedures are also depriving Americans of their rightful privacy protection. ECPA needs to be revised to close these loopholes and ensure that private information is only released outside of the standard process when truly necessary.

Under previous law, a company could only turn records over if it had a "reasonable belief" that there was an emergency involving "imminent harm" of death or injury to any person. However, in 2001 that standard was lowered so that the company's belief only needed to be held in "good faith" and that the harm no longer needed to be imminent. This lowered standard reduced a company's obligation to ensure that its decision to release private information about a user was balanced by the exigency of the situation.

In addition, exceptions to prohibitions on "voluntary" disclosure need to be revised to prevent coercive abuse by law enforcement. For example the Inspector General for the Department of Justice has reported that the FBI circumvented its National Security Letter (NSL) authority by using "exigent letters" to obtain information with the promise that the agent had already requested a grand jury subpoena or an NSL.[33] To prevent such abuse, all requests for "emergency" voluntary disclosures under ECPA should clearly state that compliance with the request is voluntary and ECPA should require thorough documentation and reporting of all such requests.

Exceptions to the procedural requirements for government access to electronic records should be just that: exceptional. ECPA reform should restore the original emergency exception for ECPA and require documentation and reporting to ensure that these exceptions are used properly and not abused.

*Conclusion*

We applaud the Internet Policy Task Force for conducting a review of the relationship between privacy policy and innovation in the information economy because it is clear that the future of our economy will take place in the cloud. We urge the Department to work with Congress to reform and modernize ECPA in order to maintain Americans fundamental right to privacy so that they will be able to engage, compete and innovate in this space.

Changes in the way we communicate with each other in today's world are wondrous when viewed through 1980's spectacles. That wonderment should not be tempered by the realization that our personal privacy is slipping away. Comprehensive reform of ECPA is a needed

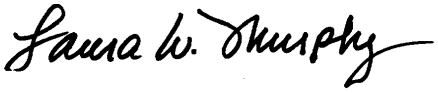
---

[32] Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong. § 2 (2000).

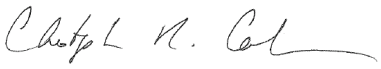
[33] Dep't. of Justice, Office of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007), at 86–97, *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

legislative initiative that will help preserve the real innovative value of the technology boom and set us on a path for even greater innovation to come.

Sincerely,



Laura W. Murphy
Director, Washington Legislative Office



Christopher Calabrese
Legislative Counsel

# Cloud Computing: Storm Warning for Privacy?

A publication of the ACLU of Northern California
Available online at www.DotRights.org

**"Cloud computing"**—the ability to create, store, and manipulate data through Web-based services—is growing in popularity. Cloud computing itself may not transform society; for most consumers, it is simply an appealing alternative tool for creating and storing the same records and documents that people have created for years. However, outdated laws and varying corporate practices mean that documents created and stored in the cloud may not have the same protections as the same documents stored in a filing cabinet or on a home computer. Can cloud computing services protect the privacy of their consumers? Do they? And what can we do to improve the situation?

*Cloud Computing: Storm Warning for Privacy?* is the first in a series of issue papers by the ACLU of Northern California that discuss new technology trends and their consequences. This paper examines the current state of legal and technical privacy protections for consumers of cloud computing services and explores opportunities for consumers, businesses, and policymakers to work together to update and enhance these protections.

Part I of this paper provides background information on cloud computing. Part II examines the privacy concerns that arise from the use of cloud computing services and Part III surveys the current state of privacy protections for consumers of these services. Finally, Part IV identifies opportunities for legal, technological, and social mechanisms to be reinforced so that Internet consumers are not forced to lose control of their information when they use cloud computing services.

For more information about cloud computing and other online privacy and emerging technology issues, please visit the ACLU of Northern California's Demand Your dotRights campaign website at **www.dotRights.org**.

# CONTENTS




AUTHORS: Nicole A. Ozer, Chris Conley



Thank you to Tamar Gubins, David Hari O'Connell, Christopher Soghoian, Aaron Brauer-Rieke, Monique Pham, and the staff of the ACLU Technology and Liberty Project for their assistance with this issue paper.

COVER DESIGN: Gigi Pandian, ACLU of Northern California


For more information about cloud computing and other online privacy issues, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our online privacy Web site at www.dotrights.org.


**The ACLU of Northern California wishes to thank the following funders for their support of this publication:**

Block v. eBay cy pres fund

California Consumer Protection Foundation

Consumer Privacy Cases cy pres fund

Rose Foundation for Communities and the Environment

The David B. Gold Foundation

**Published by the ACLU of Northern California, January 2010**

# INTRODUCTION

"Cloud computing" services—tools accessed via the Internet that allow consumers to create, edit, and store documents (such as private photos and videos, calendars and address books, diaries and journals, and budgets and financial spreadsheets) online—are growing in popularity as Internet speeds increase and the cost of data storage drops. Companies are offering a wide range of cloud computing services, ranging from "free" basic applications for the general public to sophisticated and well-supported services designed for corporations and even governments.[1] Many popular offline applications, including Microsoft Office and Adobe Photoshop, now offer cloud computing editions with familiar interfaces. Other tools allow consumers to "drag and drop" files to or from online storage exactly as though the storage site were just another folder or hard drive. Once documents are online, consumers can access and share them from any Internet-enabled device. From the consumer perspective, cloud computing services make the transition from offline to online activities increasingly seamless.

Unfortunately, while consumers can easily carry their information into the cloud, the privacy protections for that personal information may not transition as easily. The Fourth Amendment requires law enforcement officials to obtain a warrant from a judge before entering a person's home and searching her file cabinet or computer hard drive for documents and related information, but courts have yet to definitively determine how these privacy protections apply to cloud computing documents. Furthermore, many existing privacy statutes were written decades ago and may not apply to documents stored with online services like cloud computing that were not anticipated when these laws were drafted. In addition, when documents are stored in a filing cabinet or on a home computer, the owner of the documents often has the opportunity to challenge a demand to hand over those documents—but a cloud computing service may not have the ability or incentive to resist such demands or even to notify the document owner if her documents are demanded by a third party.

As cloud computing becomes increasingly popular and the boundary between personal devices and the Internet "cloud" becomes less meaningful, consumers and companies alike will benefit from protections that ensure that documents created and stored using cloud computing services carry the same rights and protections as documents created or stored elsewhere.[2] These rights and protections will preserve the privacy of consumers, strengthen loyalty and trust in cloud computing services, prevent costly litigation, and encourage the use of beneficial technologies like cloud computing to create, edit, share, and store documents.

Part I of this paper provides background information on cloud computing. Part II examines the privacy concerns that arise from the use of cloud computing services and Part III surveys the current state of privacy protections for consumers of these services. Finally, Part IV identifies opportunities for legal, technological, and social mechanisms to be reinforced so that Internet consumers are not forced to lose control of their information when they use cloud computing services.

In several areas of the paper we have more questions than answers. It is our hope that this issue paper will help to support a robust conversation between consumers, businesses, and policymakers to address these important questions about cloud computing and develop plans to address potential gaps in the existing legal framework for protecting privacy and freedom of expression.

# Part I: Understanding Cloud Computing

"Cloud computing" is an increasingly popular buzzword, though it has been inconsistently used. Some definitions are so broad that it can be difficult to distinguish cloud computing from general Internet use.[3] For the purposes of this issue paper, we define cloud computing as "outsourcing" computing functions traditionally controlled directly by a consumer—operating and maintaining hardware, installing and running software, storing data—to a third-party service via the Internet.[4] The most common cloud computing services allow Internet consumers to use a Web browser to create a spreadsheet or presentation,[5] store and manipulate photos,[6] store medical records,[7] organize and play multimedia files,[8] back up data,[9] or maintain calendars or address books.[10] Business-oriented cloud computing services allow companies to manage customer relations,[11] store data, or run their own applications on remote computers.[12] (The definition in this paper excludes Web-based email and social networking services that broader definitions might include.)

For example, Google Docs and Microsoft Office Live are online suites of office applications for consumers that are similar to Microsoft's Office suite (Word, Excel, and PowerPoint). Like Microsoft Office, these online suites enable consumers to create and edit documents through a graphical interface. However, rather than installing software on a personal computer and storing the created documents on a hard drive, a Google Docs or Microsoft Office Live consumer accesses the application through her Web browser and saves her documents on a remote server controlled by a third party.

Computer consumers are increasingly taking advantage of cloud computing services. According to a 2008 Pew Internet & American Life Project memorandum (Pew memo),[13] at least 40% of American Internet consumers, and at least 59% of such consumers in the 18-29 age range, have engaged in some form of cloud computing activity (as defined above) by either storing data online or using Web-based software applications.[14] The rise of cloud computing can be ascribed at least in part to efforts by cloud computing providers to make their services as consumer-friendly as possible. Cloud computing consumers enjoy the convenience of accessing their information from any Internet-connected device, the ability to share documents and information with others, and the security of protection from data loss.[15]

For the consumer, the transition from local applications and storage to cloud computing services can be nearly seamless. In effect, the cloud may be seen simply as an extension of a personal computer or device. From technical and legal perspectives, however, moving to cloud computing has significant ramifications. Relocating the storage and processing of a consumer's data and personal information from a consumer's own computer to a third party's servers impacts her ability to retain control over information, potentially exposing far more private details

about that consumer's life than she might realize and possibly undermining the privacy protections she expects for her private information.

# Part II: Why is Privacy Important for Cloud Computing?

Privacy is both an individual and a social good. As individuals, privacy gives us the autonomy to address sensitive issues without fear of exposure, the ability to explore facets of our personality and individuality, and the power to form close bonds with some by excluding others.[16] Privacy allows a healthy society to experiment and grow, and safeguards the balance between individual liberties and government powers. As such, privacy is a fundamental building block of a robust democracy. But this privacy, autonomy, and control over personal information, so essential to American society, may be at risk as consumers increasingly place private data in the hands of third-party cloud computing services—and consumers are increasingly concerned about this.[17]

**Consumers of cloud computing services have a simple message for their service providers: "Let's keep the data between us."**

## Privacy Risks of Cloud Computing

Cloud computing services may hold a consumer's diaries, business records, photographs, calendars, address books, medical records, and many other sensitive documents – documents that the consumer regards as private. The information contained in such documents can implicate every part of a consumer's life – her family and friends, politics and religion, interests and activities – and requires meaningful safeguards to protect her privacy and freedom of action.

Moreover, cloud computing activity – like any Internet activity – generates additional information that a provider might collect, such as the identity of each consumer who accesses content stored online and the time and place they do so. For example, when a consumer accesses Google Docs, "Google records information such as account activity (e.g., storage usage, number of log-ins, actions taken), data displayed or clicked on (e.g., UI elements, links), and other log information (e.g., browser type, IP address, date and time of access, cookie ID, referrer URL)."[18] Collecting this information raises questions about privacy even when done independently; when linked to other cloud computing activity, it threatens to reveal far more about a consumer than she might imagine. For example, IP addresses and login times could be used to determine when and where a user was—and who else has used that same computer—if she logs into a cloud computing service away from home.

In addition, some cloud computing service providers may "subcontract" parts of the service to additional third parties who then may have some degree of access to private data. For example, some companies like Amazon provide hosting services that allow other companies to use their servers to run web applications and store data[19]—but claim the right to disclose this data under certain circumstances. The Amazon Web Services

Agreement states that Amazon may disclose data to "comply with…the request of a governmental or regulatory body, subpoenas or court orders." [20] Language like this demonstrates that it is important that each link in the chain have robust privacy and security safeguards or consumers may find that their personal information is vulnerable. [21]

**Cloud computing consumers are "very concerned" by scenarios in which companies:**

- **Turn their data over to law enforcement (49% of consumers);**
- **Keep copies of files even after they try to delete them (63%);**
- **Analyze data in the cloud for targeted advertisements (68%);**
- **Use cloud documents in marketing campaigns (80%); and**
- **Sell files to others (90%).[22]**

## Consumers Are Worried About Cloud Computing Privacy

Cloud computing consumers are increasingly aware of—and alarmed by—the risks associated with creating and storing their documents in the cloud. Thus, discussions about cloud computing privacy are not merely academic; they reflect the views and concerns of real consumers. Unless these concerns are addressed, privacy fears may limit adoption of cloud computing tools overall.

According to a 2008 survey, cloud computing consumers "show high levels of concern when presented with scenarios in which companies might use their data for purposes consumers may or may not fully understand ahead of time" and "worry over control of the information they store online."[23] The survey summarized the underlying message of cloud consumers to companies as, "Let's keep the data between us."[24]

Consumers are right to be concerned about what goes on in "the cloud." Abstracting away the technical details makes computing easier and more convenient for many, but without transparent sharing policies and meaningful consumer controls, cloud computing could weaken a consumer's ability to maintain control over her own information. Unfortunately, the legal protections that consumers should be able to rely on for information stored with cloud computing services are currently uncertain.

# Part III: Legal Privacy Protection and Cloud Computing

The law has long recognized the importance of privacy as both a breathing space for personal autonomy and a necessary constraint on the power of the government.[25] Most privacy law, however, was written or decided decades ago, before the advent of the Internet and other communications technologies. The combination of outdated law and rapidly evolving technology results in inconsistent and uncertain privacy protections. This lack of clear and up-to-date law harms everyone involved: consumers, businesses, and the government.

Because privacy law is badly outdated, the legal protections that apply to information stored with or collected by cloud computing services are unsettled. For example, it is unclear whether the Constitution prevents law enforcement access to cloud computing data without a judicially-approved search warrant, or whether and to what extent the current patchwork of statutory privacy laws provide additional privacy protection. For now, consumers, cloud computing providers, and the government alike are acting in a legal domain filled with grey areas.

Ultimately, this lack of legal clarity benefits no one. Consumers are unsure how or whether using cloud computing services affects their privacy and anonymity. Providers are hampered in attracting consumers who worry their privacy won't be properly protected, and are hamstrung by confusion about whether they legally may, must, or must not disclose consumer information in various circumstances. Even law enforcement officials are harmed when this confusion leads providers to resist legitimate requests for information.

There are three basic categories of legal protection for information stored with cloud computing providers: Constitutional protections, statutory protections, and privacy policies. Each of these three is currently unclear or inadequate to protect the interests of consumers and cloud computing providers. Courts, policymakers, and companies all need to use the tools at their disposal to clarify and extend these legal protections to ensure the privacy of information stored with cloud computing providers.

## Constitutional Protections: Cloud Computing and the Third Party Doctrine

Privacy is an essential civil liberty protected both by the United States Constitution[26] and several state constitutions, including the California State Constitution.[27] The federal constitutional protection for private records is housed in the Fourth Amendment, which prohibits "unreasonable searches and seizures."[28] The Supreme Court, in a long history of decisions, has extended this protection beyond the home to any location where an individual has a "reasonable expectation of privacy."[29]

Legal decisions have conferred a reasonable expectation of privacy on many of the closest analogues to cloud computing. For example, the Fourth Amendment protects various forms of containers, including:

- Personal containers, such as purses, even if left with another for safekeeping;[30]
- Physical storage facilities such as safety deposit boxes[31] and rented storage lockers;[32]
- Personal computers, in some cases even if the computer is completely under the control of another;[33] and,
- Files on networked computers.[34]

Since cloud computing is really a modern version of a storage locker or personal computer hard drive, it makes sense for cloud computing consumers to expect that their data will have the full protection of the Fourth Amendment and be protected against warrantless searches.

However, questions arise about the constitutional protections for online data, including cloud computing records, because of a legal doctrine called the "business record doctrine," also termed the "third party doctrine." The business record doctrine, which was established in a pair of pre-Internet Supreme Court cases, holds that there is no reasonable expectation of privacy, and thus no Fourth Amendment privacy protection and warrant requirement, when a person turns over information to a third party business.[35] In relinquishing exclusive control over the information, the person "assume[s] the risk" that the third party might voluntarily pass on this information, and thus can no longer reasonably consider the information private.[36] Based on this doctrine, law enforcement officials have claimed that records of online activities are not protected by the Fourth Amendment.[37]

The tension between these two approaches to the Fourth Amendment has yet to be resolved, and lawyers and the courts continue to address the issue of constitutional protections for online data. Two courts have held that email messages stored in a Web mail account and text messages stored with a service provider retain full Fourth Amendment protection,[38] suggesting the same protection should apply to cloud computing documents. But the question remains open, particularly where the provider accesses the consumer's content in some manner (such as to provide recommendations, scan files for viruses or check for spelling or grammatical errors, or generate targeted advertising based on the content) rather than solely storing it at the consumer's behest.

Adding further complexity, state constitutional protections may apply even where federal constitutional protections do not. For example, the California Supreme Court has explicitly rejected the third party doctrine as a limitation on the right to privacy in the state constitution.[39] Thus, the privacy protections for a cloud computing user could differ depending on the state where she lives or where her data is stored.

While the legal landscape is unsettled, consumer expectations—the basis of constitutional privacy protections—are not. Internet consumers treat cloud computing services as the modern equivalent of storage lockers, safe deposit boxes, filing cabinets, and (most recently) home computers and personal hard drives. They expect these documents and any associated information to remain private—and strongly express their concerns about scenarios where their data is shared with others, as discussed above. Like papers or other objects residing in these storage facilities, information stored with cloud computing services merits the full protection of the Fourth Amendment and state constitutional privacy provisions.

## Statutory Protections: Cloud Computing, ECPA, and Other Laws

Federal and state laws provide additional sources of privacy protection. Such "statutory law" can be particularly important in providing greater certainty in a situation, like cloud computing, where technology has advanced and constitutional protections have not yet been tested. Unfortunately, many of the statutory laws that might apply to cloud computing services were written decades ago, before the Internet even existed, and thus provide questionable protection for cloud computing consumers as well.

In particular, the Electronic Communications Privacy Act (ECPA)[40] should—but does not—clearly define the statutory protections applicable to cloud computing services. ECPA is a federal statutory law that provides specific protections for electronic communications (in transit or in storage) to supplement any protections offered by the Fourth Amendment. But ECPA does not clearly state whether documents stored with many cloud computing services are protected at all. ECPA, as currently written, provides protection where content is stored with a service "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[41] It is not clear whether sites that provide collaboration and sharing functions or employ a targeted advertising business model based on information contained in documents are covered by this clause.

Even if ECPA does cover cloud computing records in a specific situation, the protections that it provides are insufficient to properly safeguard the privacy of sensitive documents being stored with cloud computing services. ECPA allows law enforcement officers to either (a) demand content (such as cloud computing documents) from a provider with a subpoena or court order, rather than the search warrant required by the Fourth Amendment, if the target of the search is notified or (b) refuse to notify the consumer at all, and possibly prohibit the service from notifying the consumer, if law enforcement demands content via a search warrant.[42] Government entities can also demand transactional records from cloud computing services – records that may also contain private information – without either obtaining a warrant or notifying the consumer.[43]

Beyond ECPA, there are questions about whether other specific privacy laws or regulations fully protect consumers of cloud computing services. For example, the Health Insurance Portability and Accountability Act (HIPAA)[44] is designed to protect the privacy of health records. However, HIPAA applies to health care providers, health care clearinghouses, and health plans (insurers). Do HIPAA protections apply to cloud computing services that store consumer health records? Similarly, does the Video Privacy Protection Act[45] (VPPA), which provides statutory protection for video rental records and "other similar material," protect records of audiovisual material shared or retrieved through a cloud computing service?[46]

Without comprehensive federal privacy legislation, consumers are left with a patchwork of sector specific privacy law to safeguard their rights. It is now unclear whether even this patchwork of laws adequately covers innovations related to cloud computing. Given the already weak and now increasingly uncertain protections in ECPA and other statutory privacy laws, the time is now to take a thorough look at statutory privacy protections and update privacy law to keep pace with the modern online world.

## Privacy Policies

Internet consumers want greater control over their own information. A 2009 study found that 69% of adult Internet consumers want the legal right to know everything that a company knows about them, and 92% want the right to demand that their personal records be deleted.[47] A separate study in 2008 found that many Internet

consumers were “very concerned” about the possibility that their personal information could be shared with law enforcement or other third parties without their knowledge or consent.

Unfortunately, while the majority of companies doing business online now have privacy policies, the reality is that most of these policies do little, if anything, to actually protect consumer privacy. Many policies are just paragraph after paragraph of statements reserving broad latitude for the company to collect vast amounts of information about a consumer, keep it for an extended period of time, and use it in any way that the company can imagine. The consumer is given few methods to control her own information and often no assurance that the company will protect information from inappropriate demands for information from third parties. Further steps must be taken to ensure that “privacy policies” are worthy of that name.

# Part IV: Reinforcing Privacy Protections for Cloud Computing

As cloud computing continues to develop and expand, it is critical to establish mechanisms—legal, technological, and social—to protect the privacy of consumers. Courts and policymakers need to recognize the realities of modern Internet use and information storage and satisfy the continued expectations of privacy and free speech, regardless of whether the information is created and stored online or offline. Companies should invest in privacy-friendly technologies and practices that put consumers in control of their own private information. They should also support legal reform to update the outdated constitutional and statutory understandings of online privacy. Internet consumers also have a role to play: by using their collective voice, they can demand stronger protections and meaningful control from companies and policymakers. By doing so, these groups can pave the way for use of cloud computing by ensuring that legal, technological, and social mechanisms adequately safeguard privacy and free speech.

## Legal Reform: Privacy Laws Don’t Auto Update

Technology has developed at an astounding rate in the past two decades and the law has not kept pace. The law needs to evolve to match today’s new online world and continue to properly safeguard the privacy and free speech rights of individuals.

### Constitutional Privacy Protections Should Apply Online as well as Offline.

Cloud computing services, like their real-world analogues, deserve the full protection of the Fourth Amendment and state constitutional privacy protections. The line between cyberspace and the “real world” is rapidly fading, and businesses, policymakers, and the public should reject any attempt to create an artificial distinction between records stored in a locker or

> “Privacy does not end at the doorstep; it also cannot end at the edge of the cloud.”

on a personal computer and records stored with a cloud computing provider. Privacy does not end at the doorstep; it also cannot end at the edge of the cloud.[48]

## Existing Statutory Privacy Law Needs a Technological Upgrade

Statutory electronic privacy law should be updated to make it clear that a warrant supported by probable cause is required for any law enforcement access to records stored with a cloud computing provider. The definitions in ECPA should also be redrafted to apply to advertising-based business models and add-on online services. Privacy protections should apply to cloud computing services even if a provider is accessing stored content to deliver specific services or targeted advertising.

Lawmakers also need to reevaluate the distinction between "content" and "non-content" information and establish robust standards for secondary information collected by cloud computing providers that reveals sensitive details about Internet users. Information about a user's activities—such as when and from where the user logs in, which documents the user views and for how long, and who the user shares documents with—also contains private information that should be protected by law.

## Laws Should Require Notice and Oversight of Demands for Cloud Computing Records

Statutory privacy law should also require that a consumer be notified prior to any disclosure by a provider of any documents or records. In the offline world, such a law was typically unnecessary, as notice to the subject of a search was often unavoidable when third parties demanded documents stored in a file cabinet or on a personal computer. This notice, which gives individuals the ability to defend their own rights, needs to be written into law in the online world where an individual's documents or records could be obtained from a cloud computing provider without the individual ever knowing.

In addition, the law should require that all demands for online information, including cloud computing documents and records, be recorded and compiled so that policymakers and the public are aware of the scope of such requests. It is very difficult for consumers to feel confident about utilizing cloud computing platforms if they are left to worry that their personal information is far more vulnerable in the cloud than it is on their hard drive or in their filing cabinet because they have no basic information about disclosure rates. This lack of notice can lead some consumers to underestimate the implications of using such services, while others might have more fear than necessary.

Current law requires that law enforcement agencies compile and publish statistics about the nature and number of wiretaps orders obtained and used to intercept communications in real time[49] —but there is no such requirement for the also-invasive practice of obtaining access to online information via search warrants, subpoenas, and other means. Few companies will provide any data about how often personal information is requested and disclosed to third parties. For example, Google, which operates both Google Docs and Picasa photo services, has continually refused to state the number of requests it receives for consumer information or its number of

disclosures. This problem is systemic.[50] No company currently provides consumers with statistics about disclosure rates to third parties.

To ensure that consumers have the information that they need to trust that their information is safe, there should be a mechanism in place to require all online companies to keep a record of all information requests and to submit an annual report to a federal agency such as the Federal Trade Commission. An annual report should detail:

- The number of Federal warrants, State warrants, grand jury subpoenas, civil and administrative subpoenas, and court orders received in the previous year;
- The number and types of action taken by the company for each category of request;
- The number of individuals whose personal information was disclosed by the provider by category of request;
- The type of personal information disclosed by category of request; and
- The total amount of money received by the company to fulfill each category of request.

The agency should then make all reports accessible to the public in an online, searchable format within a reasonable time after filing. Any company with an online privacy policy should also create a prominent hyperlink from the disclosure section of its privacy policy to its latest report.

As cloud computing continues to develop and expand and the boundary between personal devices and the Internet "cloud" becomes less meaningful, it is imperative that privacy laws and policies are updated so that consumers have the transparency they need to make informed choices and feel confident that their personal information is being protected.

## Business Practices: Companies Can Lead the Way

Businesses have an important role to play in helping to safeguard the privacy of their consumers. Right now, consumers are very concerned about their information being used in ways that they did not intend.[51] This concern is not good for the public or for business. Businesses have the most to gain from a public that trusts cloud computing because more people will use the technology if they trust that their personal information will remain private.[52] Through robust privacy practices and support for necessary upgrades to privacy laws and technical development, businesses can help ease the transition and give consumers confidence that their information will be safe if they use a cloud computing service.

### Services Should Establish and Follow Robust Privacy Practices

Businesses have the opportunity to proactively address much of this consumer concern by establishing and following robust privacy practices. A "privacy policy" that does little to protect privacy is not adequate. Companies should re-dedicate themselves to following the core principles of the Fair Information Practices: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.[53] This means providing meaningful notice about how information is used and to whom it is

disclosed, collecting and retaining only the information that is needed to provide services, giving consumers real choice about how any personal information collected about them will be used, properly safeguarding consumer information from disclosure and misuse, and enabling consumers to control, modify, and delete their own records and accounts.[54] Providing consumers with meaningful control and protection for their personal information will help give consumers the confidence to utilize cloud computing and may also help companies avoid negative press, government investigations, and costly lawsuits.[55]

## Providers should protect their consumers' information with all available technical tools

Consumers expect that data stored with a cloud service provider will remain private; providers have a business incentive to ensure that it does. By designing a service with technical measures to protect consumers—tools that allow consumers to manage and protect their own information, encryption and anonymity protocols to protect information by default, and access controls and data security measures to prevent breaches and inappropriate disclosures—cloud computing providers can establish a platform where consumers are in a position to control their own information and can feel more confident storing private content.

The first step in giving consumers control is to build a robust and usable interface to allow consumers to manage their own content and records. Consumers should be able to view and control their entire record—not merely the documents that they upload, but any additional records that the service may retain about consumer action or the actions of others with whom the consumer has shared documents. Building such an interface is much easier if it is part of the design process of the service and not tacked on as an afterthought or in response to consumer demands for greater control and transparency.

Anonymization and encryption can also protect consumers by reducing the risk of disclosure of information that is captured and stored by the service. Anonymization procedures need to go beyond removing obvious markers, however, and ensure that data is irreversibly de-identified—which, again, requires forethought to ensure that "anonymization" procedures are not wholly inadequate.[56]

Finally, creating a solid data security plan protects both customers and providers. Data breaches can be disastrous, leading to lawsuits, fines, and lost trust.[57] To avoid these outcomes, providers should use access controls to prevent unauthorized access to content by both employees and third parties and take additional steps such as promptly deleting data that is no longer necessary in order to reduce the risk of breach. Such practices will help safeguard both customer privacy and the provider's bottom line.

> "The more 'locks' a provider puts in the consumer's control, the less likely it is that third parties will be asking providers for the keys."

Providing technical measures that protect and secure consumer information may carry both practical and legal significance. Practically, the measures suggested above – and others that may emerge – reduce the likelihood of breach or unnecessary disclosure. In addition, these mechanisms may strengthen the legal positions of both

consumers and providers by making it clear that the consumer, and not the provider, is the party with access to and control over any stored content. The more "locks" a provider puts in the consumer's control, the less likely it is that third parties will be asking providers for the keys.[58]

### Consumer Action: Demand Your dotRights!

If privacy laws and practices are to be brought into the modern era, consumers must provide the political and commercial will to make it happen. As a united force, Internet consumers have the political power to force policymakers to update privacy laws and regulations and the financial power to force companies to build privacy and free speech protection into product design and business models. Consumers are currently paying a very high price for many online services—control of their personal information. It is time to demand that protections for privacy and free speech be part of the foundation for cloud computing services, not an afterthought.

## CONCLUSION

Moving from filing cabinets and personal computers to cloud computing appears to offer many advantages. But outdated privacy laws, inadequate privacy policies, and lack of technological tools allowing for consumers to control their own information signal stormy skies for privacy. The time is now for policymakers, businesses, and consumers to work together to safeguard privacy and help cloud computing reach its full potential. For more information about cloud computing, please visit the ACLU of Northern California's online privacy Web site at www.dotRights.org.

# ENDNOTES

[1] *See* Thomas Claburn, *Google's 'Gov Cloud' Wins $7.2 Million Los Angeles Contract*, INFO. WEEK, Oct. 28, 2009, http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=221100129.

[2] PEW INTERNET & AMERICAN LIFE PROJECT, USE OF CLOUD COMPUTING APPLICATIONS AND SERVICES [hereinafter PEW MEMO], Sep. 2008, *available at* http://www.pewinternet.org/Reports/2008/Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1.

[3] *See id.* ("For everyday consumers of the internet and computers, cloud computing is any online activity, such as accessing data or using a software program, which can be done from different devices regardless of the on-ramp to the internet.").

[4] *Cf.* Jeff Dorsch, *What Is Cloud Computing?*, BIZMOLOGY, http://www.bizmology.com/2008/10/17/what-is-cloud-computing/ ("The simple definition is that it involves using Web-based computing tools and storing information on remote servers maintained and operated by another company.").

[5] *E.g.*, Google Docs, http://docs.google.com/; SlideShare, http://slideshare.com.

[6] *E.g.*, Flickr, http://flickr.com/; Snapfish, http://snapfish.com/; Adobe Photoshop Express, http://www.photoshop.com/.

[7] *E.g.*, Microsoft HealthVault, http://healthvault.com/; Google Health, http://google.com/health/.

[8] *E.g.*, Lala.com, http://lala.com.

[9] *E.g.*, Mozy, http://mozy.com/.

[10] *E.g.*, Yahoo! Calendar, http://calendar.yahoo.com/; Plaxo, http://plaxo.com/.

[11] *E.g.*, SalesForce.com, http://salesforce.com/.

[12] *E.g.*, Amazon Elastic Computing Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[13] *See* PEW MEMO, *supra* note 2, at 5.

[14] *Id*. This study found that 40% of consumers used multiple cloud computing services under their definition, which includes Web-based email, and thus used at least one cloud computing service under ours. More specifically, the study found that 34% of Internet consumers store personal photos online, 29% use online applications, 7% store personal videos, 5% pay for file storage, and 5% use online hard drive backup services. *Id.* at 1. Among consumers in the 18–29 age range, 50% store personal photos. 39% use online applications, 14% store personal videos, 9% pay to store computer files, and 7% back up hard drives to an online site. *Id*. at 5.

[15] *Id.* Other factors cited include ability to access information on any Internet-connected device, ability to share information with others, and protection from data loss.

[16] One scholar notes that once people know they are being "observed and recorded, their habits change; they change." 150 years ago sociologist Jeremy Bentham theorized that prisoners would self-censor their behavior if they believed they were under surveillance but did not know exactly when and where they were observed. According to Bentham, under such a system the "only logical option was to conform." 4 JEREMY BENTHAM, *Plan for a Penitentiary Inspection-House*, *in* THE WORKS OF JEREMY BENTHAM 37 (John Bowring ed., 1962) (1843).

[17] 59% of adults in a 2008 study had refused to provide information to a business or company because they thought it was not necessary. 68% of consumers in 2000 were "not at all comfortable" with companies that create profiles that link browsing and shopping habits to identity, with 82% "not at all comfortable" when profiles include income, driver's license numbers, credit data, or medical status. PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/node/2. A 2009 study found that 92% of adult Internet consumers want the legal right to

demand that their personal records be deleted. Joseph Turow, et al., *Americans Reject Tailored Advertising*, 4 (2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[18] Google Docs Privacy Policy, http://google.com/google-d-s/privacy.html (last visited Nov. 12, 2009).

[19] See Amazon Web Services, http://aws.amazon.com/.

[20] *See* Amazon Web Services Customer Agreement, Jan. 20, 2010. http://aws.amazon.com/agreement/ (last visited Jan. 22, 2010).

[21] *See* Matthew D. Sarrel, *The Darker Side of Cloud Computing*, PC MAG., Sep. 25, 2008, http://www.pcmag.com/article2/0,2817,2330921,00.asp:

> And worse, there are clouds within the cloud—your provider may subcontract with another provider for data storage, and that provider might also subcontract for data storage management. Your provider may not even be able to tell you where your data is, or even which country it is in and whether the laws that apply to you regarding data security and breach disclosure even apply in that twice-removed jurisdiction.

[22] *See* PEW MEMO, *supra* note 2, at 4, 10.

[23] *Id. at 10.*

[24] *Id.*

[25] The modern legal understanding of privacy evolved in large part from Justice Brandeis's lengthy dissent in *Olmstead v. United States*. 277 U.S. 438 (1928) (Brandeis, J., dissenting). According to Brandeis:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

*Id*. at 478.

[26] *Cf. id.*

[27] CAL. CONST, Art. 1 § 1.

[28] U.S. CONST. amend. IV.

[29] *See* Katz v. United States, 389 U.S. 347, 361 (1967).

[30] In *United States v. Most*, this was extended to a plastic bag accidentally left with a grocery clerk, although other courts may not extend protection that far. 876 F.2d 191 (D.C. Cir. 1989). In addition, while a jointly used container may allow other consumers to consent to a search, *see* United States v. Matlock, 415 U.S. 164 (1974) (right to consent derives from common authority over premises or property), a private storage container does not lose Fourth Amendment protection simply because it is located in a common area. *See* United States v. Block, 590 F.2d 535 (4th Cir. 1978) (locked footlocker in common area retains Fourth Amendment protection).

[31] *Cf.* United States v. Spilotro, 800 F.2d 959 (9th Cir. 1985) ("[T]here is no question that defendant … has standing to challenge the search of his … safe deposit box.").

[32] *See* United States v. Karo, 468 U.S. 705, 721 n.6 (1984).

[33] *E.g.*, United States v. Barth, 26 F.Supp.2d 929 (W.D. Tex. 1998).

[34] Fourth Amendment protection granted unless there is a clear policy of monitoring network use. *See* United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007); United States v. Simons, 206 F.3d 392 (4th Cir. 2000).

[35] *See* United States v. Miller, 425 U.S. 435 (1976) (banking records are not protected by the Fourth Amendment); Smith v. Maryland, 442 U.S. 735 (1979) (records of dialed phone numbers are not protected by the Fourth Amendment).

[36] *Smith,* 442 U.S. at 744.

[37] *See, e.g.*, US DOJ Computer Crime and Intellectual Property Section, SEARCHING & SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, 1.B, Sept. 2009, *available at* http://www.cybercrime.gov/ssmanual/01ssma.html.

[38] Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008) (Web email); Quon v. Arch Wireless, 529 F.3d 892 (9th Cir. 2008), *cert. granted sub nom.* City of Ontario v. Quon, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332) (text messages).

[39] People v. Chapman, 36 Cal. 3d 98, 106-7 (1984) (affirming a right to privacy in unlisted telephone directory information even though the information was "shared" with the third-party telephone company); People v. Blair, 25 Cal. 3d 640, 651-555 (1979) (finding a reasonable expectation of privacy in hotel phone records and credit card charge records); Burrows v. Superior Court, 13 Cal. 3d 238, 244-45 (1974) (finding a privacy right in bank records).

[40] 18 U.S.C. §§ 2701–12 (2008).

[41] *Id.* §§ 2702(a)(2)(B), 2703(b)(2)(B).

[42] 18 U.S.C. § 2703(b), (e) (2008). Under certain circumstances, law enforcement agents can defer the required notice if they demand information with a subpoena or court order rather than a warrant. *See id.* §§ 2703(b)(1)(B), 2705.

[43] *Id.*§ 2703(c).

[44] 45 C.F.R. §§ 160–64.

[45] 18 U.S.C. § 2710 (2008).

[46] *Compare* Kurt Opsahl, *Court Ruling Will Expose Viewing Habits of YouTube Consumers*, July 2, 2008, http://www.eff.org/deeplinks/2008/07/court-ruling-will-expose-viewing-habits-youtube-us (arguing that the VPPA encompasses records of YouTube consumers) *with* e-consultancy, *YouTube Consumers Learn the Hard Way that Online Privacy Doesn't Exist*, July 7, 2008, http://www.e-consultancy.com/news-blog/365921/youtube-consumers-learn-the-hard-way-that-online-privacy-doesn-t-exist.html (arguing that the VPPA likely does not apply to records of YouTube consumers).

[47] Joseph Turow, et al., *Americans Reject Tailored Advertising* 4 (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[48] As Judge Martin put it in his *Warshak* dissent, "If I were to tell James Otis and John Adams that a citizen's private correspondence is now potentially subject to ex parte and unannounced searches by the government without a warrant supported by probable cause, what would they say? Probably nothing, they would be left speechless." Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (Martin, J., dissenting).

[49] 18 U.S.C. § 2519 (2008).

[50] Few companies have even provided partial information about disclosure. Verizon only recently admitted that it receives "tens of thousands of requests" annually from law enforcement. David Kravets, *Google Talks Transparency, But Hides Surveillance Stats*, WIRED, Dec. 17, 2009, http://www.wired.com/threatlevel/2009/12/google-talks-out-its-portal/. Facebook has admitted it receives up to 20 law enforcement requests per day but has not provided consumers with any information about

disclosures to third parties in the civil context. Nick Summers, *Facebook's 'Porn Cops' Are Key to Its Growth*, NEWSWEEK , May 18, 2009, *available at* http://www.newsweek.com/id/195621.

[51] *See* PEW MEMO, *supra* note 2, at 11.

[52] *See generally Privacy Practices*, PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at*, http://dotrights.org/business/primer/; *see also* Yvonne Jones, *Editorial Correspondence*, WIRED, Sept. 2009, at 20 ("Facebook's changes to its privacy settings killed my affection for the company . . . it's revoking one of the things I valued most about it and in the process ensuring that I trust it less.").

[53] Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Jan. 18, 2010).

[54] *See* Joseph Turow, et al., *Americans Reject Tailored Advertising* (2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[55] *See* PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/.

[56] *See, e.g.*, AOL, PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at*, http://dotrights.org/business/primer/node/37 (describing a 2006 incident in which AOL made public "anonymized" search results which were not, in fact, properly anonymized, accidentally releasing identifiable search records of hundreds of thousands of consumers) *and* Arvin Narayanan and Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *available at* http://www.cs.utexas.edu/~shmat/shmat_netflix-prelim.pdf (describing how the researchers' "de-anonymized" anonymized Netflix-consumer movie reviews that had been released by Netflix).

[57] *See generally* PRIVACY AND FREE SPEECH: IT'S GOOD FOR BUSINESS, *available at* http://dotrights.org/business/primer/.

[58] *See* Peter Wayner, *You Know About Backups. Now, Do It Online*, N.Y. TIMES, Oct. 22, 2008, *available at* http://www.nytimes.com/2008/10/23/technology/personaltech/23basics1.html ("Intronis, for instance, has never received a subpoena for stored data and couldn't provide the information even if it did. 'We don't consider ourselves as having access to customer's data. It's not even a thought,' said Mr. Webster.").



A Publication of the ACLU of Northern California

January 2010

www.dotrights.org
www.aclunc.org/tech

June 14, 2010

*Via email: privacy-noi-2010@ntia.doc.gov*

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: Comments on the Notice of Inquiry on "Information Privacy and Innovation in the Internet Economy"

The American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau (collectively "we" or the "undersigned associations") appreciate the opportunity to provide our views in response to the Department of Commerce's ("Department") Notice of Inquiry on information privacy and innovation in the Internet economy. We encourage the Department to consider the tremendous value created by online advertising for both consumers and the economy, and the impact that self-regulation and consumer education have on consumer privacy.

The undersigned associations believe that the appropriate approach to address consumer online privacy is through industry self-regulation and education. Existing and emerging robust self-regulatory principles address privacy concerns while ensuring that the Internet can thrive, thereby benefiting consumers and the U.S. economy.

## I. Online advertising generates a significant consumer and economic benefit.

For almost two decades, online advertising has been an economic driver that has fueled Internet growth and delivered innovative tools and services used by consumers and business to connect, communicate, and contribute to the continued evolution of the Internet. This advertising-based model continues to drive Internet growth and deliver consumer benefit. According to a recent study entitled *Economic Value of Advertising-Supported Internet Ecosystem* conducted by Harvard Business School Professors John Deighton and John Quelch, e-commerce and online advertising contribute $300 billion each year to the U.S. economy and employ 3.1 million Americans.[1]

The revenue generated by online advertising supports the creation and entry of new businesses, communication channels (*e.g.*, micro-blogging sites and social networks), and free or low-cost services and products (*e.g.*, email, photo sharing sites, weather, news, and entertainment media). Online advertising enables consumers to compare prices, learn about products, and find out about new and local opportunities. Additionally, the Internet empowers small businesses, enabling them to flourish and compete where costs would otherwise hinder their entry into the market. Consumers

[1] Deighton & Quelch, *Economic Value of Advertising Supported Internet Ecosystem*, at 4, 12 (June 10, 2009), *available at* http://www.iab.net/media/file/Economic-Value-Report.pdf.

value the tremendous benefit that they gain from such ad-supported services and products and from the diversity of online companies. Thus, the Department should avoid making recommendations that could unintentionally stifle this positive contribution to the economy and consumer benefit.

Perhaps most importantly, the record demonstrates that consumers are increasingly embracing and participating in Internet activities. A quick analysis of the most recent indicators reveal that online retail sales during the 2009 holiday season increased 5 percent from 2008, according to a report by the research firm comScore, with consumers spending $27 billion more than the previous year. Consumers were more satisfied than ever with their e-commerce experiences, according to ForeSee Results' E-Retail Satisfaction Index, giving their online shopping adventures a score of 79 out of 100, the highest rating since the survey began in 2001. Perhaps most informative, research demonstrates that consumers are generally not reluctant to participate online due to advertising and marketing practices. According to a 2009 survey by the National Retail Association, of those consumers who were reluctant to shop online, just 0.1% cited concerns over privacy and the same miniscule percentage (0.1%) cited concerns about retailers tracking online activity.

**II. Self-regulation addresses concerns with online advertising.**

Self-regulation continues to be the appropriate approach for addressing the interplay of online privacy and online advertising practices. This approach has successfully demonstrated its ability to address consumer concerns while ensuring that the marketplace is not stifled or smothered by overreaching and rigid regulation. Unlike formal regulations, which can become quickly outdated in the face of evolving technologies, self-regulation provides industry with a nimble way of responding to new challenges presented by the evolving Internet ecosystem.

In the specific area of online behavioral advertising, recent self-regulation should be given more opportunity to succeed. The undersigned associations, with the Council of Better Business Bureaus, spearheaded the development of the groundbreaking *Self-Regulatory Principles for Online Behavioral Advertising* ("Principles"), which were released in July 2009.[2] The Principles are designed to apply broadly to the diverse set of actors that work interdependently to deliver relevant advertising intended to enrich the consumer online experience, and to foster consumer friendly standards that are to be applied throughout the online ecosystem. There are seven basic Principles, which call for consumer education, the provision of new choice mechanisms, data security, heightened protection for certain sensitive data, consent for certain material changes to online behavioral advertising data collection and use policies, and strong enforcement

[2] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

mechanisms.[3] Lastly, the Principles require enhanced notice outside of the privacy policy so that consumers could be made aware of the companies they interact with while using the Internet. Together, these Principles will increase consumers' trust and confidence in how information is gathered from them online and how it is used to deliver advertisements based on their interests.

This cross-industry self-regulatory initiative represents an unprecedented collaborative effort by the entire marketing-media ecosystem. The effort began in April 2008 by convening a task force to evaluate existing self-regulatory efforts. In October 2008, the task force began drafting principles together with eight industry associations and 25 companies. In January 2009, we publicly announced our efforts, and in April 2009, we began socializing the principles within industry.[4] In July 2009, we formally released the *Self-Regulatory Principles for Online Behavioral Advertising*.[5]

Beginning in August 2009, the undersigned associations have turned to enforcement, operational implementation, and educational planning related to the Principles. The Direct Marketing Association ("DMA") has incorporated the Principles into its *Guidelines for Ethical Business Practice*, which are binding on all DMA member companies and are actively enforced by the DMA.[6] The Council of Better Business Bureaus is also implementing accountability mechanisms and evaluating technology solutions for a robust monitoring and compliance program.

In January 2010, the same coalition announced its intention to select wording and a link/icon that participating companies will use when engaged in online behavioral advertising to indicate their adherence to the Principles and as the link that provides consumers with easily accessible disclosures about data collection and use practices associated with online behavioral advertising. In April 2010, the IAB, along with the Network Advertising Initiative, released the CLEAR (Control Links for Education and Advertising Responsibly) Ad Notice Technical Specifications, a set of common technical standards for this standard, clickable icon.[7]

---

[3] The Principles apply heightened protection for children's data by applying the protective measures set forth in the Children's Online Privacy Protection Act. Similarly, this Principle requires consent for the collection of financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for online behavioral advertising purposes.

[4] Press Release: *Key Advertising Groups to Develop Privacy Guidelines for Online Behavioral Advertising Data Use and Collection*, January 13, 2009, available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-011309.

[5] Press Release: *Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising*, July 2, 2009, available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

[6] Direct Marketing Association, *Guidelines for Ethical Business Practice* (revised January 2010) available at http://www.dmaresponsibility.org/guidelines/.

[7] Press Release: *IAB and NAI Release Technical Specifications for Enhanced Notice to Consumers for Online Behavioral Advertising: Critical Step in Interactive Industry's Ongoing Self-Regulatory Efforts*, April 14, 2010, available at http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-041410.

Industry's quick response in the area of online behavioral advertising demonstrates the benefits of self-regulation. Self-regulation is responsive to government and consumer concerns, feasible in light of existing technology and business practices, and flexible enough to respond to the rapid innovation that is characteristic of the high-technology marketplace. The undersigned associations are committed to vigorous enforcement of our self-regulatory programs, which helps compliant businesses by promoting consumer trust.

**III. Consumer and business education is critical to protecting consumers online.**

The undersigned associations believe that consumer education is vital to demystifying online advertising practices and informing consumers of the availability of choice and tools to control one's online experience. The "Privacy Matters" consumer education initiative to deliver information about online advertising is now expanding into its second phase. In this phase of the educational campaign, we will promote awareness of the Principles among both consumers and businesses.

A. Phase One: Consumer Education

In December 2009, IAB launched "Privacy Matters," an education campaign designed to educate consumers about how they can manage their online experience and to help consumers better understand and appreciate how Internet advertising supports the Internet.[8] IAB, through the participation of its online publisher members, has committed to deliver more than 500 million online public service announcements ("PSAs"), providing details about online advertising and tools that consumers can use to manage their online privacy. The eye-catching "Privacy Matters" campaign is designed to provide interactive educational messages for consumers about key aspects of online advertising, as well as to make resources available to consumers about the availability of choice, online security, and tips on how to safely surf the web.

Through February 2010, the campaign has delivered more than 353 million impressions. The results thus far have been excellent. Ten percent of all delivered impressions are being "moused-over" by consumers and the average amount of time that consumers spend on the PSA once they roll over it is 28 seconds. Thus, the time spent viewing a PSA is equivalent to about twice the exposure time of the most common, 15-second, TV commercial. Perhaps most encouraging, the click-through-rate ("CTR") for this campaign is out performing the standard 0.03% - 0.06% CTR range for public service campaigns. These numbers demonstrate that consumers are taking the time to read the information and interact with the educational resources. In all, the "Privacy Matters" campaign is effectively engaging consumers.

B. Phase Two: Principles

Currently, the undersigned associations are poised to embark upon a second educational phase intended to educate consumers and businesses about the Principles.

[8] IAB's "Privacy Matters" campaign, available at http://www.iab.net/privacymatters/.

This multifaceted campaign will include the launch of an industry Web site that will include educational resources, the delivery of public service announcements regarding the Principles, and community outreach by the participating trade associations.

This campaign will educate the online community about the nature and operation of the new self-regulatory program. We will educate the community on the purpose and functionality of the selected icon/link used to provide notice of online behavioral advertising practices. For consumers, the campaign will describe the availability of this enhanced notice in all instances when and where online behavioral advertising occurs. Consumers will be made aware of the types of information collected and used for advertising purposes and will be informed of the availability of new choice mechanisms and how to exercise such choice. The campaign will also provide educational materials and resources to the business community that will explain the scope and purpose of the Principles. In addition, the trade associations will continue to work with their members to explain how businesses can come into compliance with the industry principles.

* * *

We thank you for the opportunity to offer our comments on this important matter, and we look forward to continuing to work with you as the Department addresses these matters. Please contact Stuart Ingis at (202) 344-4613 with any questions.

Sincerely,

American Association of Advertising Agencies
Association of National Advertisers
Direct Marketing Association
Interactive Advertising Bureau

cc: Stuart Ingis, Venable LLP
Michael Signorelli, Venable LLP

# ALAN CHARLES RAUL

Comments of Alan Charles Raul. These comments do not necessarily reflect the views of Sidley Austin LLP or any of its clients.

1. The Department of Commerce Should Promote Harmonization, Coordination, and Streamlining of Privacy, Security and Consumer Protection in the United States and Internationally in Order to Achieve a High Level of Substantive Privacy Protection Without Imposing Needless Burdens; and Commerce Should Ensure that the Costs and Benefits of Privacy Regulation Are Consistently and Fairly Evaluated.

There is a prevailing sense today that existing privacy and data security standards are more complicated, conflicting and onerous than necessary or appropriate in order to achieve a high substantive level of personal protection. There are so many international, federal, state, local and private standard-setters striving to achieve fairly comparable substantive objectives that the transaction costs of compliance are not always producing commensurate benefits for society. Moreover, while territorial jurisdiction, and separate regulation for separate political communities, continue to be immensely germane even as the world flattens, it is indisputably true that the flow of data and deployment of innovations in the information-based economy are inherently less territorial than other elements of international trade, commerce, finance, manufacturing or agriculture.

More effective coordination of privacy, data security and trade practice regulation could foster greater certainty, predictability and innovation – and substantive protections – benefiting both businesses and consumers involved in the Internet economy. Today, there is too much counter-productive conflict – or perceived conflict – between the rules of different states, agencies, countries and multilateral institutions.

In view of the relatively substantial degree of agreement over fundamental principles and fair information practices, the conflict of regulatory standards is pure friction – it imposes a drag on the economy in terms of excessive compliance costs and citizen confusion without necessarily achieving meaningful additional benefits in privacy, security or consumer protection.

The Department of Commerce should thus ensure that data protection regulations are analyzed under Executive Order 12866 to assess whether

the costs and benefits (including intangible benefits) are properly and reasonably aligned. This process should also cover privacy and data security regulations issued or administered by agencies that are not directly accountable to the President, such as the Federal Trade Commission, Federal Communications Commission, Securities and Exchange Commission, etc. The American people are entitled to privacy and security regulations that are substantively protective and cost-effective (taking into account relevant non-pecuniary harms where appropriate). Regulation that has not been submitted to cost-benefit analysis will surely not be as beneficial or efficient as regulation that does pass through this salutary process. To the extent that independent agencies are not formally covered by or subject to Executive Order 12866, the Commerce Department should encourage such agencies to submit to such review and inter-agency comment as a matter of good government and sound administration.

The Department of Commerce should therefore exercise a leadership role within the United States, perhaps in tandem with the Office of Management and Budget, to help harmonize, or coordinate, and streamline the conflicting standards at play throughout the federal government (banking agencies, HHS, FCC, FTC, etc.), state governments and international regulators. Such harmonization or coordination could perhaps be advanced internationally through the Transatlantic Economic Council with the EU, or through parallel activity at the OECD or similar multilateral institutions.

The Department of Commerce, together with the Office of the U.S. Trade Representative, should also ensure that impediments to the flow of personal information and other data do not constitute barriers to international trade that can thwart digital innovation and efficiencies that benefit the economy of the United States, employment and consumer welfare. To the extent, that foreign barriers to information cannot be justified in accordance with legitimate policy objectives to advance substantive privacy rights and protection, those barriers should be challenged under available international agreements.

The Department of Commerce should seek to advance an international approach to the cost-benefit evaluation of privacy and security regulations that could be fairly and reasonably applied to improve different regulatory approaches around the world.

Domestically, Commerce should consider convening councils of interested parties throughout the U.S. including businesses, state attorney generals, consumer regulators, insurance commissioners, etc., to help elaborate best practices and narrow perceived differences in applicable substantive standards for privacy, data protection and Cybersecurity. Specifically, Commerce should determine whether the state-by-state standards for privacy and data security adopted in (e.g.) Massachusetts, California, and elsewhere help advance or impede a robust national digital economy.

In short, the extraterritorial effects of a jurisdiction's regulation of digital and electronic information should be the subject of the Department of Commerce's attention.

Such consideration should take account of the insightful analysis set forth by Judge Loretta A. Preska in American Library Association v. Pataki, 969 F. Supp. 160 (S.D. N.Y. 1997), under the heading of "Federalism and the Internet: The Commerce Clause." Judge Preska wrote:

> The borderless world of the Internet raises profound questions concerning the relationship among the several states and the relationship of the federal government to each state, questions that go to the heart of "our federalism." . . . .
>
> The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation -- and in particular, the national infrastructure of communications and trade -- as a whole.
>
> The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in *Gibbons v. Ogden,* recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to

> term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce. Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.
>
> . . . . Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether.

2. <u>The Commerce Department Should Advocate Internationally on Behalf of the Adequacy of the U.S. Data Protection Regime</u>

As is well known among privacy experts and multinational companies, the EU has not deemed the U.S. regime for privacy and data protection to be adequate, and the E.U. presumably considers the U.S. regime not to be substantially equivalent to that of the EU and its member states. This judgment by the EU results in the imposition of significant hurdles to the efficient management of human resource and customer data within global corporations. Personal data emanating from an organization's EU locations cannot be shared with the same organization's U.S. locations unless certain specific compliance mechanisms are put into place. While most large entities have managed to cope successfully with the demands of the E.U., the necessity of U.S. companies being compelled to do so should be addressed by the Commerce Department.

Given the numerous privacy laws and regulations, and general unfair and deceptive trade practice statutes, enforced by the banking and financial regulatory agencies, the Federal Trade Commission, the Federal Communications Commission, the Department of Health and Human Services, the Department of Education, state attorneys general, state insurance commissions, private plaintiffs, the Payment Card Industry and a vigorous advocacy community, it cannot reasonably be argued that the United States has a lower level of data protection than any jurisdiction in the world. Indeed, a strong case can and should be made that the U.S. data protection regime leads the world in both substantive rigor and

practical flexibility -- especially with regard to particularly sensitive categories of personal information such as financial, medical or communications data (each of which is subject to specific Acts of Congress and dedicated, sectoral regulation).

The United States has also plainly led the way internationally with regard to data security, where data breach notification and affirmative information security requirements are now well entrenched in U.S. law and practice.

Accordingly, Commerce should consider advocating that the E.U. determine without further delay that the U.S. system for protecting personal privacy and information security is at least as stringent as that of the E.U. To the extent that the E.U. can identify any specific areas of data collection or use where the U.S. system does not adequately protect the regulatory interests of E.U. citizens, those specific, limited circumstances could be addressed separately with special protections or limitations, rather than bogging down the entire international flow of data across the Atlantic.

The Commerce Department, with the Department of Justice and the Securities and Exchange Commission, should also play a role in ameliorating international disputes over civil discovery, internal investigations, and compliance with U.S. corporate laws. While it must be acknowledged that certain other countries object to the substantive policies underlying discovery in U.S. civil litigation and the obligations of U.S. companies to ferret out violations of the Foreign Corrupt Practices Act and other corporate malfeasance, Commerce should help lead an effort to diminish the considerable tensions and conflicts faced by U.S. companies that strive to comply simultaneously with legal obligations in all of the numerous jurisdictions in which they operate.

3. <u>The Greatest Threats to Personal and Proprietary Information Today Arise in the Realm of Cybercrimes and Breaches of Cybersecurity Perpetrated by Sophisticated Criminals and Hostile State-Supported Actors; Commerce Should Facilitate Collaboration Between the Public and Private Sectors and Help Reconcile the Resources Allocated to Cybersecurity with Those Allocated to Basic Information Security and Data Breaches.</u>

The Department of Commerce, working with White House, OMB, the Office of the Director of National Intelligence, the Department of Homeland

Security and the Cyber Command in the Department of Defense could help mediate the necessary collaboration between the federal government and the private sector to ensure that the requisite knowledge and resources are shared with private companies to help protect personal information, critical information infrastructures, and important intellectual property and proprietary information against aggressive exploitation by sophisticated cybercriminals.

The risk of such cyber attacks has been identified as a leading threat to the national security and economic well being of the United States. The Department of Commerce should play a role in ensuring that concerns over marketing uses of personal information by legitimate businesses do not overwhelm attention to the greater risks of cyber attacks and cybercrimes by avowedly hostile and criminal enterprises.

4. Commerce Should Ensure that the Benefits of the "Notice and Choice" Paradigm – Namely, Allowing Considerable Freedom of Contract, Flexibility and Innovation – Are Preserved Even as Additional Privacy Regulations Are Being Considered by Other Federal, State and International Regulators.

There has been considerable consternation over whether the current "notice and choice" paradigm, which requires companies that collect information about consumers to provide notice about their data practices and obtain the express or implied consent of their consumers to those practices, is working well enough to protect consumers' privacy interests. In particular, concern as been expressed whether any consumers actually read and understand the privacy polices that are intended to convey such notice and effectuate such consent.

While addressing such concerns can and should be the subject of extensive comments and deliberation, the Commerce Department should take note of the fact that there is an extensive community of privacy advocates that routinely scrutinizes privacy policies and often raises (effective) objections when such policies are perceived to over-reach. While the content of privacy policies, and the interaction of such policies and affected consumers, can no doubt be considerably enhanced, there is little reason to thoroughly abandon a paradigm that the federal government has itself championed in legislation, regulation and enforcement, and which allows companies to innovate and communicate relatively flexibly.

**Before the**
**Department of Commerce**
**National Telecommunications and Information Administration**
**Washington, D.C. 20230**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0238-02 |
| | ) | |

# Recommendations of the American Federation of Musicians of the United States and Canada, AFL-CIO

The American Federation of Musicians of the United States and Canada, AFL-CIO ("AFM"), submits these comments in response to the National Telecommunications and Information Administration's (NTIA) request published in the Federal Register on April 23, 2010. These comments address privacy concerns and their relationship to piracy. A balanced approach to fighting piracy must be implemented. While AFM agrees that no ISP should be allowed to unreasonably invade users' privacy, there must be enough flexibility in the regulations to allow ISPs to root out illegal conduct, such as copyright infringement, on the Internet.

The AFM is an international labor organization composed of over 230 Locals across the United States and Canada, with over 90,000 professional musician members. AFM members perform live music of every genre – from symphonic and opera to Broadway musicals, and from jazz, country, folk and rock to Latin, hip-hop, blues and pop – and in every size and type of venue from major concert halls to the smallest bars and lounges. AFM members record music pursuant to industry-wide agreements negotiated by the AFM with the recording, motion picture, television, radio and commercial announcement industries, so that their work is an integral part of the sound recordings, movies and television programs that make up so much of America's culture and America's economy. AFM members include studio musicians who record film scores and appear as "background" performers on sound recordings. They also include featured artists of every type, from the glamorous and successful, to the mid-tier artists with solid careers and loyal fan bases, to the emerging artists who are struggling to succeed in the business.

The Internet is crucially important to AFM members. Members use it and are affected by it in a multitude of different ways, including ways that affect their live performance opportunities and ways that affect their ability to market their recorded work. The AFM and its members have struggled to preserve and enhance the role of live music performance in America's culture and economy for most of the AFM's one-hundred-year-plus existence, and the Internet now plays a

very significant role in that important mission. AFM Locals use the Internet not only to communicate with AFM members, but also to reach out to their local communities, educating them on the desirability and availability of live music, and providing referral services that serve the twin goals of leading local community members to choose live music and providing gigs to musicians.

For individual musicians and groups, the Internet provides a means not only to advertise and expand their live performances, but also to sell their recordings on sites like iTunes and CD Baby, or on their own websites, or to reach audiences via streaming services like Pandora or Slacker. Indeed, the Internet has become a means to promote all facets of their careers by communicating directly to the public and building relationships with fans and potential fans. This is true for virtually all musicians, but particularly for the many musicians who record with small or intermediate-size independent labels, or who form their own labels and are building careers with little or no outside investment. It is also true for large and small arts associations like symphony, opera and ballet orchestras, who increasingly rely on the Internet as a means of growing their relationships with and support from the public as well as a means of promoting their live performance seasons and distributing recordings of their music.

However, the Internet is a double-edged sword: it creates unprecedented opportunities for musicians to sell their work, but it also allows piracy and theft to proliferate. Musicians must be able to take full advantage of the Internet, while being confident that their work is safe. And in order to have a serious discussion about curbing Internet piracy, Internet users' privacy rights must be addressed.

Throughout the debate regarding curbing Internet piracy, many methods for protecting copyrighted content have been suggested, some more invasive than others. One of the most invasive methods is Deep Packet Inspection (DPI). DPI software, once deployed over the Internet, will open and examine the packets of information traversing the network, no matter if it is an illegal file transfer or a personal e-mail. If the software finds copyrighted content contained in those information packets the software will deal with it accordingly. While this may be an effective method for rooting out illegal piracy, the invasive nature of DPI makes it unsuitable for wide deployment. DPI can indiscriminately look at any packet of information traversing the Internet; therefore it can conceivably examine non-suspicious, personal Internet traffic. Thus, DPI serves as a prime example of an anti-piracy method that is not suitable for implementation on a widespread basis because of privacy concerns.

If DPI lies on one end of the spectrum – the most invasive – then there are other technologies that lie on the other – less invasive – end. For example, software can be installed in the network that examines links contained in websites for copyrighted works. If the software finds that the links contain copyrighted content, then the software can alert the ISP, copyright holder or third party. At no point will the software open private packets of information; it merely follows publicly available links.

Mentioning these two particular methods for curbing Internet piracy is to demonstrate that, contrary to some rumblings from activists, curbing Internet piracy does not automatically equal an invasion of users' privacy. It all depends on the method used, and the rules for the use of the method. Thus, it is important that the NTIA work with other government agencies, lawmakers and outside organizations to implement methods for curbing Internet piracy that do not allow

ISPs or other businesses to unduly invade users' privacy. Ideally, the NTIA will recommend to the President specific methods that are acceptable for curbing Internet piracy. NTIA's recommendations should not represent an exhaustive list, but merely the "best practices" for combating piracy in a way that respect users' privacy.

Publishing a list of best practices for piracy protection is recommended for a number of reasons, namely it will show ISPs, businesses or other organizations what methods are acceptable for curbing Internet piracy. Furthermore, publishing a best practices list instead of implementing specific methods or dictating what may and may not be deployed, allows for new methods to be experimented with without fear of burdensome regulations.

In order to properly develop and publish the "Best Practices List," NTIA should solicit the advice of experts in the field, other governmental agencies, labor unions, businesses, members of the public and advocacy groups for their opinions. Each method should then be studied and examined in order to make sure its implementation does not unreasonably violate users' privacy. It is important to recognize that the goal of anti-piracy methods is to root out illegal activity (which copyright infringement is), thus a certain invasion of users' privacy must be tolerated (if a transfer is suspected to contain illegal content). The key is that there is not an undue invasion of users' privacy rights.

In conclusion, AFM understands that requiring ISPs to curb piracy opens the door to increased invasion of users' privacy. However, AFM believes that technologies do exist that will allow for effectively combating piracy while respecting users' privacy. AFM asks NTIA to study the methods that exist for curbing piracy, determine which methods will not unduly invade users' privacy and then publish a list of acceptable methods.

Respectfully submitted,

Thomas F. Lee, International President
AMERICAN FEDERATION OF MUSICIANS
OF THE UNITED STATES AND CANADA
1501 Broadway, Suite 600
New York, New York 10036

June 14, 2010

**Comments of ARMA International**
**Information Privacy and Innovation in the Internet Economy**
**[Docket No. 100402174–0175–01]**
**RIN 0660–XA12**

**Submitted electronically (as a PDF document) to: privacy-noi-2010@ntia.doc.gov by fmoore@smithbucklin.com for Bob.Tillman@armaintl.org.**

**Subject line: "PRIVACY NOTICE OF INQUIRY DOCKET NO 100402174-0175-01"**

**Date: June 7, 2010**

## INTRODUCTION AND SUMMARY

ARMA agrees with the importance of creating systems and regimes that will give consumers the confidence that their personal information is properly created, managed, used and disposed of relative to engaging in Internet commerce –

> Consumers have expressed concern regarding new or unexpected uses of their personal information by online applications. Since Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained. At the same time, companies need **clear policies**[1] that enable the continued development of new business models and the free flow of data across state and international borders in support of domestic and global trade. Our challenge is to align flexibility for innovators along with privacy protection.

ARMA commends the Department[2] in its search for policies that will –

---

[1] ARMA has long held that safeguarding records, information and data depends not only on effective and emerging tools, but also on flexible, principles-based recordkeeping programs – articulated as policies and procedures that are endorsed across an enterprise and supported by an organization's senior leadership.

[2] Office of the Secretary, U.S. Department of Commerce; National Telecommunications and Information Administration, U.S. Department of Commerce; International Trade Administration, U.S. Department of

1. Enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy

2. Enhance the public confidence necessary for full citizen participation with the Internet

3. Uphold fundamental democratic values essential to the functioning of a free market and a free society.

We also look forward to the progress of the Task Force[3] and its ability to identify and evaluate privacy challenges[4].

Of particular interest to ARMA is the observation –

> In addition to the growth of online commerce, the Internet, the World Wide Web, and associated information systems have lead to an unprecedented growth in productivity over the last decade. More businesses are using the Internet to provide **electronic records** to customers and trading partners, and enterprises are shifting to a digital back office and greener business environment. Although this has spurred additional green innovation, the fact that increasingly **more data is being stored electronically and aggregated** creates new challenges in the privacy arena.
>
> Sustaining the growth of digital commerce and U.S. commerce generally will require continued innovation in **how information is used**

---

Commerce; and National Institute of Standards and Technology, U.S. Department of Commerce.

[3] Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education and political and cultural life, the Department has made it a top priority to ensure that the Internet remains open for innovation. The Department has created an Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment.

[4] Responses to this Notice will assist the Task Force in preparing its report on Privacy and Innovation in the Information Economy. The purpose of this report will be to identify and evaluate privacy policy challenges, and to analyze various approaches to meet those challenges.

**and shared**[5] across the Internet. Commerce today depends on online communication and the transmission of significant amounts of data. Key to the current inquiry, the Department believes this development places **data protection**[6] in a new light.

With these comments, ARMA respectfully recommends the use of *generally accepted recordkeeping principles* for addressing concerns relating to the use and protection of records and files of all formats, which will contain personal information required in commerce today. Internet commerce will present its own challenges relative to tools (technology) that should be employed, but ARMA believes that more effective protections are achieved by combining appropriate tools with enterprise-wide policies and procedures that speak to the management of records and information.[7] The information collected from consumers and maintained, used, and disposed of by various business models are records, however stored, and should be covered by appropriate

---

[5] How information is used and shared is better characterized as an organization's recordkeeping policies and procedures (program), and as such, would speak to the creation, retention, and disposition, including destruction as and when appropriate, of records of information.

[6] Effective data protection will include an enterprise-wide program of policies and procedures that speak to the life cycle management of information sought to be protected. ARMA believes that the most innovative approach to data management (and therefore protection) is through a flexible application of generally accepted recordkeeping principles. A principles-based approach to data management will allow organizations to tailor programs to their sectors, business models, and types of records and information required. Generally accepted recordkeeping principles also speak to 1) transparency of an organization's recordkeeping program – documenting the disposition of information in an understandable manner, and 2) accountability through the support of senior management and adoption of policies and procedures to guide personnel and ensure program auditability.

[7] From the perspective of ensuring appropriate management of personal information, it should be unnecessary to distinguish between online commerce and other forms of commerce where the sellers of goods or services also collect information from clients, consumers, patients or others with relationships with vendors and providers.

recordkeeping policies, informed by generally accepted recordkeeping principles, and supported by appropriate technology.[8]

The *generally accepted recordkeeping principles* speak to accountability, transparency, and compliance by the enterprise and integrity, protection, availability, retention and disposition of records and information. These principles create a foundation for an appropriate and effective recordkeeping program that speaks to enterprise-wide commitments and life cycle management of records and information – and their flexibility provide appropriate and effective application to protecting personal information associated with Internet commerce and in the possession and custody of Internet businesses. With these principles –

1. The enterprise would establish a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

2. The recordkeeping program would be constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate manner and the appropriate or required time, and such disposition is documented.

## GENERALLY ACCEPTED RECORDKEEPING PRINCIPLES

ARMA believes that eight *generally accepted recordkeeping principles* can provide effective and objective guidance for the development of clear policies relative to managing records and information, including personal information that is part of Internet commerce.

---

[8] Furthermore, it should be noted that information collected on-line for purposes of enhancing Internet commerce, or supporting business models or consumer needs via the Internet, should be viewed as records, whether more accurately described as record series, files of records or classes of records.

Organizations have historically been challenged to establish appropriate and effective recordkeeping regimes, intended to promote records and information management that meets vital business needs, supports contractual obligations, and ensures compliance with statutory and regulatory obligations. Too often, by organizations and by those with oversight responsibilities over regulated entities, records and information management has been defined solely by regulatory requirements (e.g. safeguarding and disposal responsibilities as recognized by the Federal Trade Commission for non-financial institutions). However, protecting personal information from inappropriate or criminal use requires an enterprise-wide approach more comprehensive than simply complying with statutory and regulatory recordkeeping regimes (often referred to as "document retention").

ARMA believes that recordkeeping requirements can and should be tailored to any organization that possesses and controls personal information. This makes it more likely that organizations will voluntarily develop and engage meaningful recordkeeping, and it also provides guidance to others looking to organizations to demonstrate the stewardship over records and information reasonably expected of them[9].

Relative to this inquiry, ARMA further believes that a principles-based standard will position organizations to more likely mitigate known and unknown risks and creates a reasonable standard for purposes of determining compliance with any statutory or regulatory requirements.

As such, the policies and procedures that should be expected of these organizations are made most effective, with objectivity and reasonable levels of investment, by being based on the *generally accepted recordkeeping principles* set forth below – recognizing at the very least that no one size or format of any operational policies and procedures will fit all similarly situated entities.

For these reasons, ARMA recommends, as the foundation of any expectations that may be created regarding clear policies for managing personal information, that the Task Force look to these *generally accepted recordkeeping principles* –

---

[9] We note the expectations of customers and consumers that their personal information be appropriately safeguarded. As such, the most effective safeguards are those that are made systemic to the entire organization through known policies and procedures.

**Accountability** – An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.

Essential to this principle are the following program elements:

1. The records manager is an officer of the organization and is responsible for the tactical operation of the ongoing program on an organization-wide basis.
2. The records manager is actively engaged in strategic information and record management initiatives with other officers of the organization.
3. Senior management is aware of the program.
4. The organization has defined specific goals related to accountability.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The records manager is a senior officer responsible for all tactical and strategic aspects of the program.
2. A stakeholder committee representing all functional areas and chaired by the records manager meets on a periodic basis to review disposition policy and other records management-related issues.
3. Records management activities are fully sponsored by a senior executive.

**Transparency** – The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

Essential to this principle are the following program elements:

1. Transparency in recordkeeping is taken seriously and information is readily and systematically available when needed.
2. There is a written policy regarding transparency.
3. Employees are educated on the importance of transparency and the specifics of the organization's commitment to transparency.
4. The organization has defined specific goals related to transparency.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Exceeds the essential elements above in the following ways:
    a. Transparency is an essential part of the corporate culture and is emphasized in training.
    b. The organization monitors compliance on a regular basis.

**Compliance** – A recordkeeping program shall be constructed to comply with the applicable laws and other binding authorities, as well as the organization's policies.

Essential to this principle are the following program elements:

1. The organization has identified all relevant compliance laws and regulations.
2. Record creation and capture are systematically carried out in accordance with records management principles.
3. The organization has a strong code of business conduct which is integrated into its overall information governance structure and recordkeeping policies.
4. Compliance and the records that demonstrate it are highly valued and measurable.
5. The hold process is integrated into the organization's information management and discovery processes for the "most critical" systems.
6. The organization has defined specific goals related to compliance.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The organization has implemented systems to capture and protect records.
2. Records are linked with the metadata used to demonstrate and measure compliance.
3. Employees are trained appropriately and audits are conducted regularly.
4. Records of the audits and training are available for review.
5. Lack of compliance is remedied through implementation of defined corrective actions.
6. The hold process is well-managed with defined roles and a repeatable process that is integrated into the organization's information management and discovery processes.

**Integrity** – A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.

Essential to this principle are the following program elements:

1. The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes.
2. Appropriate data elements to demonstrate compliance with the policy are captured.
3. The organization has defined specific goals related to integrity.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. There is a clear definition of metadata requirements for all systems, business applications, and paper records that are needed to ensure the authenticity of records.
2. Metadata requirements include security and signature requirements and chain of custody as needed to demonstrate authenticity.
3. The metadata definition process is an integral part of the records management practice in the organization.

**Protection** – A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.

Essential to this principle are the following program elements:

1. The organization has a formal written policy for protecting records and centralized access controls.
2. Confidentiality and privacy are well defined.
3. The importance of chain of custody is defined, when appropriate.
4. Training for employees is available.
5. Records and information audits are only conducted in regulated areas of the business. Audits in other areas may be conducted, but are left to the discretion of each function area.
6. The organization has defined specific goals related to record protection.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. The organization has implemented systems that provide for the protection of the information.
2. Employee training is formalized and well documented.

3. Auditing of compliance and protection is conducted on a regular basis.

**Availability** – An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Essential to this principle are the following program elements:

1. There is a standard for where and how official records and information are stored, protected, and made available.
2. Record retrieval mechanisms are consistent and contribute to timely records retrieval.
3. Most of the time, it is easy to determine where to find the authentic and final version of any record.
4. Legal discovery is a well defined and systematic business process.
5. The organization has defined specific goals related to availability.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. There are clearly defined policies regarding storage of records and information.
2. There are clear guidelines and an inventory that identifies and defines the systems and their information assets. Records and information are consistently and readily available when needed.
3. Appropriate systems and controls are in place for legal discovery. Automation is adopted to facilitate the implementation of the hold process.

**Retention** – An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.

Essential to this principle are the following program elements:

1. A formal retention schedule that is tied to rules and regulations is consistently applied throughout the organization.
2. The organization's employees are knowledgeable about the retention schedule and they understand their personal responsibilities for records retention.
3. The organization has defined specific goals related to retention.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Employees understand how to classify records appropriately.
2. Retention training is in place. Retention schedules are reviewed on a regular basis, and there is a process to adjust retention schedules as needed.
3. Records retention is a major corporate concern.

**Disposition** – An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.

Essential to this principle are the following program elements:

1. Official procedures for records disposition and transfer are developed.
2. Official policy and procedures for suspending disposition have been developed.
3. Policies and procedures exist and they are standardized across the organization.
4. Individual departments have devised alternative procedures to suit their particular business needs.
5. The organization has defined specific goals related to disposition.

As applied to personal information requiring protection and security, this principle would require at least the following additional program elements –

1. Disposition procedures are understood by all and are consistently applied across the enterprise.
2. The process for suspending disposition due to legal holds is defined, understood, and used consistently across the organization.
3. Electronic information is expunged, not just deleted, in accordance with retention policies.

## RESPONSE TO NOTICE OF INQUIRY QUESTIONS

ARMA respectfully submits its comments to the questions raised by the Department and restated below, focusing our observations and recommendations on the role that programs, policies, and procedures relative to records and information management can play in effectively creating transparent and auditable regimes intended to safeguard personal information.

*The U.S. Privacy Framework Going Forward*

The Department raises the question whether the traditional "notice and choice" approach to consumer protection may be outdated, especially in the context of information-intensive, highly interactive, Web-based services:

**Does the existing privacy framework provide sufficient guidance to the private sector to enable organizations to satisfy these laws and regulations?**

ARMA has long believed that "notice and choice" does not on its own evidence appropriate data management or demonstrate necessary or appropriate safeguards of personal information.[10] Notice can be considered a statement of intention by an organization without demonstrated regimes or mechanisms in place to ensure, document, or audit compliance. Choice is rendered meaningless if personal information is required for the provision of specific goods and services.

**Are there modifications to U.S. privacy laws, regulations and self-regulatory systems that would better support innovation, fundamental privacy principles and evolving consumer expectations? If so, what areas require increased attention, either in the form of new laws, regulations or self-regulatory practices?**

The various regimes established by statute or regulation that speak to protecting the personal information lack 1) a comprehensive approach to the management of information and 2) a clear statement of core principles upon which a management regime should be built. ARMA believes that any program established to protect personal information should be applied across the entire enterprise and thereby deeply imbedded in the business model and mission of the organization. Rather than simply speaking to specific information by establishing retention schedules or requiring safeguarding regimes, ARMA believes that the integrity and management of information is most effectively and efficiently achieved by an enterprise-wide commitment to processes and procedures that ensure –

The enterprise establishes a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and

---

[10] See Final Model Privacy Form Under the Gramm-Leach-Bliley Act: A Small Entity Compliance Guide issued by the Security and Exchange Commission at http://www.sec.gov/divisions/marketreg/tmcompliance/modelprivacyform-secg.htm.

guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

The recordkeeping program is constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate manner and the appropriate or required time, and such disposition is documented.

**What is the state of efforts to develop a self-regulatory privacy framework? Are there certain minimum or default requirements that should be incorporated either into self regulation or to law?**

ARMA believes that the *generally accepted recordkeeping principles* provide the foundation for voluntary, sound business practices relative to managing records and information, as well as for any recordkeeping and information management requirements established through statute or regulation. A principles-based approach allows the necessary flexibility to ensure a recordkeeping program is appropriate to the organization and meets the needs and expectations of regulators, enforcement agencies, and the general public.

**What is the proper goal of privacy laws and regulations: Should the focus on commercial data privacy policy be on satisfying subjective consumer expectations or is it also necessary to enact objective privacy principles?**

ARMA supports the concept of principles-based privacy and recordkeeping programs. Various iterations of fair information practices have been promoted over the years[11], and these stand as sound guidance for policy

[11] For a currently posted articulation of fair information practices by the FTC, see http://www.ftc.gov/reports/privacy3/fairinfo.shtm. However, it should be noted that this iteration relies on both notice and consent. See the testimony of Robert Pitofsky, Chairman of the Federal Trade Commission (May 25, 2000) on the same: http://www.ftc.gov/os/2000/05/testimonyprivacy.htm.

makers and business leaders[12]. ARMA believes that safeguarding and disposal requirements, as well as fair information practices, are incorporated, appropriately, in the recognized generally accepted recordkeeping principles. Treated in isolation, safeguarding, disposal or other attempts to address protection, are at risk of being less effective, less efficient, and easily marginalized in enterprises whose business models rely so intensely on information sharing and consumers' willingness to add their personally identifiable information to the records and files of Internet businesses. These privacy principles are incorporated in and enhanced by an enterprise-wide recordkeeping program, which speaks not only to privacy principles (protection of personal information), but also to senior management engagement, transparency, auditability, and appropriate life cycle management.

*Sectoral Privacy Laws and Federal Guidelines*

The various sectoral privacy laws and regulations[13] have emerged in the absence of a more comprehensive approach to the stewardship of records and

---

[12] ARMA believes that a principles-based approach, focusing on outcomes relative to records and information, is applicable to both public and private sector entities. See *Memorandum Number: 2008-01* (December 29, 2008) for 8 Fair Information Practice Principles endorsed by the Department of Homeland Security pursuant to the Privacy Act of 1974: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[13] As defined by this Notice: "The U.S. privacy framework is composed of sectoral laws combined with constitutional, statutory, regulatory and common law protections, in addition to industry self-regulation. Sectoral laws govern the handling of personal data considered most sensitive. For instance, the Communications Act includes privacy protections that telecommunication providers and cable operators must follow when handling the personal information of subscribers. The Health Insurance Portability and Accountability Act (HIPAA) stipulates how "covered" health care entities can use and disclose data. The Fair Credit Reporting Act (FCRA) governs how consumer reporting agencies share personal information. The Gramm-Leach-Bliley Act (GLBA) covers certain data held by financial institutions. The Children's Online Privacy Protection Act (COPPA) protects information collected online about children under 13. In addition to these sectoral laws, the Federal Trade Commission Act (FTC Act) provides the FTC authority to combat "unfair or deceptive" business practices. The FTC also provides guidance for businesses regarding privacy and security practices. These laws and guidelines affect U.S. economic activity by controlling how organizations

information that are either required by regulators or enforcement agencies, or are created through the business imperative or other mission critical aspects of an organization.

**How does the current sectoral approach to privacy regulation affect consumer experiences, business practices or the development of new business models?**

ARMA believes that this sectoral approach represents a well intended effort to address the privacy expectations of society; however, the effect of this approach has been to create silos in the management of records and information throughout an organization that result in inefficiencies, break downs in effective auditing and compliance measures, and ignores the practical fact that records and information are not used in isolation to other functional or business activities within most organizations today.

**How does the sectoral approach affect individual privacy expectations?**

This sectoral approach unintentionally results is unnecessary confusion for most individuals. Individuals are faced with notices at their various health care provider offices, such as doctors, dentists, other specialists, as well as providers such as hospitals. Individuals also receive these notices from various financial institutions, and increasingly online as a part of Internet commerce. It is unlikely that most individuals could articulate what these notices say or what obligations if any they impose on the persons or entities giving notice.

More importantly, however, these sectoral requirements have failed to demonstrate to the general public that a set of core principles exist that are applicable to any personal information an individual is required or expected to divulge in the course of seeking goods or services in today's economy.

**What practices and principles do these sectoral approaches have in common, how do they differ?**

Continuing the theme of our comments above, ARMA believes that these sectoral approaches have in common the fact that they are the result of public policy reactions, drawn as narrowly as possible around the records and

---

can use data to develop new products and services or improve existing ones. The laws and guidelines differentiate between categories of data (e.g., health care, financial and other), and they differentiate between data subjects (e.g., children and others)."

information in question, and that these approaches impose a silo-styled set of requirements for purposes of compliance.

**Are there alternatives or supplements to the sectoral approach that should be considered?**

As suggested above, ARMA believes that a principles-based approach to enterprise-wide management of records and information would result in efficiencies for the organizations required to comply with these sectoral approaches, establish a common set of expectations between these organizations and their regulators and any enforcement agencies with jurisdiction over their activities, and inform consumers of the core principles that every organization will employ in the management of their personal information.

**What can be done to make the current framework more conducive to business development while ensuring effective privacy protections?**

As noted above, a principles-based approach to managing records and information creates efficiencies for organizations, both in the consolidation of managing information across its various functions, but also in the consistencies created between regulatory requirements and best practices in the absence of statutory or regulatory mandates. A single set of principles, acknowledged by public policy and public expectations, enhances the ability of organizations, regulators, enforcement agencies, customers, consumers and business partners to understand and dialogue on common ground.

*New Privacy-Enhancing Technologies and Information Management Processes*

The Department points to researchers at universities, think tanks, international organizations and company laboratories that are developing privacy-enhancing technologies and business methods to implement company privacy policies and user preferences and to increase company accountability.

In particular, the Department asks: **What steps can be taken to assure that privacy-enhancing business processes are robust, complied with and regularly updated?**

ARMA believes that an application of generally accepted recordkeeping principles would uniquely motivate innovate business processes, consistent with the recognition that sector, size, complexity, and offerings will influence

the actual policies and procedures employed to appropriately manage records and information.

*The Role for Government/Commerce Department*

The Department notes that "surveys continue to indicate that consumers are concerned or confused about what happens to their personal information online," and asks for input on how to help address barriers to increased innovation and consumer trust in the information economy.

**How can the Commerce Department help address issues raised by this Notice of Inquiry?**

As discussed above, and consistent throughout these comments, ARMA believes that the sectoral approach to protecting personal information has created confusion for the general public and has left regulators with little assurance that records and information are accurate, that the recordkeeping practices of the subject organization is transparent and auditable, or that the expectation that personal information be appropriately managed has become an enterprise-wide value proposition.

ARMA urges the Department to consider the role of *generally accepted recordkeeping principles* in establishing clear policies for internal management, clear ground rules for regulators and enforcement agencies, and clear expectations for consumers.

## CONCLUSION

With these comments, ARMA respectfully recommends the use of *generally accepted recordkeeping principles* for addressing concerns relating to the use and protection of records and files of all formats, which will contain personal information required in commerce today. Internet commerce will present its own challenges relative to tools (technology) that should be employed, but ARMA believes that more effective protections are achieved by combining appropriate tools with enterprise-wide policies and procedures that speak to the management of records and information of all types and for all purposes. Principles for the management of personal information does not require distinguishing between online commerce and other forms of commerce where the sellers of goods or services also collect information from clients, consumers, patients or others with relationships with vendors and providers.

The information collected from consumers and maintained, used, and disposed of by various business models are records, however stored, and

should be covered by appropriate recordkeeping policies, informed by generally accepted recordkeeping principles, and supported by appropriate technology. It should be noted that information collected on-line for purposes of enhancing Internet commerce, or supporting business models or consumer needs via the Internet, should be viewed as records, whether more accurately described as record series, files of records or classes of records.

ARMA supports the concept of principles-based privacy and recordkeeping programs. ARMA believes that safeguarding and disposal requirements are incorporated, appropriately, in an organization's recordkeeping program. Treated in isolation, safeguarding, disposal or other attempts to address protection, are at risk of being less effective, less efficient, and easily marginalized in enterprises whose business models rely so intensely on information sharing and consumers' willingness to add their personally identifiable information to the records and files of Internet businesses. Privacy principles are incorporated in and enhanced by an enterprise-wide recordkeeping program, which speaks not only to privacy principles (protection of personal information), but also to senior management engagement, transparency, auditability, and appropriate life cycle management.

These principles create a foundation for an appropriate and effective recordkeeping program that speaks to enterprise-wide commitments and life cycle management of records and information – and their flexibility provide appropriate and effective application to protecting personal information associated with Internet commerce and in the possession and custody of Internet businesses. With these principles –

The enterprise would establish a recordkeeping program that 1) is overseen by a senior executive, 2) is informed by clear policies and procedures to train and guide personnel, 3) is auditable, and 4) is transparent through documentation in an understandable manner and available to all personnel and appropriate interested parties, including the appropriate regulatory and enforcement bodies.

The recordkeeping program would be constructed to ensure that 1) the records and information have a reasonable guarantee of authenticity and reliability, 2) there is an appropriate level of protection for records and information that are private, confidential, privileged, or in the case of this inquiry, personal information, 3) records and information are maintained to ensure timely, efficient, and accurate retrieval, 4) records and information are maintained for the appropriate or required period of time, and 5) disposition of records and information will be accomplished in an appropriate

manner and the appropriate or required time, and such disposition is documented.

Respectfully submitted,
**ARMA INTERNATIONAL**

**Before the**

**DEPARTMENT OF COMMERCE**
**National Telecommunications and Information Administration**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0175-01 |
| | ) | |
| | ) | RIN 0660-XA12 |
| | ) | |

# COMMENTS OF AT&T INC.


David A. Gross
Scott D. Delacourt
Amy E. Worlton
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000
*Counsel for AT&T Inc.*

Paul K. Mancini
Bruce R. Byrd
Theodore R. Kingsley
AT&T INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3862


June 14, 2010

## TABLE OF CONTENTS

**Before the**

**DEPARTMENT OF COMMERCE**
**National Telecommunications and Information Administration**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0175-01 |
| | ) | |
| | ) | RIN 0660-XA12 |
| | ) | |

**COMMENTS OF AT&T INC**.

AT&T Inc., on behalf of itself and its affiliates, hereby submits these comments in response to the Department of Commerce ("DOC") Notice of Inquiry ("NOI" or "Notice") entitled "Information Privacy and Innovation in the Internet Economy."[1] AT&T appreciates DOC's ongoing focus on Internet policy, and privacy in particular. To maintain the pace of innovation on the Internet, both the government and the private sector must continue to find ways to strengthen consumer trust online, which will, in turn, increase Internet usage and adoption both domestically and internationally. AT&T is committed to working with the Internet Policy Task Force and other stakeholders to develop policies and tools that both protect consumer privacy and nurture investment and innovation, consistent with DOC's objectives.

**INTRODUCTION**

DOC's Notice is timely and important. Changes in technology, services and business models have fundamentally expanded the scope and magnitude of online data being collected and used in a wide variety of contexts. Consumers increasingly utilize the Internet for everyday transactions – banking, shopping, accessing electronic health records, engaging in job training and education. And consumers are taking advantage of new innovative services, such as cloud

[1] 75 Fed. Reg. 21,226, Notice of Inquiry (Apr. 23, 2010) ("NOI").

computing social networking and location-based services, which generate entirely new categories of online information. In these contexts, consumers are choosing to share an unprecedented amount of personal information with trusted parties and each other. As opportunities for collection and use of consumer information will only increase, consumers must feel confident about the privacy and security of their data online.

Even where discrete user information may be anonymous on a stand-alone basis, a growing capability to accumulate and associate disparate data can be used to create a highly detailed, multi-dimensional view of an individual user that goes far beyond anything possible in the offline world. The explosion in both the amount and type of available information, and the potential to use that information in ways not apparent to consumers compels an equally multi-dimensional approach to privacy protection. Empowering individuals with up-to-date privacy tools to optimize their online experience is a cornerstone of that approach. Equally significant will be a change in thinking about individual privacy that must occur at all levels of the Internet ecosystem towards enabling users to meaningfully control how they present themselves in, interact with and experience their online environments.

Moreover, the Internet holds great promise as a platform for furthering important governmental objectives and delivering solutions for achieving the nation's health care, education and energy sustainability goals. For example, online services can increase transparency, accessibility, and civic engagement by enabling the delivery of government services and increasing the availability and accessibility of government information (both through easier access and reduced costs of making information available). In addition, online services will expand the availability of emerging solutions for healthcare IT and telemedicine, distance learning and modernization of the electric grid. These services raise the stakes for

consumers because of the amount of information that will be collected and shared online, as well as the sensitivity of the information. The full potential of these emerging services will only be realized if consumers trust that their privacy will be protected online.

AT&T agrees with DOC that a policy framework which protects consumer privacy and engenders consumer trust is the foundation for promoting continued innovation and the free flow of information on the Internet. The changing Internet marketplace requires a model of privacy protection that moves beyond notice and consent, and toward customer engagement and control. Indeed, as more and more of our personal and business lives are conducted electronically and online, consumers will be increasingly concerned about privacy issues and businesses must respond appropriately in order to achieve success in the marketplace.[2] Consistent with marketplace imperatives, privacy cannot be a "back-end" compliance consideration, but rather must be a foundational value under a "privacy-by-design" approach. For AT&T, such an approach means we are committed to integrating privacy as a feature into AT&T's product design and various business models, and building capabilities for our customers to understand how information is used and to exercise meaningful control over their privacy. And in order for consumers truly to be in control of their information, *all* entities involved in the Internet will need to adopt this consumer control approach to privacy protection. The DOC must ensure that any policy framework is fully inclusive of all entities in the data collection and use value-chain.

Equally important is the development of innovative approaches and tools that allow consumers to effectively manage their privacy and control their personal information as they

---

[2] *See, e.g.*, CMO Council, *Competitive Crunch and Convergence in the Commc'ns Marketplace Fueling Increased Customer Churn, Testing Loyalty* (Aug. 3, 2009)*, available at* http://www.marketwire.com/press-release/Competitive-Crunch-Convergence-Communications-Marketplace-Fueling-Increased-Customer-1213143.htm (last visited June 13, 2010) (discussing new challenges in customer retention in the communications industry).

navigate the Internet and the dizzying array of content and services that are available to them. As discussed further herein, AT&T and others in the industry have developed a variety of innovation solutions that can serve as a model for the next phase in the evolution of privacy practices. For example, last summer AT&T, through and open and inclusive process involving feedback from customers, adopted a new, simplified, plain language privacy policy that applies, with very limited exceptions, to all AT&T services. AT&T has also emphasized bringing privacy-enhancing technologies to consumers through its commitment to a "privacy-by-design" approach in the roll out of new products, including in the online advertising space. The Internet Policy Task Force should encourage and support such industry efforts to accelerate the paradigm shift toward deeper customer engagement in all aspects of the consumer Internet experience.

DOC and the Internet Policy Task Force have several key roles to play. First, they can foster the development of a national privacy framework that applies consistently to a wide variety of services and providers on the Internet. In performing this role, the Task Force should coordinate privacy-related activity across the Federal government and serve as a clearinghouse for ideas and innovative thinking regarding privacy issues. Second, both DOC and the Internet Policy Task Force should continue to promote and support private sector innovation in privacy protection and increasing consumer security as a means of furthering freedom of expression and the free flow of information. Third, they should provide leadership that helps to achieve national-level harmonization around consistent privacy standards and best practices while working to eliminate overly restrictive and inconsistent regulation that stifles innovation. Fourth, DOC is uniquely well-positioned to advance privacy standards and best practices internationally in an effort to promote greater global privacy harmonization and reduce barriers to commerce and innovation.

## I. PROMOTING THE TRUST ENVIRONMENT

AT&T proposes a national privacy policy framework that is fundamentally rooted in the consumer's interest in controlling the integrity, use and dissemination of her identity in the online world. In turn, this consumer control focus will strengthen the trust environment on the Internet, which will be essential to unlocking its potential social, economic and cultural benefits. Enabling user control over information as a means to building trust should guide further policy making by all actors in the Internet ecosystem, including both public and private sector entities.

### A. Consumer Control As The Foundation

As a matter of overarching policy, the privacy framework applicable to the online commercial ecosystem must start with a focus on consumer engagement and meaningful user control. AT&T has long held this position. In September 2008, for example, AT&T's Chief Privacy Officer, appearing in a hearing concerning online behavioral advertising, advocated a "consumer-focused" framework to the Senate Commerce Committee to "ensure[] that consumers have ultimate control over the use of their personal information."[3] The approach outlined by AT&T at that time, based on engaging consumers and offering them transparency and control over the use of their information, provides the critical foundation for promoting a trust framework.

Innovative approaches to engaging consumers through increased transparency and control tools that have begun to emerge in the marketplace can serve as a model for the next

[3] *Communications Networks and Consumer Privacy: Recent Developments Before the Subcomm. on Comm., Tech. and the Internet of the H. Comm. on Energy*, 111th Cong. (2009) (Written Statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T Inc. at pp. 1 and 5), *available at* http://energycommerce.house.gov/Press_111/20090423/testimony_attwood.pdf (last visited June 13, 2010); *see also* Comments of AT&T Inc., Federal Trade Commission Project No. P095416 (Nov. 6, 2009) *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00031.pdf (last visited June 13, 2010).

phase in the evolution of privacy practices. AT&T sees that model as shifting the current focus from merely notifying consumers of data collection towards facilitating practices that promote the creation of value for consumers. This model would focus on ensuring that data practices are fully transparent (as opposed to merely disclosed) and that customers are engaged and have the opportunity to control their privacy and the use of their personal information.

The means for effective consumer engagement must be designed as an integral attribute of the online experience, providing demonstrable value to the customer. For example, consumers will be better served if there is transparency and choice regarding the collection and use of their information at the time it is collected and used.[4] Consumers may decide to make their personal information available where they see the value of doing so and are confident about their ability to control its use. Moreover, Internet users clearly understand and accept that information will be collected in commercial relationships, and that the information will be used to offer goods and services that are of value to them. But as a general industry matter, consumers need more information about what data are collected, how personal information is used and shared, and how it is protected.

### B. The Importance of the Trust Environment

The Internet holds the promise of stimulating historic progress, not only in economic and technological development, but also in the health care and financial sectors, energy independence, education, social connectivity and cultural production, and other areas. This promise is inextricably linked to a foundation of user trust in both the public and private sector online entities with whom users interact as well as in the safety and security of the Internet itself.

[4] This does not mean that one privacy regime will be immediately supplanted by an entirely new one, as the use of straightforward and meaningful notice-and-consent systems can and will be appropriate in a variety of circumstances. However, more interactive forms of customer engagement must be part of the evolution of privacy practices.

Just as in the physical world, Internet users should have meaningful control over their transactional experiences. An online privacy paradigm that emphasizes user control will strengthen the foundational trust environment of the Internet.

Innovation on the Internet today depends on consumer participation and interaction. As a network, value is best created on the Internet through widespread use. Uninhibited use by consumers is the catalyst for social media, user-generated content, and the other exciting new developments in cultural production online. User confidence in the platform is essential to unlocking the potential of the platform for this cultural and economic growth and the other societal developments discussed above. This is because, in the words of Assistant Secretary of Commerce Lawrence Strickling, "[i]f users do not trust that their [personal information] is safe on the Internet, they won't use it."[5]

According to a study cited by the European Commission in its recently released Digital Agenda for Europe, among those Europeans who did not shop online in 2009, concerns about payment security and privacy were two of the most significant reasons why.[6] In the United States, accounts of Internet businesses misusing or not protecting from unauthorized disclosure consumers' personal information are nearly daily fare in the popular press,[7] and have shaken the

---

[5] *See* Lawrence E. Strickling, Assistant Secretary of Commerce for Commc'ns and Information, *The Internet: Evolving Responsibility for Preserving a First Amendment Miracle*, Remarks before the Media Institute (Feb. 24, 2010) *available at* http://www.ntia.doc.gov/presentations/2010/MediaInstitute_02242010.html (last visited June 13, 2010).

[6] European Comm'n *Digital Agenda for Europe* at p. 12, Fig. 3 (May 19, 2010), *available at* http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf (last visited June 13, 2010).

[7] *See* Alison Diana, *Google Wi-Fi Breach Spurs Calls for Investigation*, INFORMATIONWEEK (May 20, 2010), *available at* http://www.informationweek.com/news/infrastructure/WAN_optimization/showArticle.jhtml?articleID=224900497&subSection=Infrastructure (discussing Google's collection of payload data from unsecured home Wi-Fi networks) (last visited June 13, 2010); Emily Steel and Jessica E.

foundation of the trust environment. In order to prevent these sorts of violations, and to encourage consumer confidence in the Internet, AT&T urges the adoption of a new privacy framework by public and private parties alike across the Internet space.[8]

Among the benefits of a strengthened trust environment is that it supports the use of the Internet as a platform for free expression. As Secretary of State Hillary Clinton explained in recent remarks on Internet freedom, "the more freely information flows, the stronger societies become."[9] This strength derives from the fact that "access to information helps citizens hold their own governments accountable, generates new ideas, [and] encourages creativity and entrepreneurship."[10] Strengthening the trust environment through increased consumer involvement with and control over privacy is essential to the free flow of information and free expression and increases the value and vitality of the Internet as a whole.

### C. A New Privacy Framework Must Apply Consistently Across the Internet Ecosystem To Build an Effective Trust Environment.

For consumers truly to be in control of their information, *all* entities in the value chain, including advertisers, ad-supported products and services, ad networks, applications developers, search engines and ISPs, will need to adopt a focus on consumer engagement. Recent events have illustrated that privacy issues can arise anywhere in the value chain, particularly as online

---

Vascellaro, *Facebook, MySpace Confront Privacy Loophole*, WALL STREET JOUNRAL B1 (May 21, 2010) (discussing unauthorized distribution of user information to advertisers by Facebook, MySpace, and other social-networking sites).

[8] AT&T has also recently experienced a security breach with its iPad product. *See* Nick Bilton, "AT&T Explains iPad Security Breach" NYTIMES.COM - BITS BLOG, http://bits.blogs.nytimes.com/2010/06/13/att-explains-ipad-security-breach/ (June 13, 2010).

[9] Secretary of State Hillary Rodham Clinton, *Remarks on Internet Freedom*, The Newseum, Washington, D.C. (Jan. 21, 2010) *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm (Clinton Internet Freedom Remarks) (last visited June 13, 2010).

[10] *Id.*

services continue to evolve so rapidly. For example, both Google and Facebook are in the news lately for information collection and product design decisions that have attracted public scrutiny and eroded consumer confidence. In Google's case, the recent controversy involved its introduction of a social networking service integrated with its popular webmail platform that pre-populated and shared a contacts list semi-publicly, without clear consent from users.[11] For Facebook, concerns have been raised regarding potentially personally identifiable information transmitted without user consent to advertisers.[12] This approach of acting first and considering privacy impacts later has the effect of weakening consumer confidence in the online ecosystem and causing consumer frustration about the complexities of managing their privacy and personal information online.

Appropriate collection and use of personal information is essential to many of the developing social benefits of the Internet. For example, Internet-enabled health care services will rely upon access to accurate personal medical history details. However, to be effective in supporting the trust framework in a way that will give consumers sufficient confidence to allow the use of information in these ways, the consumer control approach to privacy must be ubiquitous. A regime that applies only to one set of actors will not protect consumers. As is illustrated in the examples above, frequently the entities pushing the envelope on the aggressive uses of data and customer information are the least regulated. In addition, an underinclusive privacy regime will arbitrarily favor one business model or technology over another by placing

---

[11] *See* Miguel Helft, *Critics Say Google Invades Privacy With New Service*, N.Y. TIMES, Feb. 13, 2010, at B1 *available at* http://www.nytimes.com/2010/02/13/technology/internet/13google.html (last visited June 13, 2010)

[12] *See* Steel and Vascellaro, *supra*, note 6.

all the costs of protecting consumers on certain sectors, while others are allowed to commercially exploit consumers' information without serious restriction.

## II. PROMOTING INNOVATION IN PRIVACY PROTECTION

The Federal government, and DOC specifically, should continue to champion policies in which privacy and innovation are mutually reinforcing. In many areas, U.S. policy to date has fostered the efficient deployment of new technologies while remaining neutral as to their specific design. This same approach should be used here to encourage the innovation in privacy-enhancing technologies that is already well underway by the private sector. As discussed in more detail below, DOC can work to encourage the development of identity management standards, promote the development of privacy control tools that consumers can understand and adopt, collaborate with stakeholders to develop best practices for privacy and security safeguards, and support positive international developments in this area. Additionally, DOC can encourage the Federal government to lead by example in this area by developing and implementing best practices in government Internet activities and employing consumer-centric privacy protections in its own offerings of online services.

### A. Privacy-Enhancing Technologies and Business Practices Currently In Development Will Improve Consumer Privacy.

The *Notice* requests information regarding ongoing efforts to develop privacy-enhancing technologies and specifically efforts towards increasing notice to consumers and anonymized browsing.[13] Further development of privacy-enhancing technologies and business practices should be encouraged to build the capability to give consumers information about how and what data is collected and used, and to track the sharing of personal data as it occurs. With improved tools, consumers will be better-positioned to make informed choices about protecting their own

[13] *See* NOI, 75 Fed. Reg. at 21,231.

privacy.

AT&T has already begun this transition in its own practices. Last year we developed and published an updated, consolidated and streamlined privacy policy that applies (with very limited exceptions) across all of AT&T's business units and services. Customer feedback helped shape this new policy, and contributed to our emphasis on a consumer-centric, plain-language presentation that clearly explains to users what data we collect, how we collect it, and how we use it. Our rollout included video explanations of our policy highlights, as well as a 45-day preview period for customer feedback. Based on that customer feedback, we made additional changes to the policy – including adding definitions and specifically confirming that we do not sell, give or "rent" personal information to marketing companies – before posting the final version.[14]

AT&T has also emphasized bringing privacy-enhancing technologies to consumers For example, in connection with targeted advertising with data from yellowpages.com ,we offer customers the ability to view and edit the interest categories that we have associated with them and a simple process for them to choose not to be targeted in this way. We believe these new capabilities not only represent best practice in this area, but also are a step towards an ecosystem-wide approach based on customer engagement.

Several technologies identified in the *Notice* would improve transparency and give consumers greater control over personal data. For example, anonymized browsing helps prevent

[14] The principles that underlie this updated policy include: We will protect your privacy and keep your personal information safe; we will not sell your personal information to anyone, for any purpose; we will fully disclose our privacy policy in plain language, and make our policy easily accessible to you; we will notify you of revisions to our privacy policy, in advance; you have choices about how AT&T uses your information for marketing purposes. *See* AT&T Privacy Policy, *available at* http://www.att.com/gen/privacy-policy?pid=2506 (last visited June 13, 2010).

the hidden or unknown collection of a user's data through data collection mechanisms, such as cookies. In addition, consumer-centric identity management systems like those recommended by the Federal Communications Commission[15] ("FCC") could include the ability to allow users to build virtual profiles that support their information sharing choices online across various websites, applications, and platforms. Using these systems, consumers could actively manage how they will exchange personal information in pre-determined ways. Improved and ubiquitous identity management solutions could help individuals and organizations form trusted communities based on varying degrees of identity exposure. Through a virtual profile, a user could have the option of identifying the level of information he or she wishes to share with different communities, including trusted businesses, friends, or even no one. Such systems could also allow users to establish notifications that alert them before certain information is shared and to track generally when and with whom their personal data is shared.

### B. The Federal Government, and the Department of Commerce Specifically, Have an Important Role in Promoting the Successful Development of Privacy-Enhancing Technologies.

By working with stakeholders, including a broad range of industry participants, the U.S. government, and DOC specifically, can play an important role in encouraging the development of privacy-enhancing technologies. Existing government research efforts, such as the White House's National Strategy for Secure Online Transactions have begun to support efforts to develop innovative new technologies. Building from existing efforts, the Federal government should develop policies that will create incentives for Internet innovators to build out the "identity layer" of the Internet ecosystem in a way that secures transactions and protects consumer privacy, while still supporting business growth and economic development.

---

[15] *See* NOI, 75 Fed. Reg. at 21,231.

Towards this end, the Federal government should:

*First*, play a role in the development of best practices for privacy and security protections. Through collaboration across a wide range of stakeholders, the government could identify best practices that allow for secure transactions and protect consumer privacy. For example, areas that need further collaboration are the development of best practices for anonymizing data, minimizing data collection, and limiting data retention periods. As the *Notice* recognizes, recent research has shown that data re-identification may be possible even after such data has been anonymized.[16] The government could specifically work to encourage best practices where they are inadequate to reduce the risks of data re-identification, including practices related to both data minimization and retention periods.

Some self-regulatory frameworks for meaningful privacy protection are already in place, helping to earn consumers' trust in the wireless Internet and cloud computing. AT&T voluntarily adopted strong protections for subscriber location information,[17] and in working with our enterprise customers, we use "privacy by design" in providing cloud computing services. In the wireless industry, CTIA has developed Best Practices and Guidelines for Location-Based Services in order to set benchmarks for the mobile Internet ecosystem in a technology-neutral way.[18] These best practices and guidelines are responsive to individuals' and policymakers' heightened privacy interests in location data while eschewing any particular format requirement, default setting or other rigidity that could hamper innovation. In another example, the Mobile Marketing Association likewise adopted a Global Code of Conduct calling for advertisers to

---

16 *See* NOI, 75 Fed. Reg. at 21,230.

17 *See* AT&T Privacy Policy, *available at* www.att.com/gen/privacy-policy?pid=13692#location (Questions about Location Information).

18 *See* CTIA, *Best Practices and Guidelines for Location Based Services* (2010) *available at* http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf .

obtain explicit opt-in from individuals for mobile marketing programs.[19]

*Second*, the U.S. government could also support the development of identity management systems and industry privacy control tools through establishing broad goals for these technologies. Although some tools and controls are available today, adoption by both consumers and Internet entities has been low due to the complexity of the ecosystem, lack of knowledge and difficulty of use. In addition, identity management has historically focused on traditional identity theft issues. Therefore, to aid the successful implementation of innovative privacy tools, the government should work with the private sector to promote the expansion of the field to address additional privacy concerns and the development of user-friendly tools and interfaces and to increase education of both consumers and the Internet industry. In this process, DOC's National Institute of Standards and Technology could also bring its technical expertise to bear in promoting development of industry standards should that prove to be necessary to encourage the successful deployment of privacy-enhancing technologies.

*Third*, the U.S. government should also continue its support for positive international developments in this area. For example, as discussed further below, the Asia-Pacific Economic Cooperation Privacy Framework ("APEC Framework")[20] promotes a consistent global approach to privacy protection to avoid the creation of unnecessary barriers to information flows and to remove impediments to trade. In addressing international issues, an important objective is giving providers technical and operational flexibility so that services can be designed to meet the needs of customers, rather than overly restrictive legal and regulatory requirements.

---

[19] *See* Mobile Marketing Association, *Global Code of Conduct* (2008) *available at* http://www.mmaglobal.com/codeofconduct.pdf.

[20] *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005) *available at* http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

## III. DISPARATE LEGAL REGIMES REQUIRE HARMONIZATION AND CONSUMER-CENTRIC APPROACHES TO PRIVACY

A strong framework for nourishing privacy and innovation will not exist in a vacuum. It will have to take hold in the midst of many legal and business complexities. In AT&T's view, holding consumer privacy interests paramount and adopting privacy by design will help to simplify this landscape. In addition, harmonization would be helpful to foster clear, predicable rules that are consistent among state and federal regimes and across industry sectors and technologies.

*A Clear Legal Foundation for Internet Innovations*: Innovation interests are compelling with respect to many dynamic new technologies that hold great prospects for growth, such as location-driven applications for wireless devices and cloud computing. Privacy interests are also at their most keen with respect to these offerings, due to the ubiquity of mobile devices, the growing prominence of cloud computing, and the fact that these technologies are driven by location data and remote data processing, respectively. Although privacy and innovation are well-served through self-regulatory mechanisms, private actors sometimes face difficult legal uncertainty with respect to many dynamic new technologies. Location data, now available through several different technologies, and data associated with cloud computing are no exception.[21] Harmonization and clarification of divergent legal rules would help service

[21] *See e.g.*, Elec. Commc'ns Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, *codified at* 18 U.S.C. § 2510 *et seq.*; Commc'ns Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, *codified at* 47 U.S.C. §§ 1001-1010; 47 U.S.C. § 222; *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747 (S.D. Tex. 2005); *In re Application Of The United States Of America For An Order Directing A Provider Of Elec. Commc'n Serv. To Disclose Records To The Government*, 534 F.Supp.2d 585, 589 (W.D. Pa. 2008); *In the Matter of the Application of the United States of America for an Order Directing the Provider of Elec. Commc'ns Serv. to Disclose Records to the Government*, 534 F.Supp.2d 585 (W.D. Pa. 2008), *aff'd by and objection denied by* 2008 U.S. Dist. LEXIS 98761 (W.D. Pa. Sept. 10, 2008) (currently on appeal to the Third Circuit, Case 08-4227); *see also* 18 U.S.C. §§ 2701-2712; *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003); *Theofel v. Farey Jones*, 359 F.3d 1066 (9th Cir. 2004).

providers understand their rights and responsibilities, and would give individuals confidence about the protections due to their data.

*Government Action to Protect Privacy.* The U.S. government can lead by example and ensure that individuals have meaningful control over their personal information. Many government agencies offer online services to the public, such as the ability to submit tax payments and apply for and renew a variety of government-issued licenses. As a provider of online services, the federal government should adopt "privacy by design" and security safeguards as appropriate.

AT&T is participating in multiple efforts to encourage policymakers to clarify and update the rules concerning government access to online information, such as location information and data stored "in the cloud." For example, we are a member of the Digital Due Process coalition working to encourage the inclusive stakeholder dialogue necessary to establish uniform protections for communications data while preserving the legal tools needed by law enforcement.[22]

*Balance of Interests in Security, Breach Notification and Data Encryption.* Forty-six states, the District of Colombia, Puerto Rico and the Virgin Islands have adopted laws requiring notice in case of a breach in the security of their personal information.[23] AT&T strongly supports the principal of notice in such cases, which is a part of the company's privacy policy.[24] Yet, companies acting in good faith can be bogged down by broad-brush encryption

---

[22] *See* Digital Due Process, *available at* www.digitaldueprocess.org (last visited June 13, 2010.

[23] *See, e.g.*, Cal. Civ. Code § 1798.82; 815 Ill. Comp. Stat. Ann. 530/5 *et seq.*; N.Y. Gen. Bus. Law § 899-aa.

[24] *See* AT&T Privacy Policy, *available at* http://www.att.com/gen/privacy-policy?pid=13692#protection (Question 4 about Data Security and Protection) (last visited June 13, 2010).

requirements, disparate notice specifications and inconsistencies in the data whose breach can trigger a notice.[25] The robust privacy framework sought by AT&T could go far in resolving these tensions. In addition, the Internet Policy Task Force should lend its support to the creation of a information security "Safe Harbor." No company can completely eliminate the risk of breach, but, a set of security safeguards should be developed that, if met and maintained in good faith, should meet the policy goals.

AT&T supports the need for ongoing U.S. government support for the so-called "Good Samaritan provisions" of the Communications Act, Section 230.[26] The statute strikes the right balance, allowing service providers to police their websites without fear that immunity will be lost, thereby creating incentives for stronger privacy protections.

## IV. CONTINUING ACTIVE ENGAGEMENT ON INTERNATIONAL PRIVACY ISSUES

U.S. leadership is essential to advancing the development of a strong privacy framework on an international basis that will facilitate transborder data flows and the growth of the global Internet. Dramatic decreases in transport costs and increased connectivity arising from the Internet create an enormous opportunity for cloud computing and other service platforms that can overcome geography and distance limitations. These advances mean that privacy concerns are global and, in the international policy arena, of paramount importance. The U.S. government is a critical partner in helping to shape international dialogues, support U.S. competitiveness and advocate on behalf of the free flow of information.

A consumer-centric approach to privacy will help to promote innovation in the United

---

[25] *See, e.g.,* 201 Mass. Code Regs. §17.03(1); Nev. Rev. Stat. §§ 205.4742; Iowa Statutes, Section 715C.1 et seq.; Utah Code Ann. §§ 13-44-101, *et seq.*

[26] 47 U.S.C. § 230(c).

States, and further, will advance these same interests on a global basis. It should appeal to foreign authorities, as it delivers substantive privacy protection and provides a basis for accountability and enforcement. In the case of cloud computing, for example, reasonable and clear protections in the United States for stored information will help reassure foreign governments wary of data collection and storage outside their borders. Simultaneously, the approach provides value to industry, avoiding prescriptive, one-size-fits-all rules in favor of flexible privacy principles that can be adapted to a particular industry. The framework insists on technological neutrality and advances the goal of harmonization. AT&T encourages a shared understanding of privacy values, in part, to establish a solid foundation for the U.S. government and U.S. industry to advocate successfully abroad for a balance of privacy and innovation interests.

Data protection policy is increasingly under discussion in foreign and international bodies. To shape these dialogues, coordinated action by the Commerce Department, the State Department, the U.S. Trade Representative, the Federal Communications Commission, the Federal Trade Commission and other relevant agencies will be critical. The following is but a short list of multinational venues where continued U.S. leadership is needed:

- As discussed above, AT&T believes that the APEC Framework[27] holds great promise as a set of broadly-applicable privacy standards that can be adapted to particular jurisdictions and industries, while enjoying mutual recognition by participating economies. We appreciate the efforts of the Office of Technology and Electronic Commerce within the Commerce Department and the Federal Trade Commission in developing the Framework. The U.S. government should continue to actively support

[27] *See* APEC, *supra* note 20.

the Framework's development and implementation, which could yield greater information flows and trade.

- The Organisation for Economic Co-operation and Development ("OECD") is celebrating the 30th Anniversary of its influential Privacy Guidelines by examining their impact and studying how they should be updated to better facilitate trans-border data flows.[28] The U.S. government should engage in this process in order to ensure that revised Guidelines reflect the Administration's view that privacy should promote free flows of information.
- The European Commission is considering whether the 15-year-old EU Data Protection Directive should be updated.[29] The lack of an efficient format for mutual recognition between EU Member States continues to be a major hurdle for international business, and the U.S. government should support the European Commission in its push for harmonization. Moreover, because the EU Directive continues to exert a strong influence on global privacy standards, coordinated U.S. action is necessary to promote models conducive to cross border data flows and responsive to real-world privacy risks and business practices.

---

[28] *See, e.g.,* OECD, "30 Years After: The Impact of the OECD Privacy Guidelines," *available at* http://www.oecd.org/document/39/0,3343,en_2649_34255_44946983_1_1_1_1,00.html (last visited June 13, 2010).

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 95/46/EC (E.U. 1995) *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited June 13, 2010); s*ee, e.g.,* European Commission, Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data, *available at* http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm (asking for public comment on whether the current legal framework meets new challenges for personal data protection) (last visited June 13, 2010).

- The recently agreed Framework for Cooperation on Trade and Investment establishes an ongoing dialogue between the United States and India to strengthen bilateral economic cooperation.[30] The U.S. Trade Representative and other U.S. government actors should seize the opportunity in upcoming meetings to promote a clear, harmonized privacy framework that preserves business flexibility while conferring consumer-oriented privacy protections on outsourced data.

In working closely with industry, the U.S. government has a track record of substantial success in facilitating trans-border trade. As an example, the U.S.-EU Safe Harbor program, negotiated by the Department of Commerce in the late 1990s, preserved the free flow of personal data from the EU for eligible companies, provided means for participating U.S. companies to meet EU data protection adequacy requirements, and enshrined the principle of self-regulation, backed-up by government enforcement where necessary.[31] AT&T is committed to working in partnership with the U.S. government to foster this type of international environment.[32]

*Freedom of Information*. AT&T commends the U.S. government for speaking out in support of free data flows.[33] We believe that Internet innovation rests on information exchanges and that strong privacy protections and user controls ultimately promote these exchanges. We

---

30 Press Release, Office of the United States Trade Representative, United States and India Sign Framework for Cooperation on Trade and Investment (Mar. 17, 2010) *available at* http://www.ustr.gov/about-us/press-office/press-releases/2010/march/united-states-and-india-sign-framework-cooperation-t.

31 *See* Dept. of Commerce, Issuance of Safe Harbor Principles and Transmission to European Commission, Notice, 65 Fed. Reg. 45,666 (July 24, 2000).

32 To be clear, the common carrier components of AT&T are ineligible to participate in the U.S.-EU Safe Harbor because they are exempt from the enforcement jurisdiction of the Federal Trade Commission. *See* 15 U.S.C. § 45(a)(2). Nonetheless, AT&T believes that the Safe Harbor exemplifies how U.S. government involvement can help harmonize disparate data protection regulatory regimes.

33 *See, e.g.*, Secretary Clinton Remarks on Internet Freedom, *supra*, note 8.

support efforts of the U.S. government to focus on fostering respect among the international community for privacy, freedom of information and freedom of expression.[34]

*Free Trade and Innovation*. Although AT&T primarily offers enterprise solutions rather than consumer offerings abroad, all U.S. companies are potentially susceptible to privacy enforcement actions motivated by protectionism. Local data storage requirements can also be barriers to trade. We have seen some foreign governments attempt to create national technical standards for the Internet; these efforts generally should be discouraged in favor of international standards that promote competitiveness and universality. In general, the Commerce Department, the U.S. Trade Representative, the State Department and the Federal Communications Commission should, in various international circles, push open doors for U.S. business and for further Internet innovations.

*Privacy by Design.* We believe the "privacy-by-design" model of integrating personal data controls into new technologies and business processes can be effective internationally. The role of the U.S. government should be to advocate on behalf of clarity and flexibility, to ensure that "privacy-by-design" initiatives neither mandate nor prohibit any particular feature or system configuration, which could hamper innovation.

[34] *See, e.g.,* Tunis Agenda For the Information Society, World Summit on the Information Society, WSIS-05/TUNIS/DOC/6(Rev.1-E) ¶ 42 (2005), *available at* http://www.itu.int/wsis/docs2/tunis/off/6rev1.html ("We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.") (last visited June 13, 2010).

## V. CONCLUSION

To maintain the pace of Internet innovation, the Administration must continue to find ways to strengthen consumer trust online. AT&T urges DOC to move forward in advancing a consumer-centric privacy framework, as articulated herein.

Respectfully submitted,

*/s/ Bruce R. Byrd*

David A. Gross
Scott D. Delacourt
Amy E. Worlton
WILEY REIN LLP
1776 K Street, N.W.
Washington, D.C. 20006
(202) 719-7000
*Counsel for AT&T Inc.*

Paul K. Mancini
Bruce R. Byrd
Theodore R. Kingsley
AT&T INC.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-3862

June 14, 2010

Comments of B Roffman:

Bluetooth needs to be secured before it compromises someone's privacy.

People might enjoy having the E911 system call their cell phones when the weather alert warning sirens sound.

**THE BUSINESS FORUM FOR CONSUMER PRIVACY**

June 9, 2010

National Telecommunications and Information Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, DC 20230

Dear Sirs and Madams,

The Business Forum for Consumer Privacy ("the Forum") appreciates this opportunity to respond to the Department of Commerce's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy." The Forum is an organization of companies whose mission is to examine issues related to the next generation of privacy governance in the United States and to propose thoughtful, workable solutions for consideration by experts, businesses and policymakers.[1]

The Forum focuses its response on Question 1 of the Notice of Inquiry. Question 1 references specifically the use-and-obligations model:

> *Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use. Describe how a use-based privacy system would work. How should policymakers determine what constitutes harmful uses of personal information in this model? Are there examples from existing privacy laws and regulations that suggest strengths and weaknesses of the use-based model? Is this "use-based" model for commercial data privacy a workable approach for companies and consumers? What is the relationship between use-based privacy rules and proposed accountability systems?*

As the primary developers of the use-and-obligations model, the Forum will respond to this question by making four points:

1. The nature, speed and volume of data collection, processing and analysis stress legacy models of privacy governance based on traditional models of notice and choice.

---

[1] The Business Forum for Consumer Privacy is an independent project of the Centre for Information Policy Leadership. A list of companies that participate in the Forum's work is attached as Appendix A. Questions related to these comments should be submitted to Martin Abrams at mabrams@hunton.com or to Paula Bruening at pbruening@hunton.com.

2. Obligations related to the way in which data is to be protected and managed must now depend, in many instances, upon the purpose for which the data is to be used.

3. The use-and-obligations model must be adopted and implemented in tandem with an accountability approach to data protection.

1. The nature, speed and volume of data collection, processing and analysis stress legacy models of privacy governance based on traditional models of notice and choice.

Question one of the Notice of Inquiry asks "does the existing privacy framework provide sufficient guidance to the private sector?" The Forum's response is "no."

In February 2010, *The Economist* published a report describing how the revolution in computing and communications technology is changing business processes.[2] The article highlighted the explosion in usable information and the potential it offers if harnessed and used. Coining the term "big data," the report explained the phenomenon of continuous collection, application and reapplication of information. It noted the capacity of big data to both promote innovation and raise significant privacy concerns.

Legacy privacy governance systems date to the early 1970s when single-application mainframe systems were the norm and data resided on punch cards. Governance was designed to facilitate the ability of individuals to control the flow of data about themselves, and relied upon notice of data collection, use and sharing, and individual choice based on that notice at the point of data collection. Organizations are obligated to use and protect data based on that choice.

Today data is collected through keystroke monitoring and by observing how long a mouse hovers over an image. Information is gathered through geo-location devices and sensor-based technologies. Data is collated and analyzed in real time to facilitate targeted advertising and optimize the online experience. Information may be processed in the facility near corporate headquarters, or in a data warehouse halfway around the globe. In the age of big data, the complexity of data collected and used and the time necessary for consumers to make informed decisions based on notices test the current model of governance.

---

[2] "Data, data everywhere: A special report on managing information," *The Economist*, February 27, 2010.

2. Obligations related to the way in which data is to be used and protected must now depend, in most instances, upon the purpose for which data is to be used. The use-and-obligations model provides such an approach.

When the Forum began its exploration of new approaches to privacy governance, it assumed traditional notions about data: that it is or is not sensitive; that it is personally identifiable or it is not; and that uses of data fall into two categories — primary and secondary. In testing governance approaches based on these assumptions, it quickly became clear that in the current environment of data collection, analysis, storage and processing, these commonly accepted distinctions did not facilitate effective protection. The Forum looked instead to a model that turns on distinctions about the *use* of the data, rather than about the data itself.

The use-and-obligations model, explained in depth in the Forum's release " A Use-and-Obligations Approach to Protecting Privacy: A Discussion Document,"[3] has the following characteristics:

- The use-and-obligations model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment and management of the relationship with the consumer; 2) internal business operations; 3) marketing; 4) fraud prevention and authentication; and 5) external, national security and legal processes.[4]

- The use-and-obligations model does not attempt to preclude principles of fair information practices, nor to take the place of applicable law.[5] Rather, it proposes a method to implement those principles in a way that reflects current technology, business processes and data use.

- The use-and-obligations model recognizes two aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organizations must

---

[3] Released December 7, 2009, attached as Appendix B, and found at http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf (last visited June 3, 2010).

[4] While the Forum identified these five categories, there may be more. The obligations related to additional categories of use, once identified, must be tested and vetted.

[5] In particular, laws and self-regulatory codes should continue to protect individuals from the deceptive and fraudulent collection of information. Possession of data should continue to trigger security requirements. The use-and-obligations model depends on these regulatory protections.

take to facilitate individual participation: transparency (notice), choice[6], and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and appropriate; and can access and correct it in appropriate circumstances. The second aspect includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual: collection limitation and data use minimization; data quality and integrity; data retention; security; and accountability.

- The use-and-obligations model encourages trusted data protection by requiring that the obligations that attach to data — whether from law, industry guidance or the organization's promises — should remain with the data and be met wherever or by whomever it is processed.

3. The use-and-obligations model should be adopted and implemented in tandem with an accountability approach to data protection.

In an environment of rapid data sharing, business process outsourcing and use of vendors to provide services, a use-and-obligations model can work effectively only if the obligations that arise with respect to the use of data are honored no matter where the data is transferred, stored or processed. Therefore, for the use-and-obligations model to succeed, all organizations that use data must be accountable — they must be able to demonstrate their ability to honor the obligations that come with the data, and to understand and mitigate risks to individuals raised by the data's sharing and use.

Accountability is a well-established principle of data protection, found in known guidance such as the OECD Guidelines; in the laws of the European Union, the EU member states, Canada and the United States; and in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. Recently, participants in an international working group facilitated by the Centre for Information Policy Leadership[7] defined in specific terms what it means for organizations to be accountable.

---

[6] The use-and-obligations model enhances the fair information practice of transparency, by requiring transparency and choice based on the nature of the data use. Organizations would be required to provide "just-in-time" notice when the individual would not expect the data use.

[7] Participants in the work included representatives of privacy enforcement agencies, governments, civil society and the private sector. The results of the first year's meetings in Ireland are found in "Data Protection Accountability: The Essential Elements," October 2009, attached as Appendix C, and found at http://www.huntonfiles.com/files/ebupload/CIPL_Galway_Accountability_Paper.pdf (last visited June 3, 2010).

The essential elements of accountability are:

1. Organization commitment to accountability and adoption of internal policies consistent with external criteria.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

3. Systems for internal, ongoing oversight and assurance reviews, and external verification.

4. Transparency and mechanisms for individual participation.

5. Means for remediation and external enforcement.

Accountability provides an infrastructure for the use-and-obligations model that encourages organizations to engage in the risk assessment and mitigation necessary to meet obligations appropriately. It also creates a culture of privacy such that companies transferring data for processing and those receiving it do so with an understanding of what will be required to use data responsibly.

Conclusion

The Forum does not view the use-and-obligations model as a legislative framework, but rather offers it as an example of a governance approach that is workable in the current digital economy. The Forum has tested the model across various industry sectors, technologies and data applications, and has found it to consistently offer practical guidance. The model is adaptable where there is omnibus privacy law, and where industry sectors (*e.g.*, health care and finance) impose specific requirements.

The Forum is encouraged by the Department of Commerce's return to its traditional leadership role in encouraging privacy and innovation in the digital economy. We believe that the use-and-obligations model has promise, but acknowledge the significant additional work that must be carried out before it might be proposed as part of a governance package. We look forward to working with the Department of Commerce as it continues to explore this approach.

Yours sincerely,

/s/

The Business Forum for Consumer Privacy

# APPENDIX A

**THE BUSINESS FORUM FOR CONSUMER PRIVACY**

## List of Member Companies

AT&T
eBay, Inc.
Google
Hewlett-Packard
Intel
Intuit
Microsoft
Oracle
Procter & Gamble
Wal-Mart

# APPENDIX B

# A USE AND OBLIGATIONS APPROACH TO PROTECTING PRIVACY: A DISCUSSION DOCUMENT

The Business Forum for Consumer Privacy

December 7, 2009

## Introduction

This paper proposes a framework for implementation and interpretation of traditional principles of fair information practices that reflects and serves the way data is used and managed in the 21st century.

Principles of fair information practices continue to form the foundation for effective, reliable privacy and data management and protection. They provide for transparency around the collection and use of data; engagement of the individual in decisions about how data pertaining to them may be used; data security; and protections to ensure that decisions about the consumer are based on data of appropriate quality. While principles of fair information practices remain relevant to sound data protection today, our traditional way of applying those principles may not effectively provide consumers with adequate protection.

First articulated in 1973,[1] fair information practices were developed to establish ways in which individuals might exercise control over personal information. The principles provide that individuals are given notice about how their data will be used. Based on that notice, individuals either consent to or prohibit its use. Organizations specify the purposes for which data is collected and limit collection to the data that is needed. In appropriate circumstances, individuals are granted access to data pertaining to them. Organizations are required to secure the data they collect to ensure its integrity and availability, and are held accountable for the manner in which their data management reflects principles of fair information practices.

The principles are widely endorsed and adopted. They form the basis of recognized guidance promulgated by the Organization for Economic Cooperation and Development, Asia Pacific Economic Cooperation, and the United States Federal Trade Commission. They are reflected in the European Union Privacy Directive, federal and state/provincial laws in many countries, self-regulatory regimes, and industry codes of conduct. Principles of fair information practices serve as the starting point for privacy protection around the world.

These practices continue to serve the privacy interests of individuals and the needs of business. They have proven dynamic enough to address privacy through a period of rapid and dramatic evolution in data use and technology innovation. But the realities of a data-fueled economy require a re-examination of how to implement the principles in a way that most effectively serves the consumer.

As currently implemented, fair information practices enable the consumer to read a privacy notice and make choices, to the extent they are available, based on what he understands of that notice. The collecting organization promises not to use data in a manner that is not consistent with the consumer's choice.

But today, online and in public life, individuals, organizations and data analytics generate ever-growing amounts of data that fuel existing and emerging business processes. Wireless and mobile communications offer new points of data collection and provide new kinds of data. Open networks and the evolution of the Internet as a commercial medium and as a platform for connected services enable ubiquitous collection and global flow of data. Data about an individual can be easily copied and aggregated across vast, interconnected networks. That data, enhanced by analytics, yields insights and inferences about individuals based on data maintained in multiple databases scattered around the world. Asking the individual to assume responsibility for policing the use of data in this environment is no longer reasonable, nor does it provide a sufficient check against inappropriate and irresponsible data use in the marketplace.

In this paper, the Business Forum for Consumer Privacy[2] (BFCP) proposes a *Use-and-Obligations* model — a framework for implementation and interpretation of traditional principles of fair information practices in a manner that reflects and serves

1 "Records, Computers and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health Education and Welfare, 1973.

2 The Business Forum for Consumer Privacy (BFCP) sponsors this paper. The BFCP has taken up the work of the Consumer Privacy Legislative Forum to explore new privacy governance frameworks. The consensus of the BFCP is that the United States' current, often conflicting, mix of sector specific laws at both the federal and state level creates inefficiencies for businesses and often denies appropriate protections for consumers. The BFCP is dedicated to creating new frameworks that will be the basis for privacy governance as reflected in company best practices, industry codes and workable new or revised laws where necessary with a principle focus on the US marketplace.

the way data is used and managed in the 21st century. While the collection of data and consumer consent to — or choice about — its use traditionally have triggered an organization's obligations to protect data, this paper proposes an approach in which *the way an organization **uses** data determines the steps it is **obligated** to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use.*

This proposed Use-and-Obligations model in no way attempts to preclude principles of fair information practices, nor to take the place of applicable law. Rather, it proposes a practical, contemporary means to implement those principles, in the context of business processes and data uses enabled by 21st century technology, and supplements them with additional protections.

## Overview of the Use-and-Obligations Approach

The Use-and-Obligations model establishes the use rather than the collection of data as the primary driver of a data collector's obligations related to notice, choice, and access and correction. Under current implementation of fair information practices, consumer choice or consent to use data in certain ways establishes a company's responsibilities. A Use-and-Obligations model shifts responsibility for disciplined data use to the data collector and all holders (e.g. third party vendors) of data, imposing requirements for transparency and notice, consumer choice, and access and correction on the data collector based upon the way the data is to be used.

The model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment, 2) internal business operations, 3) marketing, 4) fraud prevention and authentication, and 5) external, national security and legal.[3]

The Use-and-Obligations model recognizes two aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organizations must take to facilitate individual participation — transparency (notice), choice, and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and appropriate; and can access and correct it in appropriate circumstances. The second aspect includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual — collection limitation and data use minimization; data quality and integrity; data retention; security; and accountability. The uses and obligations are discussed below.

## Categories of Use

***Fulfillment.*** Fulfillment includes the activities necessary to establish and maintain the relationship between the organization and the consumer. It includes activities related to the purchase, payment for, and delivery of a product or service. Fulfillment also involves ongoing customer service and support. Fulfillment triggers data uses that are normally expected or explicitly consented to by the consumer. It requires high-quality data, because the decisions based on that data can have significant consequences.

***Internal Business Processes.*** Internal business processes include activities necessary to operate a business, such as accounting; audit and compliance; staff scheduling; management of information technology infrastructure; and product and service development, improvement, and testing. All require data related to customers, but processing primarily involves the internal functioning of the business.

3 While the BFCP has identified these five categories, there may be more. The obligations related to those additional categories of use, once identified, must be tested and vetted.

***Marketing.*** Marketing includes activity related to making offers to existing customers and personalizing products or services at their request, targeting individuals as potential customers, developing a strategy to reach those customers, determining the prices and terms to be offered, and selling or upgrading products and services.

***Fraud Prevention and Authentication.*** Organizations use personal information to prevent fraud, identify individuals, authenticate that they are who they say they are, verify that they may act in certain ways (e.g., to access their data or to engage in an online activity, such as banking or account management), and establish their eligibility for benefits or services. Some of the data necessary to perform these functions may come directly from the individual and some may come from third-party services, such as credit reporting agencies.

***National Security and Legal.*** Government and law enforcement agencies may approach organizations with a subpoena or court order to obtain data pertaining to an individual. U.S. courts may grant fairly broad discovery rights to parties in legal proceedings. These uses are often beyond the control of the organization that collect or store the data.[4]

## Categories of Obligations

The obligations incurred by organizations fall into two categories: those that facilitate the individual's participation and those that involve an organization's internal activities to assess and mitigate risks to individuals raised by data collection and use.

### I. Facilitating Individual Participation

***Transparency/Notice.*** Transparency involves notifying the individual about the collection and use of data. The posted notice of a company's privacy policy is the foundation of transparency. The Use-and-Obligations model references two kinds of notice to ensure transparency — *discoverable notice* and *just-in-time notice.*

Discoverable notice is a posted notice of an organization's privacy policy that can be easily located and accessed by the consumer. Discoverable notice may take the form of, for example, the notices required by the Gramm-Leach-Bliley Act and sent to consumers by U.S. mail, notices posted on a website, notices made available in a health care provider's office according to the provisions of the Health Information Portability and Accountability Act, and notices made available on paper at a point of purchase in a retail establishment.

For purposes of this analysis, just-in-time notice generally is provided when uses of data likely are not to be expected by the individual.[5] It generally appears or is made available at the point where a consumer is required to make a decision about entering into a transaction or about the use or sharing of data for a specific purpose or set of purposes.

***Choice.*** In some cases, individuals may have a choice about the use of their data. That choice may be offered as an opt-in (the individual affirmatively requests that data be used in a certain way) or as an opt-out (the data collector assumes that data can be used in a certain way unless the individual indicates otherwise; the individual is offered a clearly conspicuous, easily accessible way to decline the use of his data). In some cases, the individual practically may not be able to exercise choice. For example, in order to have merchandise sent to his home, the individual must allow that his data be used for shipping. In other cases, such as direct postal marketing, the consumer may have a choice.

***Access and Correction.*** Access and correction serve two purposes. First, they facilitate transparency and individual participation by informing individuals about what kind of data about them an organization maintains and stores. Second, they promote the accuracy and quality of data and the suitability for a specific purpose.

4 Organizations that collect and process data in general take national security and legal requirements seriously and take steps to respond to them appropriately. However, an organization's inability to ensure that obligations related to data are respected once that data is shared with government may compromise the effectiveness of the Use-and-Obligations model. The BFCP believes that issues related to the accountable use of data by government should be publicly discussed and addressed. They are not, however, the subject of this paper.

5 Questions related to when and how practically to provide effective just-in-time notice remain the subject of discussion, and are beyond the scope of this paper.

The Use-and Obligations model provides for two kinds of access. To facilitate transparency, it provides for what is referred to as *generalized* access. Generalized access involves providing the individual with the categories of data the organization holds about the individual (or type of individual), but does not require the organization to provide the consumer with the data itself.

To ensure the accuracy, usability, and sufficient quality of the data, the Use-and-Obligations model also provides for access to the specific data maintained about the individual, and an opportunity to challenge and, where appropriate, to correct the data.

### II. Internal Assessment and Mitigation of Risk

***Collection Limitation.*** Collection limitation requires that organizations only collect data for which it has a use or purpose. In general, organizations typically identify three uses — prevention of fraud, fulfillment, and marketing. Collection limitation mitigates the risk of data breach, as the more data an organization holds, the greater the potential risks to the individuals and the more effort the organization must undertake to protect it. Collection limitation can prompt an organization to manage risk through more strategic and thoughtful plans for data collection and use.

***Data Use Minimization.*** While not explicitly stated in traditional expressions of fair information practices, data use minimization is included in this discussion because it functions as an adjunct to collection limitation, and reflects the orientation and application of fair information practices toward use, rather than collection, of data. Data use minimization, along with collection limitation, requires that organizations determine what data should be used to provide for the optimal function of a business process, product or service, and then use only that data. Data use minimization prompts an organization to more thoughtfully and strategically reduce the risk of exposure or breach of an individual's data that might result from the improper actions of parties internal or external to the organization.

***Data Quality/Integrity.*** Data quality and integrity requires that organizations use data whose quality is suited to the use to which it is put, and that data is usable when needed to facilitate business process or deliver products or services requested by the consumer. Data quality requirements depend on the data's sensitivity, the degree of accuracy required, the nature of the use, and the risk to individuals of inaccurate results.

***Data Retention.*** Data retention provides that organizations retain data only as long as it is of some use to the organization or the individual. Data retention protects the individual against the risk raised by use of antiquated data that no longer reflects and individual's current circumstances

***Security.*** Organizations have an affirmative obligation to keep data safe from compromise, improper use, and breach.

***Accountability.*** An organization must be responsible and answerable for its actions related to all obligations in a Use-and-Obligations model.

## Prevention of Harm

Prevention of harm to individuals through appropriate risk and data management practices serves as both the motivation for meeting these obligations and as the metric by which their successful fulfillment is evaluated.[6] Users of data must consider the risk to individuals to whom the data pertains, and take steps to prevent harm that might result from the use of the data. The concept of harm can include, among other things, compromise of an individual's financial or physical well-being, embarrassment, and damage to reputation.[7]

6 The APEC Privacy Framework sets out prevention of harm as its first principle.
7 Additional work is needed to more clearly define and describe harm, as it can result from violation of privacy and inappropriate use of data.

## The Use-and-Obligations Analysis — Table A

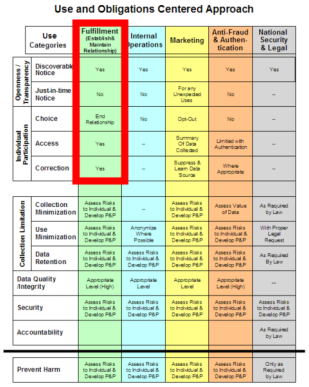
Table A offers a visual analysis of the Use-and-Obligations model. This section walks the reader through an analysis of each category of data use and the obligations triggered by that use. Part I of the analysis first examines the obligations related to individual participation. Part II reviews the internal risk assessment and mitigation obligations.

### Table A
### Use and Obligations Approach

| | | Use Categories | Fulfillment (Establish& Maintain Relationship) | Internal Business Processes | Marketing | Fraud Prevention & Authen-tication | National Security & Legal |
|---|---|---|---|---|---|---|---|
| Part I -- Individual Participation | Openness / Transparency | Discoverable Notice | Yes | Yes | Yes | Yes | Yes |
| | | Just-in-time Notice | No | No | For any Unexpected Uses | No | -- |
| | Individual Participation | Choice | End Relationship | No | Opt-Out | No | -- |
| | | Access | Yes | -- | Generalized Access: Summary of Data Collected | Limited with Authentication | -- |
| | | Correction | Yes | -- | Suppress & Learn Data Source | Where Appropriate | -- |
| Part II -- Internal Risks | Collection Limitation | Collection Minimization | Assess Risks to Individual & Develop P&P | -- | Assess Risks to Individual & Develop P&P | Assess Value of Data | As Required by Law |
| | | Use Minimization | Assess Risks to Individual & Develop P&P | Anonymize Where Possible | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | With Proper Legal Request |
| | | Data Retention | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | As Required By Law |
| | | Data Quality /Integrity | Appropriate Level (High) | Appropriate Level | Appropriate Level | Appropriate Level (High) | -- |
| | | Security | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P |
| | | Accountability | | | | | As Required by Law |
| | | Prevent Harm | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Assess Risks to Individual & Develop P&P | Only as Required by Law |

# I. Facilitating Individual Participation

## Fulfillment

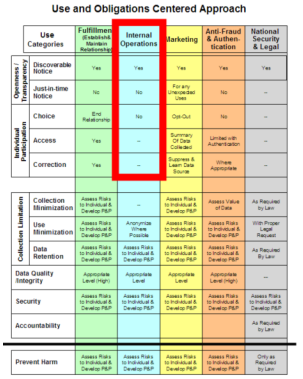



***Transparency/Notice.*** Consumers must be provided a discoverable notice about data collection and uses for transaction fulfillment and service delivery. Just-in-time notice is not required, although consumers may appreciate such a notice for certain complex transactions or services.

***Choice.*** The organization must use data necessary for fulfillment to complete the transaction or deliver the service to the consumer. For example, in the case of fulfillment of a transaction, the consumer has no explicit choice about this data use; if the company cannot collect this data, it cannot fulfill the transaction and the relationship between the company and the consumer effectively ends. In the case of delivering a service, the consumer has made an implicit choice about data use by subscribing to the service.[8]

***Access and Correction.*** Fulfillment data makes it possible for the organization to deliver a service to the customer. It also provides the basis for decisions related to the customer's ability to purchase goods or services, or to where goods or services are delivered. Fulfillment data, therefore, must be accurate and current. The consumer's ability to access his data and correct any errors is necessary to ensure its integrity. Companies are, therefore, obligated to provide consumers with the ability to access and correct data.

## Internal Business Processes

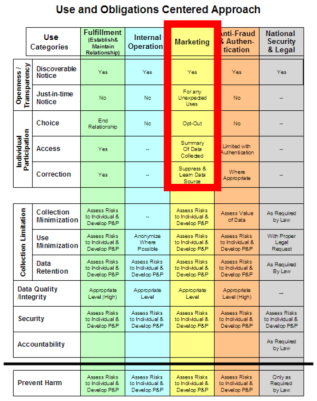



***Transparency/Notice.*** Consumers must be given notice of data use for internal business processes. Just-in-time notice is not required, because consumers would not find the uses unexpected.

***Choice.*** The consumer is not given a choice about the use of data for business operations, because this use is necessary to basic business functions such as accounting and internal auditing.

***Access and Correction.*** Organizations are not required to provide access and correction because the data used for internal business processes is generated through the fulfillment process. As noted, the Use-and-Obligations model provides for access and correction to this data for its use in fulfillment.

## Marketing



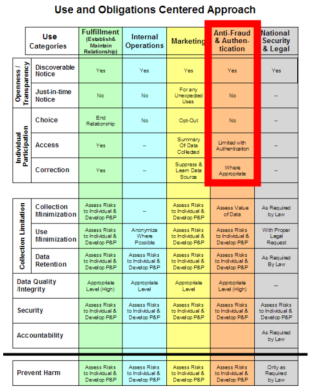

***Transparency/Notice.*** Just-in-time notice must be provided if the marketing initiatives would not be expected by the consumer. For other marketing, companies must provide an easy-to-read, discoverable privacy policy.

***Choice.*** At a minimum, the consumer must be offered the opportunity to opt out of marketing.

***Access and Correction.*** Consumers must, upon request, be provided generalized access — a summary of the kinds of data used for marketing. As marketing data does not form the basis for critical decisions about the individual, access to specific data is optional but not required.

8 In some instances, the organization may be able — and may choose — to fulfill a transaction or continue to provide the service even when the customer has chosen not to have data used for this purpose.

### Fraud Prevention and Authentication



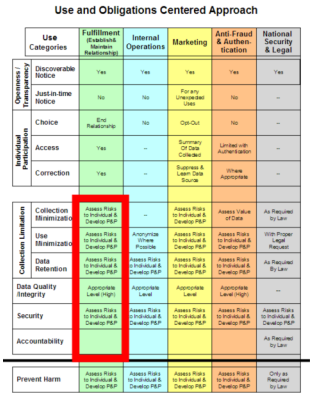

***Transparency/Notice.*** Just-in-time notice is not required. However, the privacy policy must state that the data is used to prevent fraud.

***Choice.*** Consumers have no choice about these uses, for reasons of public policy, safety and security.

***Access and Correction.*** Limited access to data that will not compromise fraud analysis and authentication functions is provided, so that individuals can understand what data about them is being processed.

## II. Risk Assessment and Mitigation

### Fulfillment




***Collection Limitation.*** Organizations must assess what data they reasonably need to complete a transaction with a consumer and deliver goods or services. It must also consider what data may be required to provide ongoing service delivery or extended service, if appropriate, and to fulfill warranty requirements. It should assess any risks related to storage of that data and address them as necessary.

***Use Minimization.*** Once collected, organizations must determine who needs to see the data, and under what conditions or circumstances. They must also decide for what other business functions besides fulfillment the data must be accessible. Use minimization involves limiting the amount and kind of data used in a specified business process, product, or service to that needed to achieve identified goals.

***Data Retention.*** Organizations must assess risks to individuals raised by retaining data, develop practices and procedures to determine when it is no longer useful, and develop schedules and procedures for appropriately retiring the data.

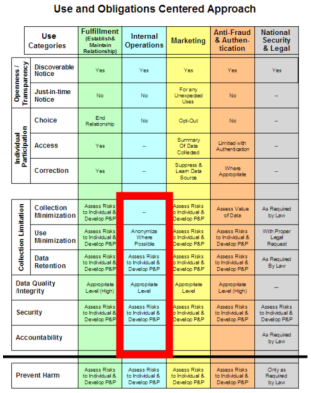
***Data Quality and Integrity.*** Data related to fulfillment usually includes, among other things, name, address, and credit card data. Because it is important both to the organization and the individual that fulfillment data be correct, data quality requires that the organization ensure that the data be complete, current, and accurate.

***Data Security.*** Organizations must assess risks to individuals raised by the capture, storage, and processing of fulfillment data and develop security policies and procedures to effectively manage those risks.[9]

***Accountability.*** Organizations must have in place policies, procedures, training, and compliance assessment to ensure that use of data for fulfillment is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

9 Organizations must also assess and manage security risks related to processing of data by business partners.

## Internal Operations




***Collection Limitation.*** Organizations must anticipate what data they will reasonably need to carry out internal functions such as accounting; marketing research and trend analysis; product analysis, improvement and development; commissions; and performance evaluations. Based on that assessment, they must collect only that data necessary to perform those internal functions.

***Use Minimization.*** Once collected, organizations must determine who needs to view or access the data for internal operations under what conditions or circumstances, and limit its use accordingly. They must also decide to which other business functions in an organization the data must be accessible and for what purposes. Use minimization also involves limiting the amount and kind of data used in a specified business process, product, or service only to that needed to achieve identified goals.

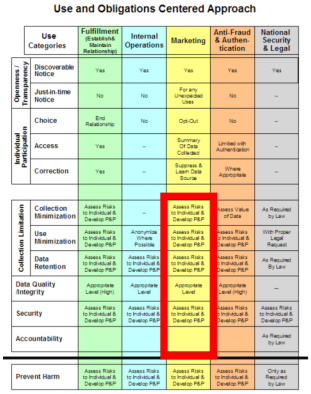
***Data Retention.*** Organizations must determine how long data is needed, and assess the risks to individuals raised by retaining data. In light of that assessment, organizations should develop a schedules, policies, and procedures for retiring the data.

***Data Quality and Integrity.*** Data used for internal operations can influence decisions related to budget planning, employee compensation, and commissions. Organizations must ensure that the quality of the data is at a level appropriate to its intended use.

***Data Security.*** Organizations must assess risks to individuals raised by the capture, storage, and processing of data and develop security policies and procedures to effectively manage those risks.

***Accountability.*** Organizations must have the policies, procedures, training, compliance assessment, and oversight in place to ensure that data is used for internal purposes in accordance with the organization's agreed-upon decisions.

## Marketing




***Collection Limitation.*** Organizations collecting and using data for marketing purposes must consider what data they legitimately need for marketing, and the risks related to storing additional data collected from consumers and third parties. They are required to consider the sensitivity of the data and the costs to secure it in light of its usefulness and predictive value. Based on that analysis, organizations must develop policies and practices to address risks raised by the data they choose to collect and retain for marketing.

***Use Minimization.*** Data may vary in its ability to identify consumer preferences and predict consumer buying behavior. Use minimization requires that organizations use in marketing applications only data that is effective and yields useful results. Use minimization enhances overall data security by reducing risk of data exposure and loss.

***Data Retention.*** Organizations must assess the risks that retaining data raises for individuals, develop practices and procedures to determine when it is no longer useful, and establish schedules and procedures for appropriately retiring it.

***Data Quality and Integrity.*** In analyzing data for potential use in marketing, organizations must consider — among other things — whether it can be used lawfully, whether its use is governed by contractual obligations, and whether permissions related to data must be respected. Organizations must determine whether data is sufficiently predictive to be suitable for marketing.

***Data Security.*** Organizations must assess risks to individuals raised by the capture, storage and processing of data and develop security policies and procedures to effectively manage those risks.

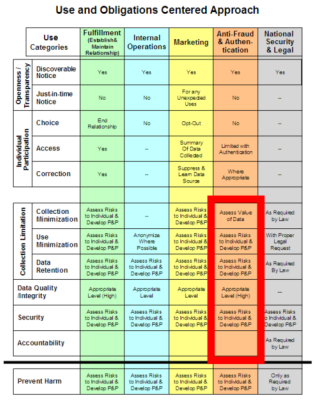
***Accountability.*** Organizations must have in place policies, procedures, training, and compliance assessment to ensure that use of data for marketing is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

### Fraud Prevention and Authentication

***Collection Limitation.*** Data required for fraud prevention and authentication — such as log-in credentials, social security number, mother's maiden name, account data, patterns of account activity — can be especially sensitive. The principle of collection limitation provides that only data necessary to carry out these functions be collected.

***Use Minimization.*** Because fraud prevention and authentication data is sensitive, organizations must take particular care to ensure that only the data necessary is used to perform desired functions. In many cases, the results of fraud analysis and authentication proofing may be provided to an organization's personnel who will need only the results of this activity. In such cases, personnel will have limited — if any — access to the raw data on which it is based.

***Data Retention.*** Organizations must determine for how long they must keep data to protect the organization from legal challenges, and assess the risks that retaining data raises for individuals. Based on that analysis, they must develop practices and procedures to determine when data is no longer useful, and develop schedules and procedures for appropriately retiring it.




***Data Quality and Integrity.*** Fraud prevention generally requires use of data of sufficiently high quality to reliably identify bad actors and avoid false positives. Authentication requires accurate and current data to assess whether an individual is who he says he is, and verify that he is authorized to engage in certain activities or to access physical places, accounts, records, or data.

***Data Security.*** Organizations must assess the risks that the capture, storage and processing of data raises for individuals, and develop security policies and procedures to address those risks. Data used for authentication purposes may be particularly sensitive because it can identify individuals and allow access to accounts and data. Fraud data, especially data that identifies a person as one who might possibly perpetrate fraud, also raises risks to reputation and to an individual's ability to engage in transactions or obtain financial services. Security for such data should be enhanced.

***Accountability.*** Organizations must have in place policies, training and procedures to ensure that data used for fraud prevention is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

## The Use-and-Obligations Approach: The Hotel Example — Table B

A stay at a hotel provides a practical example of how principles of fair information practices would be implemented according to a Use-and-Obligations model. It also illustrates the way in which data about a hotel guest flows between organizations to deliver the full range of hospitality services involved in a hotel stay. It further demonstrates how a Use-and-Obligations model would facilitate application of fair information practices as data is shared across entities.

An individual who books a reservation with a hotel engages with a complex network of entities that provide services for a guest's stay and develop a relationship with the guest so that future visits can be best tailored to his preferences. The chain (e.g., Hilton, Marriott, or Inter-Continental), the hotel (the individual physical property), the restaurant, the Internet provider, and the television and radio entertainment services delivered in the sleeping rooms are each owned and operated by discrete,

independent entities. All of these entities collect data from the guest and share that data with the hotel to provide services to the guest and to facilitate basic processes like billing and distribution of revenue to the appropriate service provider.

The guest may book his reservation through the chain's website or 800 number. The reservation is sent to the hotel with contact data, preferences, and any data the guest may have provided through the chain's loyalty program. When the guest registers at the hotel, the registration desk confirms the data and may collect additional data. At registration the hotel becomes the primary manager of the guest's data for the duration of the stay.

During the hotel stay, the guest may avail himself of various services — he may buy a book in the gift shop, dine in the restaurant, and rent movies on the entertainment system.[10] While independent entities provide each of these services, each shares data with the hotel so that fees can be charged against the guest's master bill.

## Fulfillment

The hotel collects data that it needs to book a reservation, collect payment and ensure that the guest's stay meets expectations. Fulfillment data may include preferences for furnishings in the room (bed size, pillow type, smoking/non-smoking). It may also include data about diet preferences and location of the room in the building. At the time the reservation is booked, the chain may provide the hotel with additional data derived from the guest's participation in the chain's loyalty program. To ensure payment, service providers share billing and data about charges for services with the hotel. To maintain the relationship with the consumer, the hotel shares with the chain any changes in preferences the guest may indicate during his stay.

***Transparency/Notice.*** The privacy notice posted on the hotel chain's website describes the nature of the data collected by the hotel and the way it is used.

***Choice.*** Because the data is used to complete the transaction with the consumer, there is no choice about its collection and use.

***Access and Correction.*** The consumer is granted access and the ability to challenge — and when appropriate — correct data for fulfillment.

***Collection Limitation.*** The chain and the hotel must determine how much data it needs to deliver the service expected and limit its data collection accordingly.

***Use Minimization.*** The hotel must take steps to ensure that appropriate personnel within the hotel have only the data they need to meet their job requirements. For example, the desk clerk may only need basic identification and payment data, while housekeeping may require data about pillow and temperature preferences but have no need for credit card data. Data may also be shared with independent service providers operating within the hotel. Use limitation ensures that data is available only to the appropriate parties within an organization or to its service providers or partners. Video services may share the fact and frequency of a guest's use of video services for billing purposes, but not the titles of specific movies or the nature of their viewing preferences.

***Data Retention.*** The hotel must make decisions about how long fulfillment data reasonably can be expected to be useful, and develop schedules and protocols for its destruction or retirement when appropriate. Maintaining data beyond its usefulness raises security risks of loss, misappropriation and misuse.

10 The data collected, used, and shared by the entertainment service provides an interesting example. The entertainment company can ascertain only the room occupied by the guest, the dates stayed and the services purchased. None of that data is collected or stored by the entertainment service in a way that is personally identifiable. The entertainment service sends data back to the hotel to facilitate billing. That data includes the names of the movies the guest viewed, when he viewed them, and the fee for each. Because the hotel can link that data to the guest's name, it is stored as personally identifiable by the hotel.

***Data Quality and Accuracy.*** The hotel must take reasonable steps to ensure that fulfillment data is complete, current and accurate.

***Data Security.*** As fulfillment data may contain sensitive data such as credit card numbers, it is important that it be appropriately secured to mitigate the risks to the hotel customer.

***Accountability.*** The hotel must have in place policies, training and procedures to ensure that use of data for fulfillment purposes is managed in accordance with agreed-upon decisions. The hotel is answerable for that management.

## Internal Business Processes

The chain and the hotel retain the guest's registration and a record of all purchases and transactions that take place during the stay in order to troubleshoot, maintain quality, improve processes, and conduct surveys.

***Transparency/Notice.*** The chain and the hotel are required to disclose the nature of the use of customer data for internal business processes. Just-in-time notice is not required because these uses are expected.

***Choice.*** The hotel does not give the guest a choice about the use of data for business operations, as such uses are necessary to normal business practices such as accounting and internal auditing.

***Access and Correction.*** Neither the chain nor the hotel is required to provide access and correction because this data is generated through the fulfillment process. As noted, the Use-and-Obligations model provides for access and correction to this data for its use in fulfillment.

***Collection Limitation.*** Data used for internal business purposes is derived primarily from fulfillment data. Data is not collected specifically to facilitate internal business processes.

***Use Minimization.*** To minimize exposure to risk of loss or of internal or external misuse, the hotel must use only that data necessary to support internal functions.

***Data Retention.*** The hotel should retain data only for as long as it is useful for internal business operations.

***Data Quality and Integrity.*** As data is critical to the hotel's ability to deliver its service and receive payment, the hotel must take reasonable steps to ensure that fulfillment data is complete, current and accurate.

***Data Security.*** Data used for these purposes should be secured in a manner commensurate with its sensitivity and the nature of its use.

***Accountability.*** The hotel must have in place policies, training, and procedures to ensure that use of data for internal business processes is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

## Marketing

Both the chain and the hotel use data collected from reservations and records of guest stays as a means to market to consumers.

***Transparency/Notice.*** The hotel must provide a discoverable privacy policy that describes the way in which the hotel uses data. The hotel must provide just-in-time notice if it intends to use the data for some unexpected marketing purpose.

***Choice.*** The consumer may opt out of the use of data for marketing at the time of registration and on the website.

***Access and Correction.*** The consumer has the right to generalized access — a summary of the type of information that is used for marketing, and to opt out of its use for this purpose. In this instance, the data comes directly from the fulfillment process and is therefore directly available to the consumer.

***Collection Limitation.*** Because fulfillment data is used for marketing, decisions about collection limitation are conducted in that context. The hotel collects any data needed for internal business processes from the consumer at the time of booking or reservation.

***Use Minimization.*** The hotel must assess data to determine whether it is necessary and appropriate for marketing purposes. The hotel must decide what data collected for fulfillment is used for marketing. For example, the hotel may decide that data about the use of in-room entertainment that is collected for fulfillment (and internal business processes) should not be used for marketing, because such data may raise privacy risks for the consumer. However, data about the guest's frequent use of spa services helps the hotel identify customers interested in such services and poses minimal risk to privacy.

***Data Retention.*** The hotel should develop and implement a policy for determining when data is no longer needed for marketing purposes and for its disposal.

***Data Quality and Accuracy.*** Any third-party data for marketing purposes must be assessed to determine that it is accurate enough to be used for marketing and can be managed to mitigate any risk to privacy.

***Data Security.*** The hotel should secure marketing data in a manner commensurate with its sensitivity and the risk that its loss raises for hotel customers.

***Accountability.*** The hotel must have in place policies, training, and procedures to ensure that use of data for marketing is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

## Fraud Prevention and Authentication

The hotel uses data to support fraud probability analysis and to enable authentication proofing. Third parties conduct most of that analysis. The hotel staff inspects identification documents (e.g., passport, drivers license) at check-in, but does not retain identification data.

***Transparency/Notice.*** The hotel privacy policy must indicate that data is used for anti-fraud analysis and authentication. Just-in-time notice is not required.

***Choice.*** Individuals have no choice about use of data for these purposes, for reasons of public policy, safety and security.

***Access and Correction.*** The hotel is required to provide limited access to data that will not compromise fraud analysis and authentication functions, so that individuals can understand what data about them is being processed for these purposes.

***Collection Limitation.*** The hotel likely uses an outside vendor to provide fraud prevention and authentication services. The hotel will be required to collect data deemed necessary by the service to support its analysis.

***Use Minimization.*** Data about fraud prevention and authentication will only be shared within the organization on an as-needed basis. Hotel clerks, for example, will need only the results of fraud probability analysis and the "yes" or "no" answer to identity authentication. The clerk does not need to see the raw data used to provide those results.

***Data Retention.*** Because the data required for fraud prevention and authentication is sensitive, its retention can raise risks to the hotel customer. The hotel should retain the data for as along as necessary to protect the hotel: to validate or justify its findings, to fulfill legal requirements, or to rebut challenges. The data should be disposed of when it is no longer useful for these purposes.

***Data Quality and Integrity.*** Because of the potential consequences for the consumer, it is critical that the data analyzed for prevention of fraud and authentication be of a quality necessary to yield accurate results. The hotel must ensure that the service provider it enlists for these services has sufficiently accurate, current, and complete data to serve these purposes.

***Data Security.*** The hotel should secure the data analyzed for fraud prevention and authentication proofing in a manner commensurate with its sensitivity and the risk of its loss raises for hotel customers.

***Accountability.*** The hotel must have in place policies, training, and procedures to ensure that use of data for fraud prevention and authentication is managed in accordance with agreed-upon decisions and that the organization is answerable for that management.

## Hotel Use and Obligation Chart

### Table B
### Hotel Example

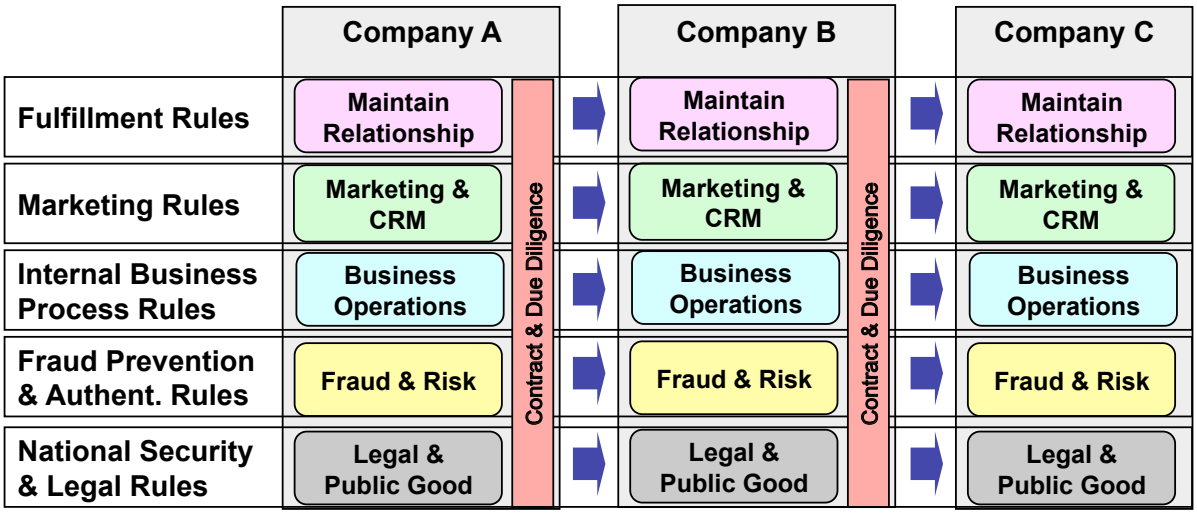
| | | Use Categories | Fulfillment (Establish& Maintain Relationship) | Internal Business Processes | Marketing | Fraud Prevention & Authen-tication | National Security & Legal |
|---|---|---|---|---|---|---|---|
| Part I -- Individual Participation | Openness / Transparency | Discoverable Notice | Yes | Yes | Yes | Yes | Yes |
| | | Just-in-time Notice | No | No | No | No | N/A |
| | Individual Participation | Choice | Yes | No | Yes | No | N/A |
| | | Access | Yes | No | Generalized Access: Summary of Data Collected | No | N/A |
| | | Correction | Yes | No | Opt-Out | No | N/A |
| Part II -- Internal Risks | Collection Limitation | Collection Minimization | Yes | There is no specific collection for this use | Only necessary for marketing | All data necessary to prevent fraud | As required by law |
| | | Use Minimization | Yes | Only use data necessary | Only necessary for marketing | All data necessary to prevent fraud | Only what required |
| | | Data Retention | For period necessary | For period necessary | For period necessary | For period necessary | As required by law |
| | | Data Quality /Integrity | Must be very accurate | Appropriate Level | Appropriate Level | Must be very accurate | N/A |
| | | Security | Appropriate for payment information | Appropriate for payment information | Appropriate for data used | Appropriate for sensitivity of the data | Data conveyed in a secure fashion |
| | | Accountability | Appropriate policies and procedures to mitigate risks | Appropriate policies and procedures to mitigate risks | Appropriate policies and procedures to mitigate risks | Appropriate policies and procedures to mitigate risks | Appropriate policies and procedures to mitigate risks |
| | | Prevent Harm | Assess risks to individual & develop policies and procedures | Assess risks to individual & develop policies and procedures | Assess risks to individual & develop policies and procedures | Assess risks to individual & develop policies and procedures | Only as required by law |

## Data Flow Among Affiliated Companies — Table C

In an information-based economy, data flows from organization to organization to facilitate fulfillment of orders and delivery of products and services; to provide customer care; to invoice customers; and to deliver advertising. As the chart below illustrates, obligations associated with the data attach to that data. New uses for data create new obligations for transparency and choice. Companies that provide data to other companies must have contracts in place that articulate obligations. They must also conduct appropriate due diligence to ensure that the company receiving the data possesses both the capacity and willingness to fulfill the obligations articulated in those contracts.

In the case of the hotel, each entity — the chain, the hotel, the independent service providers — would manage its data consistent with the Use-and-Obligations analysis of fair information practices. The decisions of each entity about the obligations must attach to the data, and be met by anyone using it. In a Use-and-Obligations model, each entity would enter into contracts that would specify the obligations related to data that flows between business partners.

**Table C**
**Data Flow Rules Between Companies with a Use and Obligations Centered Approach**



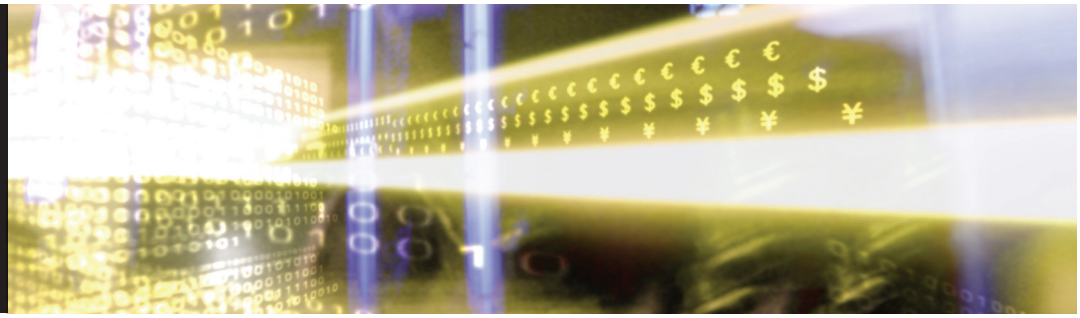

**Contracts:** The rights and obligations of parties sending and receiving data should be governed by contract. Companies that send data should conduct appropriate due diligence to ensure that organizations receiving data are willing and capable of meeting the obligations in law, regulation and company policy that come with the data. If data is transferred between companies to further a business process outsourcing arrangement, the outsourcing company must pass on the obligations via contractual requirements. If the data is transferred or sold downstream for multiple uses, the transferring organization must clearly articulate the nature of the obligations that attach to the data regarding each use.

## Conclusion

A Use-and-Obligations model for implementing fair information serves an environment where data collection is ubiquitous and broad individual choice provides an increasingly less effective mechanism to trigger data protection obligations. By establishing data use as the basis for a data holder's obligations to protect data, a Use-and-Obligations model requires that organizations assess the risks to individuals raised by data collection and use, and take steps to mitigate those risks. Such an approach better informs consumers and provides their data with enhanced and more effective protection. It also sets clear expectations for organizations collecting and using data. Additional work must be undertaken to develop a practical framework for accountability. The Business Forum for Consumer Privacy encourages the necessary dialog and engagement to make an accountability approach to data protection a reality.

# APPENDIX C

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



# Data Protection Accountability: The Essential Elements
# A Document for Discussion
# October 2009

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Galway Project

**Data Protection Accountability: The Essential Elements**
**A Document for Discussion**

## Preface

**Martin Abrams**
**Executive Director**
**Centre for Information Policy Leadership**

Innovations in technology; rapid increases in data collection, analysis and use; and the global flow and access to data have made an unprecedented array of products, resources and services available to consumers. These developments, however, in no way diminish an individual's right to the secure, protected and appropriate collection and use of their information.

The manner in which those protections are provided is often challenged by the dynamic, increasingly international environment for information. The global flow of data tests existing notions of jurisdiction and cross-border co-operation. How can companies and regulators support movement of data while providing the protections guaranteed to the individual?

Accountability, a concept first established in data protection by the Organisation for Economic Co-operation and Development ("OECD"), may provide an improved approach to transborder data governance that encourages robust data flows and provides for the protection and responsible use of information, wherever it is processed. But the practical aspects of accountability, and how it can be used to address the protection of cross-border information transfers, have not been clearly articulated.

- What will be expected of companies in an accountability system?
- How will enforcement agencies monitor and measure accountability?
- How can the protection of individuals be ensured?

The Centre for Information Policy Leadership at Hunton & Williams LLP was privileged to assemble a group of international experts from government, industry and academia to consider how an accountability-based system might be designed.[1] The experts met twice to define the essential elements of accountability, examine issues raised by the adoption of the approach and propose additional work required to facilitate establishment of accountability as a practical and credible mechanism for information governance. This report, guided by a drafting committee and reviewed by the group of experts, reflects the results of those deliberations.

[1] The group of experts is listed in the Appendix.

While this paper is focused on accountability as a mechanism for global governance of data, the issue of how accountability relates to the general oversight of privacy was raised during our discussions. It may be that accountability principles can address both international as well as domestic protection of information. Our discussion recognised that the concepts of accountability that can support an improved approach already are reflected in long-standing principles of fair information practices and are inherent in current governance in Europe, Asia and North America. Making accountability a reality requires that businesses apply those concepts so that their management of information is both safe and productive. Our talks further suggested that the growing complexity of data collection and use requires that much of the burden for protecting data must shift from the individual to the organisation.

Much of what is written about accountability in this paper can be accomplished by reinterpreting existing law. It is our hope that this paper will both chart the course forward for establishing accountability-based protection and motivate stakeholders to take the important steps to do so.

The Centre is indebted to the experts who participated in this effort for generously giving of their time and expertise, and most especially to the Office of the Data Protection Commissioner of Ireland for hosting our meetings and providing us with wise guidance. While this report reflects the results of their deliberations, the Centre alone is responsible for any errors in this paper.

**Executive Summary**

Accountability is a well-established principle of data protection. The principle of accountability is found in known guidance such as the OECD Guidelines[2]; in the laws of the European Union ("EU"), the EU member states, Canada and the United States; and in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. Despite its repeated recognition as a critical component of effective data protection, how accountability is demonstrated or measured has not been clearly articulated. This paper represents the results of the Galway Project — an effort initiated in January 2009 by an international group of experts from government, industry and academia to define the essential elements of accountability and consider how an accountability approach to information privacy protection would work in practice.

Accountability does not redefine privacy, nor does it replace existing law or regulation; accountable organisations must comply with existing applicable law. But accountability shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to

[2] Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

determine appropriate, effective measures to reach those goals. As the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability to make decisions to control the use and sharing of information through active choice, accountability requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to ensure responsible decision-making about the management and protection of data. The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

3. **Systems for internal, ongoing oversight and assurance reviews and external verification.**

4. **Transparency and mechanisms for individual participation.**

5. **Means for remediation and external enforcement.**

While many aspects of the essential elements are already established in law, self-regulation and corporate practices, some issues remain to be resolved to encourage robust adoption of an accountability approach. Policymakers and stakeholders should address questions about how accountability would work with existing legal regimes, and whether reinterpretation or amendment of existing laws might be required to make it possible to hold organisations accountable. Third-party accountability programmes have been recognised as useful in supplementing the work of government agencies. As they may play an important part in the administration of this approach, it will be necessary to clearly describe the contours of their role and the criteria by which their credibility will be assessed. Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. For the approach to work effectively, stakeholders must articulate the way in which the credibility of those programmes is established and tested. Finally, small- and medium-sized enterprises that wish to demonstrate accountability will face specific challenges that must be addressed.

While additional inquiry is needed before adoption of an accountability-based approach can be realised, its promise for international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates — robust transfer and use of data in a fashion that is responsible and protected.

## Introduction

The global flow of data drives today's information economy. Innovation, efficiency and service depend on rapid and reliable access to data, irrespective of its location. Digital technologies collect and store data in ways never before imagined, and information and telecommunications networks have evolved to provide seamless, low-cost access to data around the world.

As a result consumers have access to an unprecedented array of personalised products and services. While previously service hours ended at 5:00 p.m., the Internet enables individuals to access customer service in the middle of the night by phoning a local number that connects them to a call centre a continent away. Today, on a single server, a company can manage its email and business records for offices located in a dozen nations; travelers can rely on their debit and credit cards wherever they go; and individuals can use the Internet to download information from around the world without ever leaving their homes.

Indeed, with the increasingly global nature of data flows and the remote storage and processing of data in the "cloud", geography and national boundaries will impose few limitations on where data can be transferred but will present more practical challenges for administering and supervising global businesses.

In this environment, individuals maintain the right to the secure and protected processing and storage of their data that does not compromise their privacy. Protection must be sufficiently flexible to allow for rapidly changing technologies, business processes and consumer demand. Regulators must be equipped to articulate clear requirements for protection, educate companies and citizens, and monitor compliance in an environment in which data processing increasingly occurs outside the practical reach of most regulators, if not their legal jurisdiction.

Currently, global data flows are governed by law and guidance, which are enacted and enforced by individual countries or through regionally adopted directives or agreed-upon principles. The EU Data Protection Directive and implementing laws of member states, for example, govern the transfer of data from the European Union. The Safeguards Rule[3] imposes legal obligations on U.S. organisations to ensure that data is properly secured, wherever it is transferred or processed. And yet global data flows often challenge the way in which we have traditionally approached information protection. Daniel Weitzner and colleagues have written that information protection policy has long relied on attempts to keep information from " 'escaping' from beyond appropriate boundaries".[4] This approach is plainly inadequate in a highly connected environment in which anyone armed with a cell phone or laptop has at his or her fingertips unprecedented processing power, as well

[3] Under the Gramm-Leach-Bliley Act, the Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information.

[4] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Jay Sussman, "Information Accountability," *Communications of the ACM*, June 2008, at 82.

as the practical ability to collect, aggregate, transfer and use personal data around the world — and in an environment in which those capabilities are growing exponentially.

Weitzner and his colleagues lead a growing multinational call for an alternative approach to securing and governing personal data based on *accountability*. An accountability-based approach to data protection requires that organisations that collect, process or otherwise use personal data take responsibility for its protection and appropriate use beyond mere legal requirements, and are accountable for any misuse of the information that is in their care.

Adoption of an accountability-based approach to governance of privacy and information in global data flows raises significant questions for business, government and individuals.

Businesses express concerns about what might be expected of them in an accountability system, how their efforts to meet those expectations will be measured and how the rules related to accountability will be defined and enforced. Privacy enforcement agencies ask how accountability might work under local law. How do enforcement agencies measure an organisation's willingness and capacity to protect information when it is no longer in the privacy protection agency's jurisdiction? How does the agency work with and trust agencies in other jurisdictions? Consumer advocates worry that accountability will lessen the individual's ability to make his own determination about appropriate use of information pertaining to him.

The Centre for Information Policy Leadership, through a process facilitated by the Office of the Irish Data Protection Commissioner, convened experts to define the essential elements of accountability; to explore the questions raised by government, business and consumers related to adoption of an accountability approach; and to suggest additional work necessary to establish accountability as a trusted mechanism for information governance.

A small group of experts met initially in January 2009 to define the contours of the inquiry and identify existing research and legal precedents involving accountability. That meeting led to a draft paper that was presented to a larger gathering in April that included data protection experts drawn from government, industry and academia from ten countries. The April meeting identified a drafting committee that oversaw the Centre staff as they prepared this document, which was then circulated for comment among all of the participants. This paper reflects the results of that process.

## Accountability in Current Guidance

Accountability as a principle of data protection is not new. It was established in 1980 in the OECD Guidelines[5] and plays an increasingly important and visible role in privacy

[5] See, Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

governance. The Accountability Principle places responsibility on organisations as data controllers "for complying with measures that give effect" to all of the OECD principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly stated in the Directive, numerous provisions require that organisations implement processes that assess how much data to collect, whether the data may be appropriate for a specified purpose and the level of protection necessary to ensure that it is secure. Accountability also has featured more prominently in data governance in Europe as binding corporate rules have served as a mechanism to ensure the trusted transfer of personal data outside the EU.

The Spanish Data Protection Agency's February 2009 Joint Proposal for an International Privacy Standard includes an accountability principle that establishes a basis for data transfers based on an organisation's demonstration that it is responsible.[6]

Accountability is also the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), requiring that Canadian organisations put into effect the full complement of PIPEDA principles, whether the data are processed by the organisation or outside vendors, or within or outside Canada. In doing so, the accountability principle of PIPEDA establishes in law a governance mechanism for transborder data transfers.[7]

In the United States, the Federal Trade Commission ("FTC") applies to general commerce the Safeguards Rule of the Gramm-Leach-Bliley Act ("GLBA") — an accountability-based law that places obligations on a financial services organisation to ensure personal information is secured, but that does not explicitly explain how those obligations should be met.

The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework includes accountability as an explicit principle,[8] basing it on the OECD language and applying it to data transfers beyond national borders. The Framework states, "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above." The Framework specifically requires such accountability "when personal information is to be transferred to another person or organisation, whether domestically or internationally."

---

[6] "Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Information," version 2.3, 24 February 2009.

[7] This governance was explicitly described in a 2009 publication of the Office of the Privacy Commissioner of Canada, "Processing Personal Data Across Borders: Guidelines". In PIPEDA, accountability is an overarching principle that applies to protection and management of data, whether it is maintained and processed domestically or transferred outside Canadian borders for storage and processing.

[8] For more information about the APEC Privacy Framework and a full articulation of the principles, see <.<http://www.apec.org_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html#>.

Despite the inclusion of accountability in many data protection regimes, it is often unclear how companies demonstrate accountability for purposes of cross-border data transfers, how regulators measure it or why individuals should trust it.

**What is an Accountability-based Approach?**

An accountability-based approach to data governance is characterised by its focus on setting privacy-protection goals for organisations based on criteria established in current public policy and on allowing organisations discretion in determining appropriate measures to reach those goals. An accountability approach enables organisations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customers.

An accountability-based approach to privacy protection offers immediate advantages to individuals, institutions and regulators alike, because it recognises and is adaptable to the rapid increases in data flows.

- It will help bridge approaches across disparate regulatory systems, by allowing countries to pursue common data protection objectives through very different — but equally reliable — means. This helps to facilitate the many benefits of allowing data to move across borders, and to assure individuals a common level of data protection — even if achieved through a variety of means — irrespective of where their information is located.

- It will also heighten the confidence of individuals that their data will be protected wherever it is located and minimise their concerns about jurisdiction or local legal protections.

- It will raise the quality of data protection, by allowing use of tools that best respond to specific risks and facilitating the rapid updating of those tools to respond quickly to new business models and emerging technologies. An accountability approach requires organisations not only to take responsibility for the data they handle but also to have the ability to demonstrate that they have the systems, policies, training and other practices in place to do so.

- Allowing for greater flexibility will enable organisations to more effectively conserve scarce resources allocated to privacy protection. While it is essential that an accountable organisation complies with rules, resources devoted to fulfilling requirements such as notification of data protection authorities are not available for other, often more effective, protection measures. Accountability directs scarce resources towards mechanisms that most effectively provide protection for data. Organisations will adopt the tools best suited to guarantee that protections focus on reaching substantive privacy outcomes — measurable information protection goals — and to demonstrate their ability to achieve them.

Accountability does not redefine privacy, nor does it replace existing law or regulation. Accountable organisations must comply with existing applicable law, and legal mechanisms to achieve privacy goals will continue to be the concern of both regulators and organisations. However, an accountability approach shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified objectives.

Accountability does not replace principles of individual participation and consent that have been well established in fair information practices.[9] In many cases, consumer consent to uses of data remains essential to an organisation's decisions about data management. However, in some instances obtaining such consent may be impossible or highly impractical, and an accountability approach requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

## How Accountability Differs from Current Approaches

Accountability is designed to provide robust protections for data while avoiding aspects of current data protection regimes that may be of limited effect or that may burden organisations without yielding commensurate benefits. Accountability allows the organisation greater flexibility to adapt its data practices to serve emerging business models and to meet consumer demand. In exchange, it requires that the organisation commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a fashion that protects information and the individuals to which it pertains. Accountability requires an organisation to remain accountable no matter where the information is processed. Accountability relies less on

[9] Consent is found in the OECD Guidelines principle of Use Limitation, which states: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."

The principle of individual participation is also found in the OECD Guidelines, which state:

"An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

the rules that exist where the data is processed and more where the obligation is first established.[10]

Accountability relies less on specific rules but instead requires that organisations adopt policies that align with external criteria found in law — generally accepted principles or industry best practices — and foster a level of data protection commensurate with the risks to individuals raised by loss or inappropriate use of data. The accountable organisation complies with applicable law and then takes the further step to implement a programme that ensures the privacy and protection of data based on an assessment of the risks to individuals raised by its use. These risks should be assessed and measured based on guidance from regulators, advocates, individuals and other members of industry. Ultimately, regulators are responsible for ensuring that the risks to the data have been managed appropriately.

While the individual continues to play an important role in protecting his or her information, accountability shifts the primary responsibility for data protection from the individual to the organisation collecting and using data. Much of United States law, for example, is based on disclosure of the organisation's privacy policy, notification of individuals and obtaining their consent to specific uses of data. This approach is designed to enhance individual control over the manner in which data is used. Individuals are vested with responsibility for determining the manner in which their data is used and shared; organisations are obligated to provide the individual with sufficient information on which to base an informed choice.

In the U.S. the Federal Trade Commission is authorised to bring an enforcement action based on the organisation's notice when an organisation acts in an unfair or deceptive manner with respect to its privacy practices. In the absence of, and in some cases even with, an overarching privacy law, the individual is charged with policing the marketplace for privacy, by familiarising him- or herself with every organisation's policy and making a decision based on that information whether or not the organisation is trustworthy and using data in an appropriate manner.

Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing the marketplace for enterprises using data irresponsibly. Faced with rapid advances in data analytics and increasingly complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions, even when they can access privacy policies. Accountability demands responsible, appropriate data use whether or not a consumer has consented to one particular use or another.

Accountability does not wait for a system failure; rather, it requires that organisations be prepared to demonstrate upon request by the proper authorities that it is securing and protecting data in accordance with the essential elements.

[10] When, however, information security rules where data are processed are stronger than where the security obligation was incurred, they may indeed apply.

Enforcement of binding corporate rules ("BCRs") or the cross-border privacy rules as defined in APEC perhaps most closely approximate an accountability approach to information management and protection. BCRs, which are more fully developed, provide a legal basis for international data flows within a corporation or a group of organisations when other options are either impracticable or of limited utility. BCRs are a set of rules, backed by an implementation strategy, adopted within a company or corporate group that provides legally binding protections for data processing within the company or group. While the Directive and national laws that implement it rely on adequacy of laws and enforcement in a particular legal jurisdiction outside the EU, BCRs allow companies to write rules for data transfer that are linked to the laws where data was collected rather than look to compliance with the law of a particular geographic location where the data may be processed. Data authorities examine whether an organisation's binding rules export local European law with the data, and can determine whether its data practices and protections can be trusted to put those rules into effect — that it has in place the procedures, policies and mechanisms necessary to meet the obligations established in the BCR and to monitor and ensure compliance.[11]

**Essential Elements of Accountability**

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

   An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices. An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by

[11] BCRs cover only governance of data originating in the European Union. They do not apply to data originating from other regions.

tasking appropriate staff with implementing the policies and overseeing those activities.

Many global organisations have established policies in accordance with accepted external criteria such as the EU Directive, OECD Guidelines or APEC Principles. These companies demonstrate high-level commitment to those policies and the internal practices that implement them by requiring their review and endorsement by members of the organisation's executive committee or board of directors.

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

   The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

   Organisations in Europe, North America and Asia-Pacific have implemented comprehensive privacy programmes that incorporate personnel training, privacy impact assessments and oversight. In some cases, organisations have automated processes and integrated responsibility for programme obligations into all levels and across all aspects of the enterprise, while responsibility for compliance, policy development and oversight remains in the privacy office.

3. **Systems for internal ongoing oversight and assurance reviews and external verification.**

   Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful — and must be subject to some form of monitoring.[12]

[12] Accountable organisations have traditionally established performance systems based on their own business culture. Successful performance systems share several characteristics:

- they are consistent with the organisation's culture and are integrated into business processes;

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.

The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution. External verification must be both trustworthy and affordable. Privacy officers may work with their audit departments to ensure that internal audits are among the tools available to oversee the organisation's data management. Organisations may also engage firms to conduct formal external audits. Seal programmes[13] in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.

**4. Transparency and mechanisms for individual participation.**

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also

---

- they assess risk across the entire data life cycle;
- they include training, decision tools and monitoring;
- they apply to outside vendors and other third parties to assure that the obligations that come with personal data are met no matter where data is processed;
- they allocate resources where the risk to individuals is greatest; and
- they are a function of an organisation's policies and commitment.

[13] Seal programmes are online third party accountability agents.

provides for those instances when it is feasible. In such cases it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

**5. Means for remediation and external enforcement.**

The organisation should establish a privacy policy that includes a means to address harm[14] to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.

The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organisation and enhance its reputation for complying with its policies and meeting its obligations to individuals.

Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organisation should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organisation recognise and respond to the legal authority exercising proper jurisdiction.

## Public Policy Issues

While many aspects of the essential elements are already well established in law, self-regulation and corporate practices, consideration of several issues could usefully assist and stimulate the robust adoption of an accountability approach. These include the following:

[14] The concept of harm can include, among other things, compromise of an individual's financial or physical well-being; embarrassment; and damage to reputation. Additional work is needed to more clearly define and describe harm as it can result from violation of privacy and inappropriate use of data.

1. **How does accountability work in currently existing legal regimes?**

   Adopting an accountability approach to global information privacy governance may require reinterpretation or amendment of existing laws to enable the use of accountability mechanisms and to make it easier and more practicable to hold organisations accountable.[15]

   It may, for example, be necessary to provide in law or regulation that organisations comply with requests to inspect or review certain privacy practices to determine whether the organisation meets the essential elements of accountability as discussed in this paper. Work may be required to provide for legal recognition of the internal rules and policies organisations adopt and the measures organisations take to be accountable.[16]

2. **What is the role of third-party accountability agents?**

   Third-party review of an organisation's practices against appropriate criteria will greatly facilitate the success of an accountability approach. Qualified, authorised accountability agents will be an important element to address resource constraints in order to make the accountability approach work in practice.

   Establishing criteria for organisations that wish to serve as accountability agents, and articulating their role and the extent of their authority, will be a key task for policymakers. It will also be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

   Finally, to be useful to organisations, the services of an accountability agent must be affordable from a financial and operations perspective. Accountability agents must be able to price their services in a manner that allows them to recover their cost and build working capital, but still ensure that services are affordable to the full range of organisations that wish to avail themselves of their resources. Certification processes should be meaningful and trustworthy.

---

[15] In its 2008 report the Australian Law Reform Commission considered the possibility that Australian law be amended to assure an accountability approach could be used to improve governance of cross-border data transfers. A number of EU countries are exploring whether amending the law could better accommodate binding corporate rules.

[16] Such amendments are suggested in the APEC Privacy Framework, which requires that organisations comply with local data protection rules, but those amendments must enable them to write cross-border privacy rules that link to the APEC Principles to govern data transfers. Paragraph 46 of the Framework commentary encourages member economies to "endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with applicable laws".

They should also be designed to limit their disruption of business operations and to safeguard the confidentiality of an organisation's data assets.

**3. How do regulators and accountability agents measure accountability?**

An accountability approach does not rely on a breach to prompt review of an organisation's information practices and protections. Accountability agents and regulators must be empowered to review organisations' internal processes in a manner that allows them to ensure meaningful oversight. Policymakers may also wish to consider the measures to be taken by organisations to test for accountability and to be sure that it is working.

While an organisation's corporate policies must be linked to external criteria in the various countries where it does business, laws may differ from jurisdiction to jurisdiction. Accountability oversight must assess an organisation's overall privacy programme and allow for resolution of those differences in company policies in a manner that furthers the intent of a range of often conflicting laws or regulations.

Policymakers need to identify a way to measure confidence in an organisation's overall privacy accountability programme — commitment, policies and performance mechanisms — to determine whether an organisation is accountable even if its policies and practices are not a one-to-one match for local law and regulation.

**4. How is the credibility of enforcement bodies and third-party accountability programmes established?**

Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. Assessing accountability requires examining and judging an organisation's entire programme — a somewhat subjective analysis — so that the credibility of accountability agents is critical.[17]

Third-party accountability programmes such as seal programmes may supplement the work of government agencies. The credibility of these third parties must also be established if they are to be trusted by privacy enforcement agencies and the public. Investment in robust process and experienced, thoughtful staff will be essential to their success.

Additional work should be undertaken to determine how the credibility of these organisations is tested. It will be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the

[17] Work already undertaken at the OECD may be helpful in this regard. See Organisation for Economic Co-operation and Development, *Recommendations on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007).

criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

5. **What are the special considerations that apply to small- and medium-sized enterprises that wish to demonstrate accountability, and how can they be addressed?**

   In many cases, organisations that wish to demonstrate accountability may be small- and medium-sized enterprises, ("SMEs") for which privacy protection resources may be limited. Consideration must be given to the special needs of these organisations and the impact that fulfilling the essential element may have on these enterprises. It may be that aspects of the essential elements will need to be tailored or adapted for smaller organisations in a manner that makes them more workable but does not dilute them.

   Assessment requirements provide one example. While assessments may well serve the same function for SMEs as they do for larger organisations, such assessments may pose an undue burden on smaller enterprises with scarce resources. The nature of the assessment and the parties that may carry them out may differ for such entities, depending on the nature and sensitivity of the data in question. It will be important to examine how an SME might fulfill the assessment requirement without compromising itself financially. Similar questions of scalability as they apply to these organisations will need to be considered and resolved.

## Conclusion

Dramatic advances in the speed, volume and complexity of data flows across national borders challenge existing models of data protection. In the face of such complexity and rapid change, data protection must be robust, yet flexible. Privacy can no longer be guaranteed either through privacy notices and consent opportunities for individuals, or through direct regulatory oversight.

An accountability-based approach to data protection helps to address these concerns. It requires that organisations that collect, process or otherwise use personal information take responsibility for its protection and appropriate use beyond mere legal requirements, and that they be accountable for any misuse of the information that is in their care.

Accountability does not redefine privacy, nor does it replace existing law or regulation. While mechanisms to achieve privacy goals will remain the concern of both policymakers and organisations, an accountability approach shifts the focus of privacy governance to an organisation's ability to achieve fundamental data protection goals and to demonstrate that capability.

While there is already a greater focus on accountability in recent data protection enactments and discussion, and much can be accomplished within existing frameworks,

there is also a growing awareness that organisations that use personal data need to put in place and ensure compliance with the five essential elements of accountability:

(1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria;

(2) Mechanisms to put privacy policies into effect, including tools, training and education;

(3) Systems for internal, ongoing oversight and assurance reviews and external verification;

(4) Transparency and mechanisms for individual participation; and

(5) Means for remediation and external enforcement.

The path forward is clear, if at times daunting. The promise of an accountability-based approach to international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates alike — robust transfer and use of data in a fashion that is responsible and that ensures meaningful protections for individuals. To realise this goal, policymakers and the leaders of organisations must undertake the challenging and necessary work towards greater emphasis on true accountability.

**Appendix**
**Galway Project Participants**

The following lists the participants in the Galway Project. This list indicates participation in the Galway Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Marcus Belke, 2B Advice

Bojana Bellamy, Accenture

Daniel Burton, Salesforce.com

Emma Butler, Information Commissioner's Office, United Kingdom

Fred Cate, Indiana University, Maurer School of Law

Maureen Cooney, TRUSTe

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Peter Hustinx, European Data Protection Supervisor

Takayuki Kato, Consumer Affairs Agency, Japan

Christopher Kuner, The Centre for Information Policy Leadership, Hunton & Williams LLP

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Data Protection Commissioner, Spain

Rocco Panetta, Panetta & Associates

Daniel Pradelles, Hewlett Packard Company

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Scott Taylor, Hewlett Packard Company

Bridget Treacy, The Centre for Information Policy Leadership, Hunton & Williams LLP

K. Krasnow Waterman, Massachusetts Institute of Technology

Armgard von Reden, IBM Corporation

Jonathan Weeks, Intel Corporation

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

**UNITED STATES DEPARTMENT OF COMMERCE**

**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**

**In the Matter of**

***Information Privacy and Innovation in the Internet Economy*** **Docket No. 100402174-0175-01**

# COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

**June 14, 2010**

## Table of Contents

**COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY**

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commerce Department's Notice of Inquiry regarding the nexus between privacy policy and innovation in the Internet economy. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the global Internet.

## Summary

Over the past two decades, the Internet has created immeasurable economic growth and provided great social benefit. However, as General Counsel to the Department of Commerce ("DOC"), Cameron Kerry, observed in his remarks at the National Telecommunication and Information Administration's ("NTIA") May 7 public meeting, this growth cannot be taken for granted; it is built upon a foundation of trust in the privacy and security of online interactions and transactions. As Mr. Kerry noted, "the Internet and e-commerce depend on trust to flourish…[and] the government has an important but delicate role to play in preserving trust and enabling this digital fabric across our society to flourish."[1]

The DOC can contribute to a flourishing global digital economy by promoting the development of a comprehensive privacy framework for the US and by making the case for consumer trust as an enabler of innovation. In these comments, we present recommendations in response to the eight distinct issue areas addressed in the Notice of Inquiry ("NOI") as well as present a ninth topic – the impact on economic growth and innovation of unclear and outdated rules for access to consumer data by the US government. Throughout the comments, we explain why fully protecting consumer privacy interests online requires a rigorous mix of self-regulation, enforcement of existing law, regulatory activity, and enactment of new legislation. The DOC should consider making a comprehensive set of recommendations setting out how industry and government can protect consumer privacy online and integrate privacy into online transactions and interactions.

**1) The U.S. Privacy Framework Going Forward:** The DOC's Internet Policy Task Force ("Task Force") posed a series of questions about the strengths and weaknesses of the current U.S. privacy framework. CDT believes that the DOC can play an important role in defining and clarifying privacy protections for consumers. We urge the department to endorse a modern, comprehensive set of Fair Information Practice principles ("FIPs") and to recommend that these principles be incorporated into a new baseline federal privacy law, executive branch policies, and self-regulatory guidelines.

**2) U.S. State Privacy Laws:** The Task Force sought input on the impact of state privacy laws on U.S. businesses. In these comments, CDT notes that the states have been a critical laboratory for privacy innovation and experimentation. Data breach laws are one

[1] *See* C-SPAN, *Dept. of Commerce Conference on Internet Economy* (May 7, 2010), *available at* http://www.c-span.org/Watch/Media/2010/05/07/Economy/A/32703/Dept+of+Commerce+Conference+on+Internet+Economy.aspx.

of many examples of the important new ideas that have arisen from the states. At the same time, CDT recognizes that compliance with fifty different state privacy regimes can be burdensome for businesses, especially small or medium-sized entities and Internet startups. For that reason, DOC should support the enactment of a comprehensive federal privacy law which establishes a baseline set of privacy rules for all companies. Any preemption of state law in federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements. Even then, federal privacy law should not preempt state law unless the federal law provides as much protection as the best state laws.

**3) International Privacy Law and Regulations:** The Task Force requested comment on the intersection of foreign and domestic privacy laws and the challenges these laws pose to U.S. businesses with global operations. CDT believes that U.S. companies will be unable to adequately respond to the challenges posed by differing legal regimes until the U.S. adopts a forward looking baseline consumer privacy law based on a robust set of FIPs. Only then will the U.S. be in a position to assert global leadership on privacy to reconcile conflicting laws and find a path forward that supports both privacy and innovation. We also discuss the unsettled interaction between the EU Electronic Commerce Directive (ECD) and Data Protection Directive (DPD). In particular, we note with concern cases where Internet intermediaries such as Web 2.0 platforms have been held liable for privacy violations in user-generated content under the DPD, even as the ECD purports to protect them from liability. CDT believes that protecting technological intermediaries against liability for the conduct of their users has been critical in fostering growth and innovation in the Information Communication and Technologies ("ICT") industry. That protection, clearly enshrined in U.S. law, has supported U.S. leadership in Web 2.0 services. The DOC should reaffirm the importance of protecting intermediaries from liability and should seek, in its engagements around the world, to promote strong protections for intermediaries.

**4) Jurisdictional Conflicts and Competing Legal Obligations:** The Task Force raised timely questions about the difficulty of reconciling traditional determinants of jurisdiction and new models of cloud computing; when data is stored in multiple countries, companies and consumers alike face great uncertainty about which laws govern the data. CDT urges the DOC to keep in mind three factors that complicate these jurisdictional questions. First, multi-jurisdictional issues can arise whether or not a service strictly qualifies as cloud computing. Second, the jurisdictional issues are not limited to conflicting consumer privacy regimes, but also arise in the context of government access to private information. Third, multi-jurisdictional issues can arise even when all of the services (and thus all of the data) are in a single jurisdiction, especially if the service provider has business, marketing or other offices in other jurisdictions. In light of these concerns, the Task Force should consider cross-jurisdictional issues in a broader context than just strictly-defined cloud computing.

**5) Sectoral Privacy Laws and Federal Guidelines:** The Task Force sought comment on the effectiveness of the current sectoral privacy framework, which CDT believes is insufficient to protect consumers and promote innovation in the 21st century. American consumers and companies currently face a confusing patchwork of privacy standards

that differ depending on the type of data and the data collector; the vast majority of consumer data is not covered by any privacy law.[2] Simple flexible baseline privacy legislation which codifies a robust set of FIPs would protect consumers from inappropriate collection and use of their personal information, while enabling legitimate business. Baseline legislation should not, however, preempt the strong, sectoral laws that already provide important protections to Americans, but rather should act in concert with the protections afforded by a baseline privacy law.

**6) New Privacy-Enhancing Technologies and Information Management Processes:** The Task Force requested information about the impact of privacy enhancing technologies and information management processes on business practices and consumers' experiences. CDT believes that the foundational principles of Privacy by Design, a concept that offers a roadmap for integrating privacy considerations – and privacy-enhancing technologies – into business models, product development cycle, and new technologies, should be implemented by all companies to guide innovation in a manner that is consistent with FIPs.[3] DOC should encourage business practices that are consistent with Privacy by Design.

The government should also actively work to incentivize a robust marketplace of identity management products for consumers, as well as encourage government adoption of identity services that meet an established minimum standard for privacy. In order to ensure that there is ample room for companies to explore innovative business models and new services, the government should help guide a set of best practices for businesses to improve upon rather than creating a mandate in policy or technologies.

**7) Small and Medium-Sized Entities and Startup Companies:** The NTIA raised concerns about the burden of privacy laws and regulations on small and medium-sized entities and startup companies. CDT believes that policies that promote consumer privacy should be written such that they will not impede the growth of small and medium sized entities (SMEs) and startups, perhaps by carving out exceptions for companies that handle small amounts of non-sensitive consumer data. The Commerce Department should also recognize the potential burden that federal data retention laws would represent to SMEs and startup companies. Such laws could plausibly require online service providers to retain vast quantities of data for law enforcement purposes, potentially imposing prohibitive costs on SME's and startups.

**8) Government Access to Electronic Communications Data:** In addition to the issues specifically raised by the Task Force, CDT urges DOC to consider the impact of current government access laws on individual privacy and technology innovation. Technology innovation has far outstripped legal protections for personal data in the United States provided by the Electronic Communications Privacy Act (ECPA). While ECPA was a

---

[2] While most data collection practices and uses are not governed by a specific privacy law, under Section 5 of the FTC Act, the Federal Trade Commission has the authority to bring cases against unfair or deceptive company practices. While the Commission has recently brought such cases in the online privacy space, its enforcement resources are limited. CDT believes that FTC enforcement alone is not a long-term solution to the online privacy problem.

[3] Anne Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August, 2009)*, available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

forward-looking statute when enacted in 1986, it has not undergone a significant revision since then.

As a result, ECPA is now a patchwork of confusing standards that do not clearly apply to many new technologies. The law has been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies and putting user privacy at risk. Cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to permissive U.S. laws giving the government access to huge quantities of information with little judicial oversight. Without stronger legal privacy protection, the reluctance of consumers and businesses to use new communications services or foreign companies to use U.S. based cloud services may cause American companies to miss out on the productivity gains and new revenue sources that broader adoption of these services would offer.

**9) The Role for Government/Commerce Department:** The Commerce Department can play an important role in promoting innovation and economic growth by supporting substantive privacy protections for American consumers, encouraging the adoption of accountable practices such as Privacy by Design and providing global leadership to reconcile disparate privacy regimes. In this final section, we summarize the recommendations made throughout these comments.

## Introduction

Privacy is an essential building block of trust in the digital age. Privacy protections help to secure our communications and sensitive data, providing a foundation for e-commerce and the full realization of the potential benefits of the networked world. Privacy and the ability to remain anonymous are also fundamental to free expression, which has flourished nowhere more vibrantly than on the Internet. For the Internet to continue to thrive, consumers need to be assured that their communications and transactions will be secure and confidential.

In recent years, however, and at an accelerating pace, technology and market forces have created fundamental challenges to online privacy. More data is collected about individuals and retained for longer periods than ever before. Massive increases in data storage and processing power have enabled diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online activities. Study after study has shown that consumers do not understand how their data is collected or used under these new models – and when they find out, it is cause for great concern.[4] Privacy worries continue to inhibit some consumers from

---

[4] A poll conducted by Zogby International in June 2010 found that 88% of Americans are concerned about the security and privacy of their personal information on the Internet, while 80% are concerned that companies record their online activities and use this data to advertise and turn a profit. 88% of Americans consider the practice of tracking a user's Internet activity to be an unfair business practice. *See* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll* (June 9, 2010), *available at* http://precursorblog.com/content/americans-want-online-privacy-new-zogby-poll.

*See also* Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings,* March. 2008 (in which the majority of respondents said they were not comfortable

engaging in even more established business models such as online shopping.[5] Meanwhile, consumers cite privacy concerns as a top reason for declining to adopt location-based services, including fear of being tracked by government.[6] A 2009 Microsoft study found that more than 90 percent of the general population and senior business leaders were concerned about the privacy, security, and access ramifications of storing personal data in the cloud.[7] In some instances, successful implementation of new services, such as the Smart Grid, will require the development of more robust identification and authentication services to enable the exchange and management of user data. Consumer acceptance of these identification and authentication services – and hence to some extent the future growth of online commerce – depend on the degree to which consumer privacy is built into these new services. To increase consumer trust and truly achieve the potential of a Web 2.0 economy, these applications require a robust and comprehensive privacy protection framework.

Privacy protections must be viewed as an enabler of engagement in the Internet economy. If privacy and security are built into new services and applications and backed up by federal law, the payback in user trust will far exceed the investment. Only with strong privacy protections will consumers be willing fully participate in the Internet economy and take advantage of the full spectrum of services and opportunities that the Internet can offer.

We thank the Task Force for initiating this important inquiry into the privacy concerns raised by the ever-growing Internet economy. In these comments, we address the questions posed by the Task Force about the nexus of privacy and innovation and present recommendations for the DOC as to how the promotion of privacy can encourage innovation and consumer participation in the Internet economy.

## I. The U.S. Privacy Framework Going Forward

In Section 1 of its NOI, the Task Force requested comment on a series of questions pertaining to the ability of the existing privacy framework to both protect consumers and promote innovation. This section also solicited input on the potential of alternative privacy frameworks. Below, we discuss the weaknesses of the current model for

---

with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, *Use of Cloud Computing Services*, (September 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[5] *See* John B. Horrigan, *Online Shopping* (February 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.

[6] Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (February 2010), p 18, *available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[7] Penn, Schoen and Berland, *Cloud Computing Flash Poll – Fact Sheet,* Microsoft, *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc.

protecting consumer privacy and recommend instead a model predicated on a full set of Fair Information Practice principles.

### A. The Commerce Department should release an updated version of Fair Information Practice principles (FIPs) to guide privacy practices by the federal government and industry.

Ensuring trust on the Internet depends on the establishment of a guiding framework that recognizes the rights of consumers and the responsibilities of entities that collect, use, and share data about consumers. That framework already exists in the form of the FIPs that serve as the basis of existing privacy law and practice in the US. The first set of FIPs was released in 1973 by the Health Education and Welfare Department. Since that time, various versions of the FIPs have been used by federal agencies internally and externally; each agency adopts and abides by its own set of FIP principles. FIPs additionally appear, with some variation, in many international frameworks, including the OECD guidelines of 1980,[8] the Council of Europe data privacy convention,[9] and the EU Data Protection Directive (DPD).[10] The Asia-Pacific Economic Cooperation (APEC) Privacy Framework also incorporates some of the FIPs.[11]

The set of FIPs adopted by the Department of Homeland Security (DHS) in 2008 provides a modern and comprehensive framework for articulating privacy expectations and substantive privacy obligations. CDT presents this set of FIPs below for reference within these comments:[12]

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of information.*

---

[8] *See The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[9] *See The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1981), *available at* http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm.

[10] *See* "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT. The EU is currently reviewing the DPD in light of developments in technology since its inception. In comments filed with the European Commission, CDT stressed the continuing validity of the FIPs framework. We urged the Commission not to weaken the framework to make it more "flexible," but rather to clarify and improve it. *See* Center for Democracy & Technology, *Comments of the Center for Democracy & Technology to the European Commission in the matter of the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data* (January 2010) *available at* http://www.cdt.org/comments/cdt-comments-european-commission-personal-data.

[11] *See* APEC Electronic Commerce Steering Group, *APEC Privacy Framework* (2005), *available at* http://publications.apec.org/publication-detail.php?pub_id=390. Indeed, many tout this approach as a more flexible alternative privacy regime, in part because data protection "adequacy" is determined on an organizational basis, not a national one. However, it is currently non-binding upon member countries, leaving it up to individual nations when and how they implement its principles. For a critique of the APEC Privacy Framework, *see* Dr. Chris Pounder, *Why the APEC Privacy Framework is unlikely to protect privacy* (October 15, 2007), *available at* http://www.out-law.com/page-8550.

[12] *See* U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*

- **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*

- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as is necessary to fulfill a specified purpose.*

- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*

- **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.*

- **Security.** *Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

- **Accountability and Auditing.** *Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

### 1. The Commerce Department should emphasize substantive FIPs

Articulations of the FIPs vary widely, from a version articulated by the FTC – which focuses exclusively on notice, choice, access, and security – to a more robust set used by DHS, which we describe above. CDT believes that a privacy framework predicated on a limited set of procedural FIPs like notice and choice offers little in the way of substantive protections for consumers and does little to promote trust in the Internet ecosystem. Yet such a framework has been the dominant one in the U.S. in recent years.

In 2000, the FTC issued a report to Congress outlining four core principles of privacy protection: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation and (4) Integrity/Security.[13] The FTC's condensed set of FIPs has been largely criticized as a

[13] *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

watered down version of previous principles.[14] The result has been a narrow focus on Web site privacy policies and a stagnant notice-and-consent framework: a Web site or online service provides a notice of data collection and use practices, and the consumer's decision to interact with that site is taken as implicit agreement to the terms of that notice. The policies are generally written in legalese that is unintelligible to the average consumer.[15] Moreover, in order to ensure that data collection and use practices do not run afoul of the FTC and to avoid making "material" changes that would require consumer consent, companies often construct broad privacy policies and notifications that allow for nearly limitless data collection and use. This renders the notices of little worth to consumers since they may not accurately describe the actual data practices of a company.

We believe a greater emphasis on substantive privacy protections can be achieved by robust application of the full set of the FIP principles that we set out above. This FIPS based approach is part use-based and part collection-based. Fundamentally, incorporating substantive FIPs such as Data Minimization and Use Limitation, in addition to procedural FIPs like Transparency and Individual Participation, into any privacy framework will help construct a set of consumer rights and company responsibilities that together fortify and protect the decisions that consumers make online. We urge the Commerce Department to endorse a robust set of FIPs, based on those released by DHS, for all federal agencies. Future guidelines and principles on privacy-related topics, including those issued by the FTC and the Commerce Department, should be built around these FIPs.[16]

### B. The Commerce Department should establish benchmarks and metrics for evaluating company privacy practices.

One of the biggest challenges in establishing a framework for protecting consumer privacy is creating benchmarks and metrics for measuring whether practices developed to protect privacy are in fact accomplishing that goal.

In particular, there has been too much focus on measuring compliance efforts and not enough on identifying actual performance measures. For example, early on, the FTC

---

[14] *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341 (Jane K. Winn ed., 2006) ("The Failure of Fair Information Practice Principles"); Robert Gellman, *Fair Information Practices: A Basic History* (Dec. 2008), *available at* http://*bobgellman.com/rg-docs/rg-FIPshistory.pdf.*

[15] Researchers have shown that for a consumer to reach a basic understanding of how his or her information is being collected and used, he or she would have to spend between 181 and 304 hours each year reading Web site privacy policies. Nationally, this sums to between 39.9 and 67.1 billion hours per year spent reading privacy policies, for an estimated annual national economic cost of between 559 billion and 1.1 trillion dollars.[15] *See* Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, *I/S: A Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[16] CDT has written at considerable length about the key role of FIPs as guideposts for any consumer privacy framework. *See* e.g., Center for Democracy & Technology, *Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable* (November 2009), *available at* http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf; Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of A National Broadband Plan for our Future* - NBP Public Notice #29*:* (January 2010), *available at* http://www.cdt.org/files/pdfs/20100125_cdt-fcc_comments.pdf.

evaluated success by counting the number of privacy policies online and the comprehensiveness of these policies[17] – a measure we now understand does not equate with privacy protections.

By contrast, the FTC's annual report on the number of identity thefts is an example of a useful metric. We believe that the DOC has important research capabilities that can help regulators develop more useful metrics to measure whether particular practices or policies are in fact making a difference in protecting user privacy. Benchmarks are necessary for accountability and performance metrics are the best tools we have to see whether the policies and practices aimed at securing consumer privacy are working. This same discussion is occurring throughout the government as agencies seek to marry security and privacy measures.[18] We urge DOC to conduct a roundtable on this issue and produce a report on this specific topic of developing performance standards on privacy.

### C. Self-regulation cannot substitute for legislation

Industry members have long pointed to self-regulatory efforts as proof that baseline, federal privacy legislation would be duplicative and calamitous for innovation. In the past, the FTC too has suggested that self-regulatory regimes might play the principal role in protecting consumer privacy. But FTC commissioners have also recognized that "self-regulation cannot exist in a vacuum."[19] Indeed, after the Google/DoubleClick merger FTC Chairman Jon Leibowitz warned: "Ultimately, if the online industry does not adequately address consumer privacy through self-regulatory approaches, it may well risk a far greater response from government."[20]

CDT believes that a fair review of current business practices with regard to the use of personal and sensitive information of individuals leaves no doubt that the time for "a far greater response from government" is now: self-regulation works most effectively when consumer privacy law and effective enforcement exist to provide it with a meaningful backbone.[21] Fully protecting consumer privacy interests online requires a rigorous mix of self-regulation, enforcement of existing law, regulatory action, development of technical tools and standards, and enactment of new legislation.

---

[17] *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[18] *See, e.g.*, *Protecting Personal Information: Is the Federal Government Doing Enough?: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 110th Cong., 1st Sess. (June 18, 2008) (statement of Ari Schwartz, Vice President, Center for Democracy & Technology), *available at* http://www.cdt.org/testimony/testimony-ar-schwartz-3.

[19] Concurring Statement of Commissioner Pamela Jones Harbour, *Regarding Staff Report, Self-Regulatory Principles for Online Behavioral Advertising*, *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf.

[20] Concurring Statement of Commissioner Jon Leibowitz, *Google/DoubleClick*, *available at* http://www.ftc.gov/os/caselist/0710170/071220leib.pdf.

[21] Ira Rubinstein documents this issue in detail in his draft paper Privacy, Self-Regulation, and Statutory Safe Harbors (November 2009), *available at* http://www.law.nyu.edu/ecm_dlv3/groups/public/@nyu_law_website__centers__information_law_institute/documents/documents/ecm_pro_063814.pdf.

## II. U.S. State Privacy Laws

In Section 2 of its NOI, the Task Force sought input on the effect of state laws and regulations on both consumer privacy and industry growth.

CDT believes that the states have been a critical laboratory for privacy innovation and experimentation. States often can move more quickly that the federal government to address new privacy challenges and fill in the gaps left by federal protections. In developing federal policy recommendations on privacy, DOC should look to the states as one source of new ideas and approaches to privacy protection. For example, data breach notification laws are one of many important new ideas that have emerged from the states. These laws were developed after the information security provisions of the Gramm-Leach-Bliley Act[22] ("GLB") preempted inconsistent state laws but otherwise left the states free to develop new policy approaches to address data security. This narrow preemption language made possible California's landmark breach notification law, which requires companies to notify California residents in the case of a security breach that could put consumer information at risk.[23] Similar laws have so far been adopted by 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands.[24] And new federal rules for HIPAA-covered entities now include data breach requirements. Without the breathing room that GLB provided for the states to innovate on data security, breach notification laws and the important consumer protection they provide would never have been enacted.

This lesson needs to be kept in mind as DOC and other federal entities consider the parameters of a federal baseline consumer privacy bill. CDT recognizes that compliance with fifty different state privacy regimes can be burdensome for businesses, especially small businesses and startups, but broad preemption is not the best tool to address these concerns. Thresholds can be established in federal law which protect small data collectors, and participation in industry self-regulatory initiatives or regulatory safe harbors can help smaller companies get up to speed on best practices. Any preemption of state law in a new baseline federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements. Even then, CDT believes that preemption would only be appropriate in a federal privacy law if it provided at least as much protection as the best state laws.

---

[22] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 507, 113 Stat. 1338 (1999) (codified as 15 U.S.C. § 6807).

[23] *See* California Civil Code Section 1798.82(a).

[24] *See* National Conference of State Legislatures, *State Security Breach Notification Laws* (April 12, 2010), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx.

## III. International Privacy Law and Regulations

In Section 3 of the NOI, the Task Force sought responses to a wide range of questions, each addressing the impact of international data privacy law, regulations, and content restrictions on global Internet commerce and Internet users.

As was indicated in the NOI, U.S. companies certainly encounter compliance costs associated with doing business in countries with different privacy regimes. But it is also true that in the absence of relevant U.S. law, robust laws in other countries have had a salutary effect on the privacy practices of U.S. based companies. Companies that design for the highest common denominator in privacy will not only attract customers around the world, in many cases they will also minimize jurisdictional conflicts. CDT believes that U.S. companies will continue to be buffeted by conflicting rules until the U.S. adopts a forward looking baseline consumer privacy law based on a robust set of FIPs. Only then will the U.S. be in a position to assert global leadership on privacy to reconcile conflicting law and find a path forward that supports both privacy and innovation.

### A. The best way to address the challenge of global information flows is to incorporate the FIPs into the data management strategies of U.S. corporations and into baseline U.S. privacy law

As discussed in Section I, supra, a framework for robust privacy protection is readily at hand in the form of the widely-accepted FIP principles. The EU privacy framework is based on the FIPs, as are many other international data protection laws. Because of the general acceptance of the FIPs principles in internationally recognized privacy laws, directives, and regional frameworks, it would benefit U.S. companies with global operations to incorporate them into their business practices to minimize legal conflict and maximize international business opportunity. Likewise, the passage of comprehensive privacy legislation in the U.S. based on the FIPs would help close the gap between privacy rules in the U.S. and the EU,[25] ease jurisdictional conflicts and compliance challenges, and build consumer trust in U.S.-based services. The Commerce Department should support enactment of a baseline privacy law and should encourage industry adoption of innovative data protection practices such as Privacy by Design and other accountability measures that are consistent with the FIPs.[26] (For more on Privacy by Design, see section VI, infra).

Mechanisms exist for U.S. companies to conduct business in compliance with EU restrictions on cross-border transfers of personally identifiable information, but none is entirely satisfactory.

---

[25] Perfect harmonization of privacy rules globally is probably neither desirable nor possible. Even in Europe, the DPD has not produced total uniformity; member states may impose privacy measures stricter than those required under the DPD. Case C-101/01: Bodil Lindqvist, European Court of Justice, November 6, 2003, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:EN:PDF.

[26] *See* Marty Abrams, Ann Cavoukian, and Scott Taylor, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (November 2007). *Available at* http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

The EU DPD affects U.S. companies primarily through the "third country" principle: Article 25 of the DPD states that personal information may not be transmitted to nations outside of the EU unless those countries are deemed to have "adequate" data protection laws.[27] The effects of this rule are felt by entities that collect personal data from EU citizens and seek to store or transmit it outside of Europe.[28] The Article 29 Working Party does not consider U.S. law "adequate" (in part because the U.S. has no comprehensive data protection law), and thus in general personal information about EU data subjects may not be transferred to the U.S. for storage or other processing. However, there are several compliance mechanisms that allow U.S. companies to process personal information from the EU: the U.S.-EU "Safe Harbor" agreement,[29] Standard Contract Clauses ("SCCs"), and Binding Corporate Rules ("BCRs").[30]

Under the Safe Harbor agreement, companies self-certify with the Commerce Department that their published data protection practices satisfy seven principles.[31] Such certifications are then enforceable under the unfair and deceptive practices rule of the FTC Act.[32] However, criticisms of the program include that it is complaint-driven, that the European Commission has no enforcement power,[33] and that after ten years, the FTC has only recently begun enforcement actions.[34]

---

[27] However, Article 26.1(2)(a)-(f) provides exceptions to this general rule, including consent of the data subject, by contractual necessity, or on legal or public interest grounds.

[28] Examples include multinational corporations that manage employee or customer data on a global scale; or companies seeking to enter the "cloud computing" market in Europe, but where the cloud provider typically stores, moves, or provides access to daa on remote servers over multiple jurisdictions.

[29] "U.S.–European Union Safe Harbor," *available at* http://www.export.gov/safeharbor/eu/index.asp.

[30] *See* "Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries," Data Protection Unit of the Directorate-General for Justice, Freedom and Security, p. 48, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf. Individual countries' data protection authorities can also allow transfer to additional third countries they determine to be "safe" according to their own national data protection laws. *See id.* at p. 12.

[31] These principles are Notice, Choice, Transfer to Third Parties, Access, Security, Data Integrity, and Enforcement.

[32] In some instances, the FTC can seek administrative orders, federal court injunctions, and civil penalties of up to $12,000 per day. "European Union Safe Harbor Overview," http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

[33] Rights under the Safe Harbor initiative are only enforceable in the U.S. under U.S. law, making it difficult for EU consumers to pursue recourse.

[34] For reports on the initial FTC actions, *see e.g.,* S. Robertson, *US Prosecution for false web claim of Safe Harbor status,* (September 11, 2009), *available at* http://www.galexia.com/public/research/articles/research_articles-byte08.html; "FTC Takes Additional Safe-Harbor Related Enforcement Actions*," Privacy and Information Security Law Blog* (October 6, 2009), *available at* http://www.huntonprivacyblog.com/2009/10/articles/enforcement-1/ftc-takes-additional-safe-harborrelated-enforcement-actions/.

In the years leading up to these actions, two studies on the Safe Harbor implementation illustrated the widespread lack of enforcement. *See e.g.,* Chris Connelly, "The US Safe Harbor – Fact or Fiction?," *Galexia* (December 2008), *available at* http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.html; "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce," European Commission Staff Working Document (October 20, 2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

Two other ways that companies from third countries can comply with the DPD are SCCs and BCRs. To use SCCs, or Model Contracts, a company contracting with a controller or processor located in a third country includes approved contract language that provides adequate safeguards for privacy and fundamental rights.[35] Alternatively, a multinational corporation can implement a BCR by getting its data processing plan approved by the Data Protection Authorities ("DPAs") in the countries in which the company does business.[36] However, transfers are legal only within the corporation itself and not all EU member states recognize BCRs approved by other EU members' DPAs.[37] Thus, at this time, many companies still consider BCRs too costly, difficult, and time-consuming to obtain—and only a few companies have completed the process.[38]

These existing mechanisms for complying with EU cross-border data transfer restrictions each presents its own challenges, which could be mitigated in a number of ways. In our view, however, the most effective way of addressing the cross-border issue is for the U.S. to adopt a baseline consumer privacy law; only then will it be in a position to lead the global discussion on data protection and cross border data flows.

### B. Foreign laws aimed at "undesirable" content online can impede global trade and investment

Many countries impose restrictions on the kinds of content that can be displayed, transmitted or published online. Consider the following examples:

- In May 2010, a Pakistani court ordered the Pakistan Telecommunication Authority ("PTA") to ban Facebook in response to a page that promoted "Draw Mohammad Day" that the court found blasphemous. Access was restored in Pakistan later that month, only to be blocked by Bangladesh for similar reasons. Bangladeshi officials restored access after the content was taken down from the site. The PTA has blocked 450 other websites (including Wikipedia, YouTube, and Flickr) for "growing sacrilegious contents."[39]

---

[35] *See e.g.,* European Commission Freedom, Security and Justice Directorate-General, *Model Contracts for the transfer of personal data to third countries*, *available at* http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm; "Safer standards for European citizens' data transfers to processors in third countries*," European Commission Press Release, IP/10/130* (February 5, 2010), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/modelcontracts/ip_10_130_en.pdf.

[36] *See* documents WP 133, WP 153, WP 154, WP 155 in "Documents adopted by the Data Protection Working Party 2008," *available at* http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm.

[37] As of the end of 2009, only nineteen of twenty-seven EU countries participate in the "mutual recognition" process that allows an approval from one DPA to suffice for all (though the number is growing), necessitating additional BCR approval processes. "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," Article 29 Data Protection Working Party and Working Party on Police and Justice, *December 1, 2009), p. 11, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf.

[38] However, with some adjustments, BCRs are poised to become popular method of EU compliance.

[39] *See e.g.,* Iranda Husain, *"Losing Facebook: Inside Pakistan's decision to crack down on the Web,"* Newsweek.com (May 21, 2010,) *available at* http://www.newsweek.com/id/238324; "*Bangladesh unblocks Facebook after Muhammad row,"* BBC News (June 6, 2010), *available at* http://news.bbc.co.uk/2/hi/south_asia/10247858.stm.

- Two German citizens are suing the Wikimedia Foundation under German privacy laws to remove reference to their murder convictions on the victim's English-language Wikipedia page.[40] The plaintiffs argue that because the Wikipedia article deals with a local German public figure (the victim), Wikipedia must comply with German law.
- Under Turkish law, it is a crime to insult the founder of modern Turkey, Mustafa Kemal Ataturk, or to disparage "Turkishness." YouTube was asked to remove several videos the government found to violate this restriction. YouTube complied by blocking access to the videos in Turkey, but refused to do so for all YouTube users worldwide because the content did not otherwise violate YouTube's terms of use. In response, Turkey blocked access in the country to all of YouTube.[41]
- The Chinese government makes it illegal for users and Internet intermediaries to access, transmit, or publish any information that is "harmful to the interests of the state" (broadly defined) and regularly blocks access to a variety of foreign Internet services.[42]
- France and Germany prohibit the sale of Nazi paraphernalia on e-commerce platforms, and each country's hate speech laws further ban glorification of the Nazi party.[43]

Secretary of State Clinton announced earlier this year that it is the official policy of the U.S. to promote free expression and other human rights on the global Internet. Laws or enforcement actions restricting online content not only implicate human rights but also create barriers to the free flow of information and the growth of innovative ICTs. The kinds of content-based restrictions described above have a disproportionate impact on U.S. companies because of U.S. leadership in Web 2.0 services. When a government blocks a U.S. website or service or orders U.S. companies to take down content, it directly impacts the U.S. Internet industry's ability to reach customers in these markets and undermines U.S. brands.[44] The Commerce Department could help promote the U.S. ICT industry by:

---

[40] *See* John Schwartz, *"Two German Killers Demanding Anonymity Sue Wikipedia's Parent,"* NY Times (November 12, 2009), *available at* http://www.nytimes.com/2009/11/13/us/13wiki.html. The plaintiffs argue that under German privacy laws, they are no longer public figures because so many years have passed since their convictions and, as private citizens, the plaintiffs can act to protect their name and likeness from unwanted publicity. German editors of Wikipedia have already removed the names of the plaintiffs from the German-language version of the article. The German legal action seeks to remove content that is hosted on Wikipedia's servers, most of which are located in the United States. *See* http://wikitech.wikimedia.org/view/Server_roles.

[41] *See* Jeffrey Rosen, *"Google's Gatekeepers,"* NY Times, November 28, 2008, http://www.nytimes.com/2008/11/30/magazine/30google-t.html.

[42] *See* Testimony of Rebecca MacKinnon, before the Congressional-Executive Commission on China, on "China, the Internet, and Google" (March 1, 2010), *available at* http://rconversation.blogs.com/MacKinnonCECC_Mar1.pdf.

[43] *See* Lyombe Eko, "New Medium, Old Free Speech Regimes: The Historical and Ideological Foundations of French & American Regulation of Bias-Motivated Speech and Symbolic Expression on the Internet," 28 Loy. L.A. Int'l & Comp. L. Rev. 69, 100–104. See *also* Steve Kettmann, *"German Hate Law: No Denying It,"* Wired (December 12, 2000), *available at* http://www.wired.com/politics/law/news/2000/12/40669.

[44] This is especially true when little transparency is provided to users to explain a site's intermittent inaccessibility.

- Documenting the ways that various content-based restrictions impact the ability of U.S. businesses to compete globally.
- Raising content-based Internet restrictions as a trade issue in bilateral and multilateral discussions, including at the WTO.
- Opposing inappropriate and overbroad content restrictions as part of its efforts to promote innovation and the free flow of information.

There is also growing recognition that ICT companies have a responsibility to assess and minimize the risk that their business operations may pose to free speech and privacy.[45] The Global Network Initiative ("GNI") represents one effort to help ICT companies manage these global human rights risks.[46] The GNI works to document and promote corporate best practices for protecting privacy and free expression in difficult operating environments all over the world. [47]

The Commerce Department could help U.S. companies navigate these difficult legal and ethical questions in several ways:

- Help U.S. companies develop, document, and promote best practices for responding to governmental requests to restrict information flows or assist in surveillance.
- Encourage companies to join multi-stakeholder collaborative efforts like the GNI.

### C. Checks and balances on governmental surveillance are a key part of the privacy framework and will increase consumer trust, innovation, and trade

The rules that regulate government surveillance or that require companies to disclose customer information have a direct impact on user trust. Businesses thrive when there are clear, predictable rules to follow, and consumer trust grows when reasonable expectations of privacy are met. In the United States, technology innovation has far

---

[45] The UN Special Representative on business and human rights John Ruggie has developed a framework delineating the responsibilities businesses have to respect human rights, including free expression and privacy. *See* John Ruggie, *Protect, Respect, and Remedy: A Framework for Business and Human Rights* (April 7, 2008), pp. 11-14, *available at* http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf. This responsibility was also highlighted in Secretary of State Clinton's speech on global Internet freedom earlier this year. For more analysis of the human rights responsibilities of ICT companies, *see Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 110th Cong. (2008) (statement of Leslie Harris, President & CEO, Center for Democracy & Technology), *available at* http://www.cdt.org/testimony/testimony-leslie-harris-global-internet-freedom-corporate-responsibility-and-rule-law.

[46] The GNI is a multistakeholder collaboration between ICT companies, human rights NGOs, technology policy experts, academics, and socially responsible investor groups. *See* Global Network Initiative, *available at* http://www.globalnetworkinitiative.org.

[47] For examples, *see* Global Network Initiative Implementation Guidelines, *available at* http://www.globalnetworkinitiative.org/implementationguidelines/index.php. In addition, the GNI has developed the first revision of a Human Rights Impact Assessment tool companies can use in assessing human rights risk. This tool has not been publicly released.

outstripped legal protections for personal data provided by key statutes such as the Electronic Communications Privacy Act ("ECPA"). While ECPA was a forward-looking statute when enacted in 1986, it has not undergone a significant revision since then. The lack of strong government privacy laws in the United States makes it difficult for the U.S. to be an effective advocate for strong legal protections for digital information in the rest of the world, especially in countries with weak rule of law and non-independent judicial systems. If the U.S. wants to be a leader in global Internet freedom, it must begin by strengthening its legal protections here at home. See Section VIII, *infra*, for specific domestic policy recommendations.

### D. The trend towards intermediary liability poses grave risks to the future of the Internet

The remarkable growth of commerce, innovation and human interaction on the Internet has been made possible by ICT companies that provide open and inexpensive or free online platforms. One of the most important issues facing the Internet is whether these technological intermediaries, such as ISPs or platforms for user-generated content ("UGC"), should be liable for the content created or transmitted by their users. In the U.S. and the EU, an early consensus emerged that intermediaries should not be liable for the content created by third parties and transmitted over the services of those intermediaries. This policy of protecting Internet intermediaries from liability fostered the growth and innovation that we enjoy today. [48]

However, this policy consensus appears to be fraying. Governments are increasingly turning technological intermediaries into online cops, seeking to force them to control the content created, posted, or transmitted by their users, or be held liable for it.[49]

The Commerce Department should reaffirm the importance of protecting intermediaries from liability and should seek, in its bilateral engagements with other countries and in relevant multilateral bodies, to promote strong protections for intermediaries.

#### 1. Uncertainty abut the application of the EU Electronic Commerce Directive in the Web 2.0 era

The EU Electronic Commerce Directive ("ECD") provides a range of Internet intermediaries with significant immunity from liability for content posted or transmitted by others, including "hosting" services for UGC as long as the host quickly removes

---

[48] In the U.S., the leading social networks have rules against sexually explicit material and routinely remove even legal content if it violates their terms of service. The protection in U.S. law against liability also, importantly, insulates from challenge the efforts of intermediaries to identify, block and remove both child pornography and lawful but offensive content. These self-regulatory activities illustrate how a policy of protecting intermediaries from liability is compatible with – and can even help serve – other societal interests, such as protecting children.

[49] For more on the issue of intermediary liability in addressing unlawful behavior online, see Subsection D *supra* as well as CDT's paper on the impact of intermediary liability on free expression, and innovation: Center for Democracy & Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation" (April 2010), *available at* http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf.

unlawful content upon becoming aware of it.[50] The ECD also prohibits imposing on intermediaries a general obligation to monitor content on their services or a general duty to investigate possible unlawful activity—providing an important safeguard for user privacy. EU policymakers considered these provisions indispensable for protecting free information flows and encouraging ICT development.

However, the ECD was passed before the Web 2.0 era and the development of the UGC services that exist today. Recently, cases have begun to filter through the European national courts applying liability protection provisions to UGC sites and the results have been mixed: some courts have treated UGC sites as hosts eligible for immunity under the ECD, but they have also imputed knowledge of unlawful activity to the host (for example, because of knowledge of prior copyright infringement) thereby removing immunity. In other cases, UGC sites have been held liable as publishers (and thus not eligible for immunity), because they embed UGC into related content, provide an overall structure, or profit from advertising.[51]

Some European courts have also imposed monitoring duties on intermediaries in ways that undermine the policy choice laid out in the ECD. For example, a Belgian court held that requiring an ISP to filter certain copyrighted content did not violate the monitoring prohibition because the company was not being ordered to do so "generally."[52] German courts have also required monitoring to prevent future unlawful activity after a finding of prior infringement on the company's service.[53] One court has emphasized that "no unreasonable duties to monitor are to be entailed on [an online intermediary], which would challenge his whole business model," but at the same time admitted it is "difficult to predict what Courts would hold to be 'reasonable.'"[54] Results vary both within a member state and among member states.[55]

---

[50] Intermediaries covered include "mere conduits" that transmit information, "caching" services that provide temporary storage for facilitating onward transmission, and "hosting" services for user-submitted content as long as the host quickly removes unlawful content upon becoming aware of it. E-Commerce Directive, 2000/31/EC, Articles 12–14. In contrast to U.S. law, the ECD does not mandate the extension of immunity to search engines, though many member states provide it.

[51] *See e.g.*, ILO, *Web 2.0: Aggregator Website Held Liable as Publisher,* (June 26, 2008), *available at* http://www.internationallawoffice.com/newsletters/detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95; Crowell & Moring, *Recent French and German case-law tightens the liability regime for Web 2.0 platform operators* (July 9, 2008), *available at* http://www.crowell.com/NewsEvents/Newsletter.aspx?id=951#mediaisp2.

[52] Stephen W. Workman, "INTERNET LAW - Developments in ISP Liability in Europe," Internet Business Law Services, August 24, 2008 (also criticizing the Court for failing to apply Article 12 conduit immunity), *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2126.

[53] Henning Krieg, Bird & Bird, "Online intermediaries may have an obligation to monitor content posted by users" (June 4, 2007), *available at* http://www.twobirds.com/English/NEWS/ARTICLES/Pages/Online_intermediaries_obligation_monitor_user-posted_content.aspx.

[54] *Id.*

[55] A Dutch study noted the uneven application of ISP liability in the monitoring context occurs, in part, because of the differing types of law under which these cases can be decided. Ministry of Economic Affairs, "Liability of ISPs in the Netherlands," p. 7, (November 5, 2008), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/expert/20070220-dti_en.pdf.

These still-evolving rules create a great deal of uncertainty around the legal responsibilities of Internet intermediaries, pose difficult compliance challenges to companies seeking to offer Internet services in the EU, and can stifle innovation. The risk of liability especially burdens U.S. companies, which have developed the majority of Web 2.0 services and continue to be the global leaders in innovation in the space. Moreover, risk of liability can harm privacy by creating incentives for intermediaries to monitor users more extensively or collect and retain more personally identifiable information about them. Such expanded data collection raises serious concerns around how such information could end up in the hands of governments or be misused in other ways, further undermining consumer trust.

### 2. Intersection of ECD and DPD creates additional uncertainty, especially impacting U.S.-based Web 2.0 innovators

The protection against liability provided under the ECD is meant to be broad. However, the ECD includes an exception that refers to the DPD: the ECD states that it does not apply to "questions relating to information society services" under the DPD; it also states that "application of [the ECD] should be made in full compliance with the principles relating to the protection of personal data, in particular as regards … the liability of intermediaries…"[56] The exception may just mean that intermediaries are subject to the DPD insofar as they collect information on their users. However, the language has been interpreted by some as meaning that the protections against liability in the ECD do not apply to privacy violations that are the fault of individual users of the services. If that interpretation is correct, the DPD could become a major impediment to Web 2.0 services, for Web 2.0 hosts would be faced with the impossible task of ensuring that no content posted by any user infringed on the privacy of anyone else.[57] The chill on free expression of such an approach would be significant.

In part, the issue turns on the definition of the DPD's core concepts of "data controller" and "data processor." Controllers have certain obligations, and are liable for damages caused by unlawful processing of data. The definition of a "controller" is a functional one, however, and depends on the specific facts and circumstances of a given application or use.[58] In the Web 2.0 context, is the data controller the person who posted the content, or is it the provider of the platform? The status of a variety of Internet intermediaries in the Web 2.0 context as controllers or processors is, at the very least, unclear, creating a great deal of uncertainty for online service providers as to their liability risk for user content in the EU.

---

[56] E-Commerce Directive, 2000/31/EC, Article 1.5 and Recital 14.

[57] To illustrate, the vast majority of routine conversation and reporting on social network sites – which very often mention people other than the author – could potentially violate someone's privacy, and the service provider would have no way of answering that question.

[58] A "controller" is one who "determines the purposes and means of the processing of personal data," including delegating such processing to a processor. Article 2(d) and (e), Directive 95/46/EC. It is easy to envision how this framework applies to the example of an online store—a store is a controller when it collects personal data from a buyer, retains the data to process returns, and shares it with a shipping company to send the purchase. What is less clear is how the definition applies to a social networking site where users are uploading pictures of others to the website.

The Article 29 Working Party has issued two relevant opinions: one on the meaning of the terms "controller" and "processor,"[59] and another on the application of the DPD to social networking services ("SNS"). The policy choice laid out by the ECD indicates that SNS should be considered hosts eligible for immunity, but according to the Working Party, under the DPD they are also controllers of the personal data of the service's users.[60] The question, however, is not whether the SNS is the controller of its users' data – it clearly is – the question is whether the SNS is the controller of the non-user data that is posted (in a violation of privacy) by a user. (Users of SNS themselves could also be considered controllers if their actions involving others' personal data go beyond a "purely personal or household activity.") These two Article 29 Working Party opinions suggest that there is still much uncertainty on this question.[61]

The unsettled interaction between the ECD and DPD creates problematic incentives for privacy and innovation, and barriers to success for the U.S. Internet industry in the EU market: online service providers are much less likely to host UGC if they are liable for the privacy violations of their users. While Internet intermediaries have a role to play in advancing legitimate policy goals, imposing legal liability on intermediaries for the bad actions of their users (including for privacy violations) in the Web 2.0 context can have many unintended negative consequences for the free flow of information, technological growth and innovation, and even privacy.

The Commerce Department should address this issue. The first step might be to convene a trans-Atlantic multi-stakeholder dialogue, bringing together European officials, U.S. and European companies, and civil society representatives to explore the issues, starting with a fuller understanding of how the ECD and the DPD interact. In addition, the Commerce Department could:

- Document the beneficial relationship between strong protections for Internet intermediaries and the development and innovation of Internet industries, especially in terms of UGC and Web 2.0 services, highlighting the success of U.S. providers who benefit from the strong intermediary protections in this country.
- Urge its counterparts around the world to adopt laws that protect Internet intermediaries from liability for content posted by third parties as a key driver of innovation.
- Advocate for protections for Internet intermediaries in key multi-stakeholder bodies.
- Help companies develop best practices for safeguarding user and third party privacy in the Web 2.0, user-generated context.

---

[59] Article 29 Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor,'" 00264/10/EN WP 169, p. 29 (February 2010), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[60] Social networking services are defined in part as services that provide tools that allow user-generated content. Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking," 01189/09/EN, pp. 4–6 (June 2009).

[61] In one potentially problematic example, a provider of a UGC "lost and found" website was found to be a controller for information posted by users because the website was commercial, and because it "determined the terms of posting"—therefore, the website Is responsible for the propriety of the content posted. Article 29 Working Party, Opinion 1/2010, at p. 29.

- Promote such best practices across the U.S. Internet sector.

## IV. Jurisdictional Conflicts and Competing Legal Obligations

When data is stored in multiple countries, companies face great uncertainty about which laws govern the data. This challenge is greatly compounded in individual instances because in some cloud computing models, the data can be in multiple places at once, and a provider may not even know with certainty where any piece of data is located. Indeed, it is possible that even a query to locate and retrieve the data may cause the data to move between jurisdictions.

In Section 4 of the NOI, the Task Force sought comment on the applicability of data privacy laws to information stored in the cloud and, more generally, on the jurisdictional challenges posed by the transition to cloud computing. We assume that service providers will submit concrete examples of these jurisdictional challenges; as the Task Force considers these examples, we urge it to keep in mind three factors that complicate the issues.

First, multi-jurisdictional issues can arise outside of the specific category of cloud computing. Under the NIST definition,[62] cloud computing essentially offers flexible network-based storage and computing services that both corporations and individual consumers may find useful. But the definition would not likely cover important consumer-facing global services, such as social networking services, that may have servers in more that one jurisdiction. Ultimately, consumers and even many businesses may have no way to know whether online-based services qualify as "cloud computing," and multi-jurisdictional privacy issues arise whether or not a service strictly qualifies as cloud computing.

Second, the jurisdictional uncertainty is not limited to application of conflicting consumer privacy regimes, but also arise in the context of government access to private information. Customers of a service may assume that their information can only be disclosed to government pursuant to the laws applicable in their home jurisdiction, but foreign jurisdictions may assert the authority to compel disclosure under a different legal standard.[63]

Third, multi-jurisdictional issues can arise even when all of the services (and thus all of the data) are in a single jurisdiction, especially if the service provider has business,

---

[62] Peter Mell & Tim Grance, "The NIST Definition of Cloud Computing," Version 15, (October 7, 2009), *available at csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.*

[63] For example, after the USA Patriot Act was passed, a Canadian report expressed concern that section 215 of the Act would allow the U.S. government to order U.S. companies to turn over personal information held on Canadian citizens. Consequently, it recommended that public sector personal information not be transferred outside Canada. *See* "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing," Information & Privacy Commissioner for British Columbia (October 2004), *available at* http://www.scribd.com/doc/3697/Privacy-and-the-USA-Patriot-Act. *See also* "USA Patriot Act comes under fire in B.C. report," CBC News (October 30, 2004), *available at* http://www.cbc.ca/canada/story/2004/10/29/patriotact_bc041029.html.

marketing or other offices in other jurisdictions. In one example, Belgium has sought to compel Yahoo! to disclose information located in U.S. servers, relying solely on Belgium law and ignoring the U.S.-Belgium treaty that governs cross-border law enforcement data requests.[64]

In light of these concerns, we urge the Task Force to consider cross-jurisdictional issues in broader contexts than strictly-defined cloud computing. In a range of situations, there is a significant chance that a user's personal data will be subject to the laws of countries where protections are inadequate or significantly different than the consumer expects.

## V. Sectoral Privacy Laws and Federal Guidelines

In Section 5 of the NOI, the Task Force sought comment on the utility of the U.S.'s sectoral approach to privacy and on its effects on consumer privacy and business models. In this section, we present the view that sectoral privacy laws, while an important component of any privacy regime, alone are insufficient to accommodate the privacy risks associated with new technologies.

As the Task Force explains in the NOI, the current U.S. privacy framework is constructed in large part by sectoral privacy laws. For example, the Health Information Portability and Accountability Act ("HIPAA") provides necessarily tailored protections for health data while the Telecommunications Act of 1996 creates important protections for location data held by mobile carriers. Similarly specific laws, from the Video Privacy Protection Act to the Genetic Information Nondiscrimination Act, abound. These laws help prevent misuse of sensitive types of consumer data and they do so at a level of granularity that more general legislation likely could not address. However, as we discussed in Section I, *supra,* with no general privacy law to provide a baseline set of protections, this patchwork approach to privacy leaves much consumer data almost completely uncovered by law.[65]

Consider the example of the location information generated by cell phones, smart phones, and new location-based services and applications. The easy availability of location information raises several different kinds of privacy concerns. Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may describe both what a person is doing and where he or she is doing it. Location information can reveal visits to potentially sensitive destinations, like medical clinics, courts, political rallies, and union meetings. The ubiquity of location information has also increased the risks of stalking and domestic violence as perpetrators are able to use (or abuse) location-based

---

[64] For more information on this specific case, *see* Cynthia Wong, *Yahoo! protects user privacy – and gets fined?,* Policy Beta Blog, July 11, 2009, *available at* http://www.cdt.org/blogs/cynthia-wong/yahoo-protects-user-privacy-and-gets-fined.

[65] The exception here is the FTC's jurisdiction over unfair and deceptive practices, granted under Section 5 of the FTC Act.

services to gain access to location information about their victims.[66] And, as an increasing number of minors carry location-capable cell phones and devices, location privacy will become a child safety matter as well.

Clearly, location information can be very sensitive. Congress recognized this sensitivity when it passed the Telecommunications Act of 1996, [67] which limits the circumstances under which mobile carriers can share the information they have on customers' locations. These provisions are targeted at telecommunications carriers because at the time these protections were written, telecommunications carriers served as gatekeepers of location information – data about a cell phone user's location was primarily calculated within a carrier's network using the signals sent by the phone to the carrier's service antennas.

Nearly fifteen years later, the location of mobile devices is often determined through other technologies. Some of these technologies require the participation of an underlying wireless carrier, while others (such as WiFi positioning) work without the involvement or even knowledge of a telecommunications company – many smart phones can take advantage of both types of location determination technologies.[68] A consumer who uses the Yelp application on the location-enabled Apple iPod Touch, for example, provides her location information to Yelp entirely independently from any cell carrier – the iPod Touch is not a cellular device, and only has WiFi connectivity.[69] Congress could not have predicted these innovations and as a result, the location information generated during this interaction has very few substantive legal protections. Congress also could not have imagined the range of entities that today potentially have access to location data. While location data collected by the carriers retains protection, handset vendors, operating system vendors, advertisers, advertising networks, Web sites, application developers, and analytics companies may also have access to precise, sensitive information about where users are located but may not have any clear obligation to protect that information.

The uneven application of privacy laws to location data is but one example of how today's patchwork privacy framework provides both subpar protections for consumers

---

[66] *See, e.g.,* "Tracing a Stalker," Dateline NBC (June 16, 2007), *available at* http://www.msnbc.msn.com/id/19253352/; "Albert Belle pleads guilty to stalking ex-girlfriend," Associated Press (July 26, 2006), *available at* http://sports.espn.go.com/mlb/news/story?id= 2530911&campaign=rss&source=ESPNHeadlines.

[67] Through the Telecommunications Act of 1996, and subsequent amendments, Congress has prohibited a telecommunications carrier from disclosing Consumer Proprietary Network Information ("CPNI") – including "information that relates to the ... location ... [of] any customer of a telecommunications carrier ... that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" – except in emergency contexts or "as required by law or with the approval of the customer. *See* 47 U.S.C. § 222.

[68] As of July 2009, 3300 location-based applications were offered through application stores for mobile devices. And in May 2009, Skyhook Wireless, the company that provides WiFi positioning for Apple products, AOL, and others, was receiving 250 million location requests every day. This number has certainly grown substantially in the past year. *See e.g.,* Skyhook Wireless, *Location Aware App Report: From the Apple, Blackberry, Android, Nokia and Palm App Stores* (July 2009), *available at* http://www.locationrevolution.com/stats/skyhookjulyreport.pdf; Jenna Wortham, *Cellphone Locator System Needs No Satellite,* New York Times (May 31, 2009), *available at* http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html.

[69] *See iPod Touch: Features*, *available at* http://www.apple.com/ipodtouch/features/ (last visited Feb. 21, 2010).

and uneven guidance for companies. In countless other realms of rapid innovation – from online advertising to the Smart Grid – consumers are finding that sectoral privacy laws cannot keep pace with the data they are generating while businesses are discovering that the rules of the road are unpredictable.[70] While sectoral laws provide fundamentally necessary protections for consumers that no single piece of general legislation alone can replace, in an economy driven by innovation, only a flexible baseline privacy law can ensure that commercial data collection and use, regardless of the technology or the industry sector, is subject to fair information practices.

# VI. New Privacy-Enhancing Technologies and Information Management Processes

## A. Background

In Section 6 of the NOI, the Task Force sought comment on the impact of privacy enhancing technologies ("PETs") and privacy-enhancing business models on consumer privacy. It also requested input on the state of new identity management systems and their interaction with consumer privacy.

In this section, CDT discusses how PETs, privacy-enhancing business models, and identity management systems can all contribute to the successful implementation of a robust set of FIPs. We also describe how the federal government can promote the development of privacy-protective identity management systems

## B. Privacy enhancing technologies and Privacy by Design

Privacy Enhancing Technologies, such as encryption software, anonymizers, browser extensions that provide granular data controls, and privacy settings offered by online companies enable implementation of the Individual Participation FIP through technology; PETs additionally help users reap the benefits of other FIPs – such as Security and Data Minimization. As they have been traditionally understood, PETs are most useful for users who already understand online privacy risks; they are essential user empowerment tools, but they form only a single piece of a broader framework that should be considered when discussing how technology can be used in the service of protecting privacy.

While PETs focus on specific tools for consumers, Privacy by Design, a concept prominently championed by Ontario's Information and Privacy Commissioner Ann Cavoukian, offers a broader approach for integrating privacy considerations into business models, product development cycles, and new technologies.

As described by Cavoukian, "Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance

---

[70] *See* Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review, Vol. 63 (2010), pp. 19-22, *available at* http://ssrn.com/abstract=1568385.

must ideally become an organization's default mode of operation." Privacy by Design presents a set of "foundational principles" that can help companies innovate in ways that are consistent with FIPs. These seven principles are listed in abbreviated form below:[71]

- **Proactive, not Reactive; Preventative, not Remedial.** *The Privacy by Design approach … anticipates and prevents privacy invasive events before they happen. [It] does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.*
- **Privacy as the Default.** *If an individual does nothing, their privacy still remains intact.*
- **Privacy Embedded into Design**. *Privacy by Design … is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.*
- **Full Functionality – Positive-Sum, not Zero-Sum.** *Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.*
- **End-to-End Lifecycle Protection.** *Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish.*
- **Visibility and Transparency.** *Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.*
- **Respect for User Privacy.** *Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.*

These principles represent one set of tools that can help companies realize the implementation of a comprehensive set of FIPs; they suggest how some – though not all – of the privacy concerns raised *by* new technologies can be addressed *through* new technologies and solid business practices. Indeed, many of these principles were implicitly referenced in UC Berkeley professor Deidre Mulligan's recent interviews with industry leading privacy professionals.[72]

---

[71] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August 2009), *available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

[72] *See* Kenneth A Bamberger and Deidre K. Mulligan, *Privacy on the Books and on the Ground* (March 10, 2010). Stanford Law Review, Vol. 63, 2010, *available at* http://ssrn.com/abstract=1568385.

The DOC should encourage companies to incorporate the principles of Privacy by Design into their business models.[73] Moreover, the DOC and the federal government more broadly should lead by example by deploying PETs as part of their key public-facing activities, such as the open government initiative. Further, the DOC should recommend that evaluations of companies' implementations of Privacy by Design be part of all procurement decisions by the government.[74]

### C. Identity management systems can enhance consumer trust in Internet commerce.

In Section 6 of the NOI, the Task Force also solicited input on the potential role of trusted identity providers in the Internet ecosystem, their impact on privacy and innovation, and the appropriate role of government in guiding the development of the identity provider marketplace. In this portion of our comments, we suggest two distinct, though not necessarily mutually exclusive, approaches to incentivizing the development of a privacy-protective marketplace for identity providers.

#### 1. Background

The efficiency and convenience of online interactions continues to drive services online, and providers for online identity are offering to help consumers manage this information and further streamline online interactions. Some models for identity management place the user in the middle of an interaction between an identity provider and an online service. This method, called federated identity, allows service providers to rely on trusted third parties (the "identity provider") to authenticate users of their service. If carefully designed and implemented, user-centric, or federated, identity systems can give the user greater privacy protections and greater control over what information is provided in connection with any given transaction.

Currently, there is not a consensus around the rules of the road for identity management

---

[73] *See* e.g., Cavoukian has published a Privacy by Design Diagnostic Tool Workbook that companies can use to determine whether and how they are complying with Privacy by Design principles.[73] Meanwhile, many companies, including IBM, Sun Microsystems, Hewlett-Packard, and Microsoft have already incorporated Privacy by Design into their product development processes and made strong statements about important role that protecting privacy plays in their business models. Anne Caovukian, *Privacy Diagnostic Tool (PDT) Workbook* (August, 2001), *Version 1.0, available at* http://www.ipc.on.ca/images/Resources/pdt.pdf; IBM, Privacy is Good for Business: An Interview with Chief Privacy Officer Harriet Pearson, *available at* http://www-03.ibm.com/innovation/us/customerloyalty/harriet_pearson_interview.shtml; Microsoft Corporation, Privacy Guidelines for Developing Software and Services (February 2009) at 5, *available at* http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en ("Microsoft Privacy Guidelines"); Hewlett-Packard Development Company, Protecting Privacy at HP: Giving Individuals More Control over their Information (August, 2007), *available at* http://h41111.www4.hp.com/globalcitizenship/uk/en/pdf/Privacy_casestudy_hires.pdf; Michelle Dennedy, Sun Privacy-enhancing Desktop Technologies (January 2009), *available at* http://www.privacybydesign.ca/speaker-dennedy.htm.

[74] The extent to which the government can influence the market in a pro-privacy way was well illustrated in early 2009 when WhiteHouse.gov realized that it needed to offer YouTube videos to site visitors without placing cookies on their computers. The White House worked with YouTube to institute a fix such that merely visiting a landing page containing a video would not automatically set a persistent cookie. Within weeks, YouTube had made use of these "delayed cookies" available for any video on any site – bringing the privacy protective innovation required by government web sites to every YouTube provider. *See e.g.,* Alissa Cooper, *E-Gov 2.0 in Action* (Jan 22, 2009), *available at* http://blog.cdt.org/2009/01/22/e-gov-20-in-action; Alissa Cooper, *WhiteHouse.Gov: Moving the Cookie Forward* (March 3, 2009), *available at* http://www.cdt.org/blogs/alissa-cooper/whitehousegov-moving-cookie-forward.

– instead, each model is attempting to survive without a meaningful marketplace in which to compete on privacy practices or consumer protections. As these models for identity management processes emerge, careful attention must be paid to how they can both enhance privacy and support business models; a successful marketplace will require careful design.[75] Ensuring that the principles of Privacy by Design are included in new identity management models will require a balance of self-regulation, enforcement of applicable existing law, and possibly new laws providing safe harbors for identity management systems that can prove they meet a set of best practices. Only through a mix of incentives will an identity management industry emerge that allows privacy and online identity to co-exist in a meaningful way.

### 2. Governance of identity management systems: a FCRA model

While it is still an open question, it seems likely that there are some existing laws that would apply to the emerging identity management marketplace. One clear candidate is the Fair Credit Reporting Act[76] ("FCRA"), which requires so-called credit reporting agencies ("CRAs") to comply with Fair Information Practice principles incorporated in the law. The label CRA denotes entities that provide information to third parties about an individual's credit, reputation, or character. At its base, FCRA regulates the collection, dissemination and use of consumer information for use by third parties. The broad definitions in the Act seem to include any entity that regularly assembles or evaluates information about a consumer or their reputation for the purpose of furnishing that information to a third party – which seems to also describe the role of an identity provider.

The FTC's analysis of FCRA[77] seems to imply that any kind of screening of background or reputation to deliver the service is adequate to classify a service as a CRA subject to the provisions of the Act. Depending on how identity providers develop and what uses their services are put to, these entities may indeed be doing specialized types of background checks initiated by consumers for online consumer or government services that Congress envisioned regulating when enacting FCRA.

If FCRA does apply to identity providers and services, then both would have to comply with FIPS-like obligations. For example, if identity providers are considered CRAs under FCRA, they would have to comply with the following requirements: File Disclosure, Access and Correction, Timeliness, Use Limitations, Disclosures to Relying Parties, Disclosures to Data Furnishers. If identity services are covered under FCRA, relying parties would also have a number of important FIPs-related obligations, including Use Limitation, Certification of Purpose, Notification of Adverse Action, Notification of

---

[75] For a more complete listing of issues that need to be addressed for such a system to develop successfully, *see* Center for Democracy & Technology, *Issues for Responsible User-Centric Identity* (Nov. 2009), *available at* http://www.cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf.

[76] Codified at 15 U.S.C. § 1681, *available* at http://www.ftc.gov/os/statutes/031224fcra.pdf.

[77] Much of this analysis comes directly from a 1999 staff opinion letter from the FTC on whether reporting of public records alone makes a furnisher a CRA, *see* http://www.ftc.gov/os/statutes/fcra/sum.shtm.

Address Discrepancy, and Proper Disposal of Records.[78] Even if FCRA is found not to apply, conforming to such FIPs-like principles will significantly benefit consumer privacy and instill the trust necessary to help identity providers grow.

### 3. Governance of identity management systems: an insurance and safe harbor model

A second model for governance of identity management that is worth examining is the creation of a set of best practices integrating levels of assurance, levels of protection, and other policies that are important both to consumers and business adopters. A comprehensive set of policies and incentives to reward identity providers and set policy frameworks that integrate robust privacy protections and innovate within established standards for information protection should be created in order to drive development of privacy protective identity management systems. The creation of an insurance and safe harbor regime, as suggested in the FCC's National Broadband Plan ("NBP")[79], would be one effective way to ensure that these policies are implemented.

The insurance regime for identity management that is envisioned in the NBP is similar to the role the Federal Deposit Insurance Corporation ("FDIC") plays in the banking space. The FDIC is a private entity with government backing that protects consumers in the banking industry, providing confidence that the money entrusted with a private bank is insured in case the bank fails. As part of this program, the FDIC creates rules and regulations for participating banks, in order to effectively manage the risk taken in insuring these banks. A similar regulatory regime could provide rules for consumer data in order to insure identity providers and, potentially, could provide a safe harbor for identity providers who follow strict and robust privacy-protective guidelines and conduct audits for data

Clearly, it would not be possible for an insurance entity to reimburse a consumer for data lost or breached. However, an FDIC-like entity or regime could provide appropriate identity theft resources for affected consumers, or even damages paid out by the insurance. It could also insure that a user always has data portability. If a safe harbor, like that discussed in the NBP, were implemented, it would be imperative that the best practices required to participate under such an insurance model are strong enough to provide effective protections for consumer privacy and security. These best practices for business, government and consumers could be developed by an entity such as NIST.

### 4. Many viable regulatory approaches exist

In the past, CDT has suggested other types of private or public legal regimes to ensure

---

[78] For a detailed analysis of the potential applicability of FCRA on identity management, *see* Center for Democracy & Technology, *Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act's Application to Identity Providers (Feb. 2010), available at* http://www.cdt.org/files/pdfs/CDT%203rd%20Privacy%20Roundtable%20Comments%20-%20Protecting%20Privacy%20in%20Online%20Identity.pdf.

[79] *See* National Broadband Plan (Marc 2010), *available at* broadband.gov.

identity providers properly safeguard consumer privacy.[80] Although we believe an insurance and safe harbor model has potential, we also believe a contract regime or relying on existing regulatory frameworks, i.e., a FCRA regime, could be viable regulatory approaches here. Above all, we need rules and guidelines for these emerging identity providers that will allow for flexibility while ensuring privacy.

The key element of each of these approaches is that each features users, identity providers and services using identity information in a trusted marketplace. Such a marketplace will allow businesses to create innovative services around identity management as well as to expand services that make use of the information that consumers willingly share in a trusted environment. The government can provide significant incentives for consumer adoption of privacy protective identity management services, for example by offering government services using third party identity providers that meet a minimum level of security and privacy assurances.

As online identity becomes a more important part of the online experience, effective identity tools that ensure trust will become a prerequisite for full adoption of new innovative services. Creating a secure, privacy-enhancing identity ecosystem online will enhance trust, allow the development of innovative services, and promote the emowerment of consumers.

## VII. Small and Medium-Sized Entities and Startup Companies

In Section 7 of the NOI, the Task Force sought comment on the burdens that privacy laws and regulations can pose for small and medium sized entities ("SMEs") and startups. In this section, CDT first outlines how policies that promote consumer privacy can be written such that they will not impede the growth of these companies. Second, we discuss the burden that a federal data retention law would pose for SMEs and startups.

### A. Privacy laws do not have to impede small business development

Japan's 2003 Personal Information Protection Act provides one example of how legislation can promote privacy while preventing negative externalities like impediments to small business development. The Japanese privacy law exempts low-risk entities that handle the individual records of fewer than 5000 people during a six-month period; however, small entities that handle highly sensitive data are covered by the law.[81]

---

[80] *See Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future – NBP Public Notice #29* (Jan. 2010), *available at* http://www.cdt.org/files/pdfs/20100125_cdt- fcc_comments.pdf.

[81] *See* Martha L. Arias, *Japan's Privacy Law* (March 29, 2010*), available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2242.

American consumer privacy guidelines, regulations, or legislation could similarly exempt small entities whose activities do not put consumers at high risk.

However, even those companies exempted from coverage by privacy guidelines, regulation, or legislation, should still be encouraged to evaluate the privacy implications of their services and incorporate privacy by design long before reaching the regulatory threshold. DOC is well positioned to offer technical assistance and disseminate best practices to SMEs to ensure that privacy is built in to company policies and technologies from the outset.

### B. Data retention

The threat of draconian, federal data retention laws represents perhaps the greatest potential burden to SMEs and startup companies. Such laws, as they have been discussed by Congress[82] could plausibly require online service providers to retain vast quantities of data for law enforcement purposes, potentially imposing prohibitive costs on SME's and start ups.

Data retention is a very contentious subject from a policy perspective. In the U.S., we have achieved a kind of operational equilibrium, striking a balance between (1) law enforcement's legitimate need to investigate and prosecute crimes against children carried out or facilitated by the Internet; (2) end-users' legitimate privacy expectations and the democratic ideals of anonymous and free speech; and (3) costs of retention to Internet Service Providers ("ISPs") and online service providers ("OSPs"), costs that ultimately get passed onto consumers and, if these costs were to become onerous, could have the effect of stifling innovation and creativity on the Internet. Actions that put this balance at risk may have detrimental effects on the development of the Internet and online commerce.[83]

---

[82] For example, the Congressional mandate creating the Online Safety and Technology Working Group ("OSTWG") called for the committee to evaluate the "practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children." OSTWG released its final report on June 4, 2010, but the committee could not reach an agreement about data retention recommendations and called for continuing investigation on the issue. *See e.g.,* Broadband Data Improvement Act, Pub. L. No. 110-385, § 214, 122 Stat. 4096 (200 (to be codified at 15 U.S.C. § 6554) *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ385.110.pdf; Emma Llanso, *Keeping Kids Safe Online Report Highlights Usual Suspects: Education, Parental Empowerment* (June 4, 2010), *available at* http://www.cdt.org/blogs/emma-llanso/keeping-kids-safe-online-report-highlights-usual-suspects-education-parental-empow.

[83] Europe's attempt at data retention requirements, known as the EU Data Retention Directive, has faced implementation and constitutional challenges. The directive mandates that telecommunications service providers retain for two years detailed data on customers' activities, including phone calls and emails exchanged. In October 2009, the Romanian Constitutional Court found that the directive was inconsistent with Article 8 of the European Convention on Human Rights. In March of 2010, the German Constitutional Court held that the directive violates the right to privacy guaranteed by the German Constitution. And in May 2010, a decision by the Irish High Court made way for an Irish advocacy group to challenge the law in front of the European Court of Justice. *See e.g.,* Eddan Katz, The Beginning of the End of Data Retention (March 10, 2010) *available at* http://www.eff.org/deeplinks/2010/03/beginning-end-data-retention; Irish Court Allows Data Retention Law to be Challenged in ECJ (May 19, 2010), *available at* http://www.edri.org/edrigram/number8.10/data-retention-ireland-ecj.

Beyond privacy and free speech concerns raised by the retention itself, data retention mandates would raise serious questions about whether such retention is technically feasible and who would bear the costs of such retention. A mandate that ISPs retain IP address allocations would impose significant costs on those providers. A mandate that the other end of Internet communications – the web-based and other servers and services that citizens visit and use (provided by OSPs) – retain IP addresses and other information would in many cases be an overwhelming and extraordinarily costly burden – and would certainly lead to the reduction in content and services available on the Internet. This would in turn raise serious constitutional concerns.

As the Commerce Department weighs the potential burdens of greater privacy regulation for SMEs and startups, it should recognize that privacy protections – such as data minimization and reduced data retention periods – can actually free up company resources and promote the success of these enterprises.

## VIII. Government access to electronic communications data

In addition to the need for federal baseline legislation setting privacy rules for commercial uses of consumer information, laws on government access to communications data should also be updated, clarified and strengthened. In particular, the Electronic Communications Privacy Act ("ECPA"), drafted nearly a quarter century ago, needs to be reformed to keep up with advances in technology. Amending ECPA to provide clear, reliable rules and better protect privacy (while also preserving law enforcement access) would encourage the growth of new communications services and reflect consumer expectations.

### A. Changes in technology have outpaced ECPA

ECPA specifies standards for law enforcement access to electronic communications and associated data. ECPA was a forward-looking statute when enacted in 1986. Since then, however, technology has advanced dramatically while ECPA's privacy protections have received no corresponding update.

Congress adopted ECPA in order to provide sound footing for investment and innovation. In 1986, the fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. The stated goal for ECPA was twofold: to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement,"[84] and to support the development and use of these new technologies and services.[85] Congress recognized that consumers

[84] *See* House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).

[85] *See* S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").

would not trust new technologies if the privacy of those using them was not protected.[86]

ECPA was written to reflect the technology of 1986. Its rules are based on distinctions that are today illogical and unnecessary. ECPA does not clearly address certain sensitive information in widespread use today, such as mobile location data, the significance of which was not appreciated in 1986 when the cellular industry was in its infancy. Accordingly, the statute is now a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies. Examples of common services inadequately protected by ECPA include –

- **Email**: Because of the importance of email and the unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. For many people, much of that email is stored on the computers of network service providers.[87] However, ECPA provides only weak protection for stored email that is more than 180 days old, allowing governmental access without a warrant. The Justice Department argues that email loses the protection of the warrant the instant the recipient opens it.

- **Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based applications of great convenience and value. This location data can be intercepted in real-time, and is often stored in easily accessible logs. Location data can reveal a person's movements, from which inferences can be drawn about activities and associations. ECPA does not clearly specify a standard for law enforcement access to location information. Government agents have been obtaining location data without a warrant, and the courts have issued a series of conflicting decisions, leaving service providers uncertain of their legal obligations.[88]

- **Cloud computing**: Increasingly, businesses and individuals are storing data "in the cloud," with potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate. Under ECPA, material stored in the cloud may be accessible to the governmental without a warrant, no matter how current or sensitive the data is. ECPA needs to clarify that data stored and processed in the cloud has the same protections and standards for law enforcement access as data stored locally.

- **Social networking:** Hundreds of millions of people, including nearly half of

---

[86] *Id.*; H.R. Rep. No. 99-647, at 19 (1986).

[87] For example, Google's Gmail service offers more than seven gigabytes of free storage space. *See* Google, *Google Storage*, *available at* http://mail.google.com/support/bin/answer.py?hl=en&answer=39567 (visited Mar. 30, 2010). Google also encourages its users not to throw messages away. *See* Google, *Getting Started with Gmail*, *available at* http://mail.google.com/mail/help/intl/en/start.html (visited March 30, 2010) ("Don't waste time deleting . . . [T]he typical user can go years without deleting a single message.").

[88] *See* Michael Isikoff, *The Snitch in Your Pocket*, Newsweek (February 19, 2010), *available at* http://www.newsweek.com/id/182403.

all Americans over the age of 12, now use social media services to share information with friends and as an alternative platform for private communications.[89] Even when private records, photos and other materials are shared only with a couple of friends, ECPA may provide only weak protection, allowing governmental access without a warrant.

This legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about the privacy and security of their data in response to an access request from law enforcement. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected.

### B. Outdated standards are detrimental to businesses and consumers

American tech firms are global leaders in the digital communications industry. Breakthroughs like cloud computing and location-based services are key drivers of innovation and major market opportunities for U.S. companies. Continued growth in these areas, however, depends upon customer trust. Companies must have confidence that service providers will keep proprietary information private, and consumers must have confidence that service providers will keep personal information private.[90] Yet while service providers can afford strong privacy protection against hackers and marketers, and can promise clients that they won't use or disclose private information for their own purposes, service providers cannot promise their clients privacy from overbroad information demands from the U.S. government.

Uncertainty about the privacy afforded personal information from government snooping can hold back consumer use of emerging technologies. Consumers cite privacy concerns as a top reason for declining to adopt location-based services, including fear of being tracked by government.[91] A 2009 Microsoft study found that more than 90 percent of the general population and senior business leaders were concerned about privacy and access when it came to storing personal data in the cloud,[92] and a 2008 Pew study found that 64 percent of American Internet users are concerned about cloud computing companies turning over their files to law enforcement.[93] Moreover, cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to permissive U.S. laws giving the government access to huge quantities of information

---

[89] Arbitron, *Use of Social Media Explodes - Almost Half of Americans Have Profiles* (April 8, 2010), *available at* http://arbitron.mediaroom.com/index.php?s=43&item=682.

[90] Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Books and on the Ground*, Stanford Law Review, Vol. 63 (2010), Pp. 19-22, *available at* http://ssrn.com/abstract=1568385.

[91] *See* Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (February 2010), Pp 18, *available at* http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[92] *See* Penn, Schoen and Berland, *Cloud Computing Flash Poll – Fact Sheet,* Microsoft, *available at* http://www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc.

[93] *See* Pew Internet & American Life Project,*Use of Cloud Computing Applications and Services*, (September 12, 2008), p. 7, *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

with little judicial oversight.[94] Without stronger legal privacy protection, the reluctance of consumers and businesses to use new communications services may cause American companies to miss out on the productivity gains and new revenue sources that broader adoption of these services would offer.

ECPA's datedness also causes problems from a business operations standpoint. Companies offer services like email and data storage for free to millions of consumers, routinely using automated tools to scan users' communications to deliver relevant advertising, enhance security and reduce spam.[95] Under ECPA, and contrary to the expectations of most users, these normal business functions can significantly weaken the protections of those private communications from government access. Advertising-based services have driven the growth of the Internet; to use them, consumers should not have to sacrifice protection against governmental intrusion. Nor should consumers lose that privacy because service providers are undertaking security measures. To the contrary, the interests of service providers and consumers would be better served through policies that enable providers to monitor their networks for routine business purposes, such as to prevent attacks, without a corresponding loss of consumer privacy protection from government access.

The lack of straightforward, consistent rules makes ECPA difficult for courts and government investigators to apply.[96] Businesses likewise face substantial costs in seeking to comply with the data requests from law enforcement. ECPA's arbitrary distinctions and complexity slow providers' review of the massive volume of data requests they receive from government agencies each year. ECPA's uncertainty contributes to broad government requests of unclear legality, spurring large service providers to occasionally seek clarity from the courts; but the costs of litigation are a barrier for small- and medium-sized businesses.[97] Meanwhile, when service providers make incorrect decisions based on ECPA's uncertainty, the providers may incur liability and consequently be subject to a civil suit.[98] All of this imposes unnecessary costs and discourages innovation.

So long as the law on government access to digital communications remains hopelessly in dispute, user privacy is threatened, the trust relationship between online service providers and their clients is undermined, and businesses are needlessly subjected to inefficiency and risk. The solution is a clear set of rules for law enforcement access that

---

[94] *See* Jeffery Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, Marketspace, (March 20, 2009), p. 38, *available at* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

[95] *See* Google, *More on Gmail and privacy*, *available at* http://mail.google.com/mail/help/about_privacy.html#scanning_email.

[96] *See In re Sealed Case*, 310 F.3d 717, 743-744 (FISA Ct. Rev. 2002). The FISA Court notes the rules set forth in previous judicial decisions were "very difficult… to administer."

[97] *See* Harley Geiger, *Government Drops Warrantless Email Search Case, Highlighting Need for Reform*, Center for Democracy & Technology (Apr. 19, 2010), *available at* http://www.cdt.org/blogs/harley-geiger/government-drops-warrantless-email-search-case-highlighting-need-reform.

[98] *See* Statement of Al Gidari, before the House Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, *Hearing on Electronic Communications Privacy Act Reform* (May 5, 2010), pp. 3-4, *available at* http://judiciary.house.gov/hearings/pdf/Gidari100505.pdf.

will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

### C. The Digital Due Process Coalition

For nearly three years, CDT has engaged privacy advocates, legal scholars, and major Internet and communications service providers in a dialogue to explore how ECPA applies to new services and technologies. Earlier this year, those discussions reached a milestone when a diverse coalition developed consensus around a core set of principles for updating ECPA. The principles are open for signature and new entities are continuing to endorse them. The Digital Due Process coalition includes AT&T, Google, Microsoft, eBay, Intel, AOL, the ACLU, the Electronic Frontier Foundation, FreedomWorks, Americans for Tax Reform, and the Competitive Enterprise Institute, among others.[99]

Rather than attempt a full rewrite of ECPA, the Digital Due Process coalition has focused its reform principles just on the most important issues – those that are arising daily under the current law: access to email and other private communications stored in the cloud, access to location information, and the use of subpoenas to obtain transactional data. The principles would not change, and are subject to, the current definitions, exceptions, immunities and permissions in ECPA. The coalition's four principles for reforming ECPA are as follows:

- First, the government should obtain a search warrant based on probable cause before it can compel a service provider to disclose user communications that are not readily accessible to the public. This principle would apply to private content in the Internet "cloud" the same safeguards that the Constitution has traditionally provided to the physical files we store in our homes.
- Second, the government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.
- Third, before obtaining transactional data in real-time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation. This principle would establish meaningful judicial review of surveillance requests for this data, whereas current law gives judges no role in assessing the basis for the government request.
- Fourth, before obtaining transactional data about multiple unidentified users of communications or other online services, the government should first demonstrate to a court that the data is needed for its criminal investigation. This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than seeking the records of specific individuals that are

[99] For a more in depth-analysis of the need for ECPA reform and the nexus of reform and commerce, please see the comments of the Digital Due Process coalition in response to this NOI. *See* Comments of Digital Due Process, *In the Matter of Information Privacy and Innovation in the Internet Economy* (June 14, 2010).

relevant to an investigation. For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.

These principles would clarify and simplify the law for service providers, consumers and the government. The principles would not alter the exceptions for emergency disclosures and were designed to have no effect on disclosures relating to child pornography, cybersecurity, intelligence surveillance or information that the user chooses to make public. At the same time, the principles would enable companies to offer users greater assurance that their communications data is protected. The principles would bring consistency to ECPA that would reduce time and costs for companies complying with law enforcement requests.

Congress enacted the Electronic Communications Privacy Act to foster new communications technologies by giving users confidence that their privacy would be respected. ECPA helped further the growth of the Internet and proved monumentally important to the U.S. economy. Now, technology is again leaping ahead while antiquated laws hold the industry back.

The Obama Administration should take bold steps to build public trust in emerging communications technologies. The right policy will help American companies secure their dominance in the marketplace, while failure to update the law risks surrendering American jobs to foreign competitors. The Digital Due Process principles are a commonsense approach to reform that reflects the consensus of numerous major online service providers and thought leaders spanning the political spectrum. We urge the Obama Administration to maintain a dialogue with the Digital Due Process coalition and to support changes that would realize ECPA's goal of promoting digital innovation and growth.

## IX. The Role for Government/ Commerce Department

Throughout these comments, we have discussed how the Commerce Department and the federal government more generally can promote innovation through the promotion of privacy-protective practices, regulations, and legislation. Below, we list some of these recommendations.

- The Commerce Department should endorse a modern, comprehensive set of FIPs and recommend these principles to policymakers as the best available basis for federal legislation, executive branch decisions, regulatory actions, agency rules, and self-regulatory guidelines.

- The Administration should support baseline consumer privacy legislation that clarifies the general rules for all parties while maintaining the important protections provided by existing, sectoral legislation. Simple, flexible legislation would protect consumers from inappropriate collection and use of their personal information while enabling legitimate business use to promote economic and

social value. In principle, such legislation would codify the fundamentals of FIPs. Such legislation should exempt entities that handle small quantities of non-sensitive consumer data. Finally, any preemption in such a law needs to be carefully crafted and narrowly tailored to the specific measures that the federal government enacts. Federal legislation should not take the unusual step of preempting state common law or general consumer protection law.

- The federal government should support reform of ECPA to keep up with advances in technology. Amending ECPA to provide clear, reliable rules and better protect privacy (while also preserving law enforcement access) would encourage the growth of new communications services and reflect consumer expectations.

- The Commerce Department should oppose overly draconian federal data retention laws, which represent perhaps the greatest potential burden to SMEs and startup companies. Such laws could plausibly require online service providers to retain vast quantities of data for law enforcement purposes, potentially imposing prohibitive costs on SME's and startups.

- The federal government should commit itself to incorporating Privacy by Design into its operations and promoting Privacy Enhancing Technologies as part of its open government initiative as well as part of day-to-day government operations; it should require that companies offer innovative new technologies to protect privacy in order to gain the government as a client.

- The Commerce Department should encourage American companies to incorporate Privacy by Design into their practices and provide technical assistance to SMEs. The Commerce Department should explore the establishment of benchmarks and metrics for evaluating company privacy practices and conduct a study on the specific topic of developing performance standards on privacy.

- The Commerce Department should explore the applicability of FCRA to identity providers and investigate the potential of an FDIC-like regime for encouraging good practices amongst identity providers. The Commerce Department, in conjunction with NIST, should in the meantime draft general best practices for identity management services and for their implementation by government and businesses.

- The Commerce Department should consider convening a trans-Atlantic multi-stakeholder dialogue, bringing together European officials, U.S. and European companies, and civil society representatives to explore the unsettled interaction between the EU Electronic Commerce Directive and the Data Protection Directive.

- The Commerce Department should re-affirm the importance of protecting intermediaries from liability and should seek, in its various interactions with other countries, to promote strong protections for intermediaries. It should also seek to document the positive relationship between protecting intermediaries and

fostering innovation and track best practices for protecting privacy and serving other societal objectives in the context of user-generated content and promote these practices among U.S. companies. The Commerce Department should urge its counterparts around the globe to adopt laws that protect Internet intermediaries from liability for content posted by third parties as a key driver of innovation.

- The Commerce Department should document the ways that various content-based restrictions impact the ability of U.S. businesses to compete globally and should help U.S. companies develop, document, and promote best practices for responding to governmental requests to restrict information flows or assist in surveillance. It may also be appropriate for the Commerce Department to encourage companies to join multi-stakeholder collaborative efforts like the Global Network Initiative. The Commerce Department should additionally raise content-based Internet restrictions as a trade issue in bilateral and multilateral discussions, including at the WTO.

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

June 14, 2010

National Telecommunications and Information Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams:

The Centre for Information Leadership ("the Centre") appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy." The Centre commends the Department for conducting this inquiry and for the important work it has undertaken to address this critical issue.

The Centre's mission is development of sound information policy for a digital economy. It has led projects addressing numerous information privacy and security issues including privacy notices, global flows of data, accountability-based governance, development of privacy law in developing economies, and government use of private-sector data. The Centre has worked extensively with Asia Pacific Economic Cooperation ("APEC") and the Organization for Economic Cooperation and Development ("OECD") on issues of privacy and data protection. The Centre currently serves as secretariat for an international group of experts representing privacy protection agencies, civil society, academia and business that is exploring an accountability model for privacy governance.

The Centre was established in May 2001 by leadership companies and Hunton & Williams LLP. The Centre is located within the law firm of Hunton & Williams and is financially supported by approximately 40 companies. The Centre's views and the views expressed in this response are its own and do not necessarily reflect those of its member companies, the law firm of Hunton & Williams LLP, or the firm's clients. However, the organizations listed at the end of this submission have expressed their support for the Centre's recommendations contained herein.

In its response to this inquiry, the Centre offers ten recommendations and attaches supporting documents.

## Centre Recommendations

**1. The Department of Commerce should represent the United States in global privacy discussions.**

The Department of Commerce must play a lead role in representing US interests in international discussions on privacy and global data flows. Over the past decade the US the Department of Homeland Security and the Federal Trade Commission have served in that capacity. Both agencies have their appropriate role, and the Federal Trade Commission has been recognized as best qualified for accreditation to participate in international conferences of data privacy commissioners. However, the Department of Commerce is best positioned to develop and advocate for US policy that fosters economic growth; robust, innovative use of data; and protection of privacy in forums where issues related to privacy are cross-cutting with issues related to trade, outsourcing, innovation, and technology policy. The Department of Commerce has played this role effectively in the past, for example in its work at the OECD and on the EU-US Safe Harbor, and continues to do so at APEC. We urge the Department to lead engagement in other international multilateral forums and in bilateral negotiations.

The Department of Commerce should seek out our trading partners' knowledgeable, effective representatives to ensure that the appropriate privacy and data protection models are considered. It must continue conversations with data protection authorities, but also broaden those discussions to include experts in trade, industry and specialized fields such as pharmaceutical research, to ensure that policies reflect sound, creative thinking about innovation, the importance of robust global flows of data to trade and economic growth, and respect for privacy.

**2. The Department of Commerce should continue to support development of policy frameworks that will support the global flow of data.**

The Department of Commerce must continue to promote global policy frameworks that ensure the robust, accountable flow of data. The Centre believes that the Department's experience in negotiating the Safe Harbor with the European Commission and in its role in developing the APEC Privacy Framework should be brought to bear to eventually

create a global framework that facilitates the flexible, accountable flow of data. These frameworks work best when based on agreed-upon, common objectives for data protection. The Department of Commerce should lead stakeholders in a process to develop those common objectives.

**3. The government should articulate a vision for innovation and privacy in the information economy.**

The Department of Commerce must articulate a unified vision for an innovative, safe digital environment that serves an information-driven economy. Such a vision must reflect both benefits derived from the business innovation that is driven by data, including personal data, and the responsible protection and management of information. Privacy must be positioned within that overall vision, and innovative uses of information must be compatible with data practices that promote privacy.

**4. Information policy must have a home within the government.**

The executive branch must demonstrate ongoing support for this vision by establishing a non-regulatory office that coordinates information policy in the United States. The information policy office must be led and staffed by experts who understand the technology, economic interests and societal values at issue as new business models and data applications evolve. Its role should include reporting on the advantages and costs to innovation of privacy protection. This office could be situated within the Department of Commerce. While the Centre does not believe this office should have a regulatory role, the agency should coordinate with the regulatory bodies charged with oversight and enforcing private-sector laws on privacy, information security and cyber security. The agency should also coordinate with the Privacy and Civil Liberties Oversight Board, which has similar responsibilities related to the government's use of information.

**5. Both industry and government must be accountable for its use of information.**

To be innovative, organizations must be able to explore data to understand its predictive value. Today, almost all business processes begin with the question "what does the data tell us?" To encourage growth through innovative information use, industry must be empowered to explore and use data robustly and responsibly.

The flexibility to be innovative must be conditioned on the organization's accountability for the manner in which it uses, manages and protects data. Every use of information

affects privacy. To strike the appropriate balance between the value created by data use and the risk that use poses to privacy, organizations must implement privacy processes that are as dynamic as their business processes. To be successful, the innovative organization must understand the privacy risks to individuals associated with the innovative use, and stand ready to mitigate those risks.

The assumption of the responsibility for the risks associated with innovative data use, and the willingness to be responsible for those risks form the basis of an accountability approach to data protection.

The Centre, through its Galway Accountability Project, defined the five essential elements of accountability:

1. Organization commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training and education.
3. Systems for internal, ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanism for individual participation.
5. Means for remediation and external enforcement.[1]

Accountable organizations are responsible and answerable for the decisions they make about the use, management and protection of data. Accountability requires organizations to understand the risks they create for individuals by collecting and using information, and to mitigate those risks. In an environment where meaningful notice and choice become increasingly difficult to provide and exercise, accountable organizations make careful, balanced decisions about data, whether or not the individual has had an opportunity to make a choice about the use of his or her data. Accountability places the onus on organizations to be responsible about data, and relieves the individual of the burden of policing the marketplace against bad actors and

[1] The essential elements of accountability are more fully discussed in "Data Protection Accountability: The Essential Elements," October 2009, attached as Appendix A and found at http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (last visited June 2, 2010).

making choices about data that may, in the end, provide little consumer control or protection.[2]

In recent months, accountability has figured prominently in discussions about how to improve privacy and data protection.[3] Companies and policymakers are exploring how an accountability model for data protection might work in practice. What this inquiry has made clear is that accountability can only be effective for the private sector if government builds accountability into its information processes as well. The risk assessment and mitigation that lie at the heart of an accountability model must be adopted by government. While calls for such reform will likely be met with resistance, the private sector cannot be fully accountable if the federal government is not held similar requirements about the use and protection of data.[4]

**6. Federal privacy law must pre-empt state laws.**

U.S. business has repeatedly asserted that the "patchwork" of different, and often conflicting, state privacy laws impose significant burdens on companies that rely on data and data processing to run their business and power their product and service offerings. While many state legislatures have adopted innovative, effective approaches to privacy and security legislation, the nature of data use and data flows requires consistent, clear privacy law. Any federal privacy law should pre-empt state privacy laws from imposing requirements over and above those in federal legislation.

---

[2] The Safeguards Rule of the Gramm-Leach-Bliley Act provides an example of accountability that has worked well: the rule requires that companies secure their data, but leave decisions about how best to do so to the organization.

[3] Discussion held during the recent series of Federal Trade Commission Roundtables entitled "Exploring Privacy" repeatedly identified accountability as an approach to data governance in a world of increasingly complex data uses and flows. At the Asia Pacific Economic Cooperation forum, models for implementation of the APEC Privacy Framework depend upon accountability to facilitate protected cross-border data flows. "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" notes the significance and utility of the accountability principle. 02356/09/EN WP 168, December 1, 2009, published January 11, 2010, by the Article 29 Working Party. Attached as Appendix B and available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf (last visited June 2, 2010).

[4] A complete discussion of accountability can be found in "Data Protection Accountability: The Essential Elements; A Document for Discussion," Attached as Appendix A and available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf (last visited May 27, 2010).

**7. U.S. privacy policy should focus on successful privacy results rather than on procedures that do little to enhance privacy.**

The US should avoid placing procedural requirements before strategic management of information and privacy protection. A checklist approach to privacy often results in a completed checklist rather than enhance privacy. Furthermore, the resources required to comply with procedural requirements often reduce those available to manage the real privacy risks to individuals. Some jurisdictions, for example, require companies to register all databases and notify officials if the data is to be processed in a manner different from that asserted, creating significant work for lawyers but providing little protection for individuals. In the U.S., advocates, experts and businesses have repeatedly commented that the annual privacy notices required by the Gramm-Leach-Bliley Act (but reportedly read by few consumers) have done little to promote privacy. In both cases, resources invested in complying with legal requirements would be better spent on initiatives that yield appreciable privacy results.

Alternative, comprehensive approaches to data management require that considerations and requirements for privacy, information security, and cyber security (as well as protection of intellectual property, trade secrets and evidentiary data) be part of an organization's overall data collection, storage, use and retention strategy. Governance approaches such as privacy by design, combined with accountability offer more effective information policy governance.[5]

**8. Preventing harm must remain a significant feature of the U.S. approach to privacy.**

Prevention of harm has been a feature of US privacy law since the enactment of the Fair Credit Reporting Act. Prevention of harm is a fundamental principle of the APEC Privacy Framework that supports setting priorities about data protection and enforcement based on the extent to which data practices may expose individuals to potential harm. The harm-based approach to privacy protection has come under criticism as focusing exclusively on financial and physical harm. But the potential for harm extends beyond the physical and financial to include the negative social impact harm to reputation, for example -- that can result from the misuse of data. All three kinds of harm – physical, financial and social – should form the basis for setting protection and enforcement

[5] Cavoukian, A., Abrams, M. and Taylor, S., "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices," Office of the Information Privacy Commissioner, Ontario, November 2009, attached as Appendix C, and found at http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf (last visited June 2, 2010).

priorities. It will be important to carefully define the contours of social harm to provide businesses with a clear sense of their responsibility and the limits of their liability for such harm. [6]

**9. The Department of Commerce should undertake an initiative to develop privacy norms that apply to data analytics.**

Data analytics drive market innovation but also raise risks to individual privacy. Current data privacy guidance does not anticipate the power and speed of data analytics. The Centre urges the Department of Commerce to lead a process to set norms for analytics that encourage innovation, but create baseline guidance about their use in a manner that respects individual privacy. In developing those norms, it will be necessary to bear in mind the distinct differences in attitudes toward analytics that exist between the United States and its trading partners. Moreover, it will be important to recognize that no bright line has been identified between what information about an individual's behavior is and is not private.

Information and the ability to subject data to intensive analysis are essential to innovation and economic growth. With the freedom to understand the data comes the responsibility to use information in a judicious, disciplined fashion.

**10. Privacy oversight and enforcement are best carried out by regulatory agencies with authority over specified industry sectors.**

Any approach to privacy governance should preserve the current system whereby privacy is overseen by an industry sector's existing regulatory agency. Under such a model privacy enforcement benefits from the agency's intimate understanding of the challenges and opportunities companies face, the new business models and technologies companies adopt, the ways in which data is used and raises risks to privacy, and the overarching regulatory structure that governs the industry and that may impact the effectiveness of regulation or guidance and the opportunity for innovation and growth. Maintaining this system would preserve the value derived from familiarity with the way privacy governance works within an industry sector and within individual companies. In keeping with this model, the Federal Trade Commission should continue to oversee consumer privacy protection in general. As noted in Recommendation 3 of this submission, the Centre does not recommend creation of a

[6] While notions of physical and financial harm are well established, the concept of social harm requires further exploration and definition. Such an inquiry is beyond the scope of this submission.

single privacy regulator, however it does believe there is a role for an office that would coordinate privacy, information security and privacy security policy in the private sector. That office would work with regulatory bodies to ensure that new technologies and business processes are reviewed and understood, and that policy guidance is applied consistently and appropriately across all sectors.

CONCLUSION

The Centre appreciates this opportunity to participate in the Department of Commerce's work to encourage data-driven innovation and effective privacy protection for individuals. We hope that the Department will look to the Centre as a resource, and are available to provide further information or to elaborate on the recommendation above. Please direct any questions to Martin Abrams at mabrams@hunton.com or Paula Bruening at pbruening@hunton.com.

Yours sincerely,

Martin E. Abrams
Executive Director

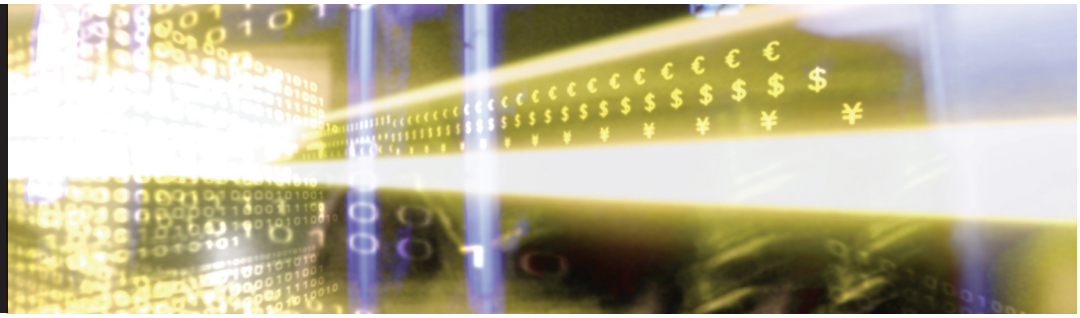
Paula J. Bruening
Deputy Executive Director

The following lists organizations that support the above recommendations submitted by the Centre for Information Policy Leadership.

Acxiom
Experian
Google
Hewlett-Packard Company
IBM
Intel
Microsoft
Oracle
salesforce.com

# APPENDIX A

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP



# Data Protection Accountability: The Essential Elements
# A Document for Discussion
# October 2009

Prepared by the Centre for Information Policy Leadership
as Secretariat to the Galway Project

**Data Protection Accountability: The Essential Elements**
**A Document for Discussion**

## Preface

**Martin Abrams**
**Executive Director**
**Centre for Information Policy Leadership**

Innovations in technology; rapid increases in data collection, analysis and use; and the global flow and access to data have made an unprecedented array of products, resources and services available to consumers. These developments, however, in no way diminish an individual's right to the secure, protected and appropriate collection and use of their information.

The manner in which those protections are provided is often challenged by the dynamic, increasingly international environment for information. The global flow of data tests existing notions of jurisdiction and cross-border co-operation. How can companies and regulators support movement of data while providing the protections guaranteed to the individual?

Accountability, a concept first established in data protection by the Organisation for Economic Co-operation and Development ("OECD"), may provide an improved approach to transborder data governance that encourages robust data flows and provides for the protection and responsible use of information, wherever it is processed. But the practical aspects of accountability, and how it can be used to address the protection of cross-border information transfers, have not been clearly articulated.

- What will be expected of companies in an accountability system?
- How will enforcement agencies monitor and measure accountability?
- How can the protection of individuals be ensured?

The Centre for Information Policy Leadership at Hunton & Williams LLP was privileged to assemble a group of international experts from government, industry and academia to consider how an accountability-based system might be designed.[1] The experts met twice to define the essential elements of accountability, examine issues raised by the adoption of the approach and propose additional work required to facilitate establishment of accountability as a practical and credible mechanism for information governance. This report, guided by a drafting committee and reviewed by the group of experts, reflects the results of those deliberations.

[1] The group of experts is listed in the Appendix.

While this paper is focused on accountability as a mechanism for global governance of data, the issue of how accountability relates to the general oversight of privacy was raised during our discussions. It may be that accountability principles can address both international as well as domestic protection of information. Our discussion recognised that the concepts of accountability that can support an improved approach already are reflected in long-standing principles of fair information practices and are inherent in current governance in Europe, Asia and North America. Making accountability a reality requires that businesses apply those concepts so that their management of information is both safe and productive. Our talks further suggested that the growing complexity of data collection and use requires that much of the burden for protecting data must shift from the individual to the organisation.

Much of what is written about accountability in this paper can be accomplished by reinterpreting existing law. It is our hope that this paper will both chart the course forward for establishing accountability-based protection and motivate stakeholders to take the important steps to do so.

The Centre is indebted to the experts who participated in this effort for generously giving of their time and expertise, and most especially to the Office of the Data Protection Commissioner of Ireland for hosting our meetings and providing us with wise guidance. While this report reflects the results of their deliberations, the Centre alone is responsible for any errors in this paper.

**Executive Summary**

Accountability is a well-established principle of data protection. The principle of accountability is found in known guidance such as the OECD Guidelines[2]; in the laws of the European Union ("EU"), the EU member states, Canada and the United States; and in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. Despite its repeated recognition as a critical component of effective data protection, how accountability is demonstrated or measured has not been clearly articulated. This paper represents the results of the Galway Project — an effort initiated in January 2009 by an international group of experts from government, industry and academia to define the essential elements of accountability and consider how an accountability approach to information privacy protection would work in practice.

Accountability does not redefine privacy, nor does it replace existing law or regulation; accountable organisations must comply with existing applicable law. But accountability shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both the ability and the responsibility to

[2] Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

determine appropriate, effective measures to reach those goals. As the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability to make decisions to control the use and sharing of information through active choice, accountability requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised external criteria, and implements mechanisms to ensure responsible decision-making about the management and protection of data. The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

3. **Systems for internal, ongoing oversight and assurance reviews and external verification.**

4. **Transparency and mechanisms for individual participation.**

5. **Means for remediation and external enforcement.**

While many aspects of the essential elements are already established in law, self-regulation and corporate practices, some issues remain to be resolved to encourage robust adoption of an accountability approach. Policymakers and stakeholders should address questions about how accountability would work with existing legal regimes, and whether reinterpretation or amendment of existing laws might be required to make it possible to hold organisations accountable. Third-party accountability programmes have been recognised as useful in supplementing the work of government agencies. As they may play an important part in the administration of this approach, it will be necessary to clearly describe the contours of their role and the criteria by which their credibility will be assessed. Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. For the approach to work effectively, stakeholders must articulate the way in which the credibility of those programmes is established and tested. Finally, small- and medium-sized enterprises that wish to demonstrate accountability will face specific challenges that must be addressed.

While additional inquiry is needed before adoption of an accountability-based approach can be realised, its promise for international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates — robust transfer and use of data in a fashion that is responsible and protected.

## Introduction

The global flow of data drives today's information economy. Innovation, efficiency and service depend on rapid and reliable access to data, irrespective of its location. Digital technologies collect and store data in ways never before imagined, and information and telecommunications networks have evolved to provide seamless, low-cost access to data around the world.

As a result consumers have access to an unprecedented array of personalised products and services. While previously service hours ended at 5:00 p.m., the Internet enables individuals to access customer service in the middle of the night by phoning a local number that connects them to a call centre a continent away. Today, on a single server, a company can manage its email and business records for offices located in a dozen nations; travelers can rely on their debit and credit cards wherever they go; and individuals can use the Internet to download information from around the world without ever leaving their homes.

Indeed, with the increasingly global nature of data flows and the remote storage and processing of data in the "cloud", geography and national boundaries will impose few limitations on where data can be transferred but will present more practical challenges for administering and supervising global businesses.

In this environment, individuals maintain the right to the secure and protected processing and storage of their data that does not compromise their privacy. Protection must be sufficiently flexible to allow for rapidly changing technologies, business processes and consumer demand. Regulators must be equipped to articulate clear requirements for protection, educate companies and citizens, and monitor compliance in an environment in which data processing increasingly occurs outside the practical reach of most regulators, if not their legal jurisdiction.

Currently, global data flows are governed by law and guidance, which are enacted and enforced by individual countries or through regionally adopted directives or agreed-upon principles. The EU Data Protection Directive and implementing laws of member states, for example, govern the transfer of data from the European Union. The Safeguards Rule[3] imposes legal obligations on U.S. organisations to ensure that data is properly secured, wherever it is transferred or processed. And yet global data flows often challenge the way in which we have traditionally approached information protection. Daniel Weitzner and colleagues have written that information protection policy has long relied on attempts to keep information from " 'escaping' from beyond appropriate boundaries".[4] This approach is plainly inadequate in a highly connected environment in which anyone armed with a cell phone or laptop has at his or her fingertips unprecedented processing power, as well

[3] Under the Gramm-Leach-Bliley Act, the Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information.

[4] Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Jay Sussman, "Information Accountability," *Communications of the ACM*, June 2008, at 82.

as the practical ability to collect, aggregate, transfer and use personal data around the world — and in an environment in which those capabilities are growing exponentially.

Weitzner and his colleagues lead a growing multinational call for an alternative approach to securing and governing personal data based on *accountability*. An accountability-based approach to data protection requires that organisations that collect, process or otherwise use personal data take responsibility for its protection and appropriate use beyond mere legal requirements, and are accountable for any misuse of the information that is in their care.

Adoption of an accountability-based approach to governance of privacy and information in global data flows raises significant questions for business, government and individuals.

Businesses express concerns about what might be expected of them in an accountability system, how their efforts to meet those expectations will be measured and how the rules related to accountability will be defined and enforced. Privacy enforcement agencies ask how accountability might work under local law. How do enforcement agencies measure an organisation's willingness and capacity to protect information when it is no longer in the privacy protection agency's jurisdiction? How does the agency work with and trust agencies in other jurisdictions? Consumer advocates worry that accountability will lessen the individual's ability to make his own determination about appropriate use of information pertaining to him.

The Centre for Information Policy Leadership, through a process facilitated by the Office of the Irish Data Protection Commissioner, convened experts to define the essential elements of accountability; to explore the questions raised by government, business and consumers related to adoption of an accountability approach; and to suggest additional work necessary to establish accountability as a trusted mechanism for information governance.

A small group of experts met initially in January 2009 to define the contours of the inquiry and identify existing research and legal precedents involving accountability. That meeting led to a draft paper that was presented to a larger gathering in April that included data protection experts drawn from government, industry and academia from ten countries. The April meeting identified a drafting committee that oversaw the Centre staff as they prepared this document, which was then circulated for comment among all of the participants. This paper reflects the results of that process.

## Accountability in Current Guidance

Accountability as a principle of data protection is not new. It was established in 1980 in the OECD Guidelines[5] and plays an increasingly important and visible role in privacy

[5] See, Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

governance. The Accountability Principle places responsibility on organisations as data controllers "for complying with measures that give effect" to all of the OECD principles.

Accountability is also fundamental to privacy protection in the European Union. While not explicitly stated in the Directive, numerous provisions require that organisations implement processes that assess how much data to collect, whether the data may be appropriate for a specified purpose and the level of protection necessary to ensure that it is secure. Accountability also has featured more prominently in data governance in Europe as binding corporate rules have served as a mechanism to ensure the trusted transfer of personal data outside the EU.

The Spanish Data Protection Agency's February 2009 Joint Proposal for an International Privacy Standard includes an accountability principle that establishes a basis for data transfers based on an organisation's demonstration that it is responsible.[6]

Accountability is also the first principle in Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), requiring that Canadian organisations put into effect the full complement of PIPEDA principles, whether the data are processed by the organisation or outside vendors, or within or outside Canada. In doing so, the accountability principle of PIPEDA establishes in law a governance mechanism for transborder data transfers.[7]

In the United States, the Federal Trade Commission ("FTC") applies to general commerce the Safeguards Rule of the Gramm-Leach-Bliley Act ("GLBA") — an accountability-based law that places obligations on a financial services organisation to ensure personal information is secured, but that does not explicitly explain how those obligations should be met.

The Asia-Pacific Economic Cooperation ("APEC") Privacy Framework includes accountability as an explicit principle,[8] basing it on the OECD language and applying it to data transfers beyond national borders. The Framework states, "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above." The Framework specifically requires such accountability "when personal information is to be transferred to another person or organisation, whether domestically or internationally."

---

[6] "Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Information," version 2.3, 24 February 2009.

[7] This governance was explicitly described in a 2009 publication of the Office of the Privacy Commissioner of Canada, "Processing Personal Data Across Borders: Guidelines". In PIPEDA, accountability is an overarching principle that applies to protection and management of data, whether it is maintained and processed domestically or transferred outside Canadian borders for storage and processing.

[8] For more information about the APEC Privacy Framework and a full articulation of the principles, see <.<http://www.apec.org_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html#>.

Despite the inclusion of accountability in many data protection regimes, it is often unclear how companies demonstrate accountability for purposes of cross-border data transfers, how regulators measure it or why individuals should trust it.

**What is an Accountability-based Approach?**

An accountability-based approach to data governance is characterised by its focus on setting privacy-protection goals for organisations based on criteria established in current public policy and on allowing organisations discretion in determining appropriate measures to reach those goals. An accountability approach enables organisations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customers.

An accountability-based approach to privacy protection offers immediate advantages to individuals, institutions and regulators alike, because it recognises and is adaptable to the rapid increases in data flows.

- It will help bridge approaches across disparate regulatory systems, by allowing countries to pursue common data protection objectives through very different — but equally reliable — means. This helps to facilitate the many benefits of allowing data to move across borders, and to assure individuals a common level of data protection — even if achieved through a variety of means — irrespective of where their information is located.

- It will also heighten the confidence of individuals that their data will be protected wherever it is located and minimise their concerns about jurisdiction or local legal protections.

- It will raise the quality of data protection, by allowing use of tools that best respond to specific risks and facilitating the rapid updating of those tools to respond quickly to new business models and emerging technologies. An accountability approach requires organisations not only to take responsibility for the data they handle but also to have the ability to demonstrate that they have the systems, policies, training and other practices in place to do so.

- Allowing for greater flexibility will enable organisations to more effectively conserve scarce resources allocated to privacy protection. While it is essential that an accountable organisation complies with rules, resources devoted to fulfilling requirements such as notification of data protection authorities are not available for other, often more effective, protection measures. Accountability directs scarce resources towards mechanisms that most effectively provide protection for data. Organisations will adopt the tools best suited to guarantee that protections focus on reaching substantive privacy outcomes — measurable information protection goals — and to demonstrate their ability to achieve them.

Accountability does not redefine privacy, nor does it replace existing law or regulation. Accountable organisations must comply with existing applicable law, and legal mechanisms to achieve privacy goals will continue to be the concern of both regulators and organisations. However, an accountability approach shifts the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified objectives.

Accountability does not replace principles of individual participation and consent that have been well established in fair information practices.[9] In many cases, consumer consent to uses of data remains essential to an organisation's decisions about data management. However, in some instances obtaining such consent may be impossible or highly impractical, and an accountability approach requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent.

## How Accountability Differs from Current Approaches

Accountability is designed to provide robust protections for data while avoiding aspects of current data protection regimes that may be of limited effect or that may burden organisations without yielding commensurate benefits. Accountability allows the organisation greater flexibility to adapt its data practices to serve emerging business models and to meet consumer demand. In exchange, it requires that the organisation commit to and demonstrate its adoption of responsible policies and its implementation of systems to ensure those policies are carried out in a fashion that protects information and the individuals to which it pertains. Accountability requires an organisation to remain accountable no matter where the information is processed. Accountability relies less on

[9] Consent is found in the OECD Guidelines principle of Use Limitation, which states: "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."

The principle of individual participation is also found in the OECD Guidelines, which state:

"An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

- within a reasonable time;
- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended".

the rules that exist where the data is processed and more where the obligation is first established.[10]

Accountability relies less on specific rules but instead requires that organisations adopt policies that align with external criteria found in law — generally accepted principles or industry best practices — and foster a level of data protection commensurate with the risks to individuals raised by loss or inappropriate use of data. The accountable organisation complies with applicable law and then takes the further step to implement a programme that ensures the privacy and protection of data based on an assessment of the risks to individuals raised by its use. These risks should be assessed and measured based on guidance from regulators, advocates, individuals and other members of industry. Ultimately, regulators are responsible for ensuring that the risks to the data have been managed appropriately.

While the individual continues to play an important role in protecting his or her information, accountability shifts the primary responsibility for data protection from the individual to the organisation collecting and using data. Much of United States law, for example, is based on disclosure of the organisation's privacy policy, notification of individuals and obtaining their consent to specific uses of data. This approach is designed to enhance individual control over the manner in which data is used. Individuals are vested with responsibility for determining the manner in which their data is used and shared; organisations are obligated to provide the individual with sufficient information on which to base an informed choice.

In the U.S. the Federal Trade Commission is authorised to bring an enforcement action based on the organisation's notice when an organisation acts in an unfair or deceptive manner with respect to its privacy practices. In the absence of, and in some cases even with, an overarching privacy law, the individual is charged with policing the marketplace for privacy, by familiarising him- or herself with every organisation's policy and making a decision based on that information whether or not the organisation is trustworthy and using data in an appropriate manner.

Accountability does not displace the individual's ability to assert his rights, but relieves him of much of the burden of policing the marketplace for enterprises using data irresponsibly. Faced with rapid advances in data analytics and increasingly complex technologies, business models and vendor relationships, consumers find it increasingly difficult to make well-informed privacy decisions, even when they can access privacy policies. Accountability demands responsible, appropriate data use whether or not a consumer has consented to one particular use or another.

Accountability does not wait for a system failure; rather, it requires that organisations be prepared to demonstrate upon request by the proper authorities that it is securing and protecting data in accordance with the essential elements.

[10] When, however, information security rules where data are processed are stronger than where the security obligation was incurred, they may indeed apply.

Enforcement of binding corporate rules ("BCRs") or the cross-border privacy rules as defined in APEC perhaps most closely approximate an accountability approach to information management and protection. BCRs, which are more fully developed, provide a legal basis for international data flows within a corporation or a group of organisations when other options are either impracticable or of limited utility. BCRs are a set of rules, backed by an implementation strategy, adopted within a company or corporate group that provides legally binding protections for data processing within the company or group. While the Directive and national laws that implement it rely on adequacy of laws and enforcement in a particular legal jurisdiction outside the EU, BCRs allow companies to write rules for data transfer that are linked to the laws where data was collected rather than look to compliance with the law of a particular geographic location where the data may be processed. Data authorities examine whether an organisation's binding rules export local European law with the data, and can determine whether its data practices and protections can be trusted to put those rules into effect — that it has in place the procedures, policies and mechanisms necessary to meet the obligations established in the BCR and to monitor and ensure compliance.[11]

**Essential Elements of Accountability**

An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria.**

   An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices. An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by

[11] BCRs cover only governance of data originating in the European Union. They do not apply to data originating from other regions.

tasking appropriate staff with implementing the policies and overseeing those activities.

Many global organisations have established policies in accordance with accepted external criteria such as the EU Directive, OECD Guidelines or APEC Principles. These companies demonstrate high-level commitment to those policies and the internal practices that implement them by requiring their review and endorsement by members of the organisation's executive committee or board of directors.

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

   The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

   Organisations in Europe, North America and Asia-Pacific have implemented comprehensive privacy programmes that incorporate personnel training, privacy impact assessments and oversight. In some cases, organisations have automated processes and integrated responsibility for programme obligations into all levels and across all aspects of the enterprise, while responsibility for compliance, policy development and oversight remains in the privacy office.

3. **Systems for internal ongoing oversight and assurance reviews and external verification.**

   Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful — and must be subject to some form of monitoring.[12]

[12] Accountable organisations have traditionally established performance systems based on their own business culture. Successful performance systems share several characteristics:

- they are consistent with the organisation's culture and are integrated into business processes;

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.

The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution. External verification must be both trustworthy and affordable. Privacy officers may work with their audit departments to ensure that internal audits are among the tools available to oversee the organisation's data management. Organisations may also engage firms to conduct formal external audits. Seal programmes[13] in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.

**4. Transparency and mechanisms for individual participation.**

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also

---

- they assess risk across the entire data life cycle;
- they include training, decision tools and monitoring;
- they apply to outside vendors and other third parties to assure that the obligations that come with personal data are met no matter where data is processed;
- they allocate resources where the risk to individuals is greatest; and
- they are a function of an organisation's policies and commitment.

[13] Seal programmes are online third party accountability agents.

provides for those instances when it is feasible. In such cases it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

**5. Means for remediation and external enforcement.**

The organisation should establish a privacy policy that includes a means to address harm[14] to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.

The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organisation and enhance its reputation for complying with its policies and meeting its obligations to individuals.

Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organisation should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organisation recognise and respond to the legal authority exercising proper jurisdiction.

## Public Policy Issues

While many aspects of the essential elements are already well established in law, self-regulation and corporate practices, consideration of several issues could usefully assist and stimulate the robust adoption of an accountability approach. These include the following:

[14] The concept of harm can include, among other things, compromise of an individual's financial or physical well-being; embarrassment; and damage to reputation. Additional work is needed to more clearly define and describe harm as it can result from violation of privacy and inappropriate use of data.

1. **How does accountability work in currently existing legal regimes?**

   Adopting an accountability approach to global information privacy governance may require reinterpretation or amendment of existing laws to enable the use of accountability mechanisms and to make it easier and more practicable to hold organisations accountable.[15]

   It may, for example, be necessary to provide in law or regulation that organisations comply with requests to inspect or review certain privacy practices to determine whether the organisation meets the essential elements of accountability as discussed in this paper. Work may be required to provide for legal recognition of the internal rules and policies organisations adopt and the measures organisations take to be accountable.[16]

2. **What is the role of third-party accountability agents?**

   Third-party review of an organisation's practices against appropriate criteria will greatly facilitate the success of an accountability approach. Qualified, authorised accountability agents will be an important element to address resource constraints in order to make the accountability approach work in practice.

   Establishing criteria for organisations that wish to serve as accountability agents, and articulating their role and the extent of their authority, will be a key task for policymakers. It will also be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

   Finally, to be useful to organisations, the services of an accountability agent must be affordable from a financial and operations perspective. Accountability agents must be able to price their services in a manner that allows them to recover their cost and build working capital, but still ensure that services are affordable to the full range of organisations that wish to avail themselves of their resources. Certification processes should be meaningful and trustworthy.

---

[15] In its 2008 report the Australian Law Reform Commission considered the possibility that Australian law be amended to assure an accountability approach could be used to improve governance of cross-border data transfers. A number of EU countries are exploring whether amending the law could better accommodate binding corporate rules.

[16] Such amendments are suggested in the APEC Privacy Framework, which requires that organisations comply with local data protection rules, but those amendments must enable them to write cross-border privacy rules that link to the APEC Principles to govern data transfers. Paragraph 46 of the Framework commentary encourages member economies to "endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with applicable laws".

They should also be designed to limit their disruption of business operations and to safeguard the confidentiality of an organisation's data assets.

**3. How do regulators and accountability agents measure accountability?**

An accountability approach does not rely on a breach to prompt review of an organisation's information practices and protections. Accountability agents and regulators must be empowered to review organisations' internal processes in a manner that allows them to ensure meaningful oversight. Policymakers may also wish to consider the measures to be taken by organisations to test for accountability and to be sure that it is working.

While an organisation's corporate policies must be linked to external criteria in the various countries where it does business, laws may differ from jurisdiction to jurisdiction. Accountability oversight must assess an organisation's overall privacy programme and allow for resolution of those differences in company policies in a manner that furthers the intent of a range of often conflicting laws or regulations.

Policymakers need to identify a way to measure confidence in an organisation's overall privacy accountability programme — commitment, policies and performance mechanisms — to determine whether an organisation is accountable even if its policies and practices are not a one-to-one match for local law and regulation.

**4. How is the credibility of enforcement bodies and third-party accountability programmes established?**

Trusted movement of data based on accountability requires that privacy enforcement agencies rely upon the oversight of enforcement bodies in jurisdictions other than their own. Assessing accountability requires examining and judging an organisation's entire programme — a somewhat subjective analysis — so that the credibility of accountability agents is critical.[17]

Third-party accountability programmes such as seal programmes may supplement the work of government agencies. The credibility of these third parties must also be established if they are to be trusted by privacy enforcement agencies and the public. Investment in robust process and experienced, thoughtful staff will be essential to their success.

Additional work should be undertaken to determine how the credibility of these organisations is tested. It will be necessary to determine ways to ensure that accountability agents are worthy of public trust, and to develop the

[17] Work already undertaken at the OECD may be helpful in this regard. See Organisation for Economic Co-operation and Development, *Recommendations on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007).

criteria by which they can be judged. Such criteria would ideally be developed through a consultative process that includes businesses, government representatives, experts and advocates.

5. **What are the special considerations that apply to small- and medium-sized enterprises that wish to demonstrate accountability, and how can they be addressed?**

   In many cases, organisations that wish to demonstrate accountability may be small- and medium-sized enterprises, ("SMEs") for which privacy protection resources may be limited. Consideration must be given to the special needs of these organisations and the impact that fulfilling the essential element may have on these enterprises. It may be that aspects of the essential elements will need to be tailored or adapted for smaller organisations in a manner that makes them more workable but does not dilute them.

   Assessment requirements provide one example. While assessments may well serve the same function for SMEs as they do for larger organisations, such assessments may pose an undue burden on smaller enterprises with scarce resources. The nature of the assessment and the parties that may carry them out may differ for such entities, depending on the nature and sensitivity of the data in question. It will be important to examine how an SME might fulfill the assessment requirement without compromising itself financially. Similar questions of scalability as they apply to these organisations will need to be considered and resolved.

## Conclusion

Dramatic advances in the speed, volume and complexity of data flows across national borders challenge existing models of data protection. In the face of such complexity and rapid change, data protection must be robust, yet flexible. Privacy can no longer be guaranteed either through privacy notices and consent opportunities for individuals, or through direct regulatory oversight.

An accountability-based approach to data protection helps to address these concerns. It requires that organisations that collect, process or otherwise use personal information take responsibility for its protection and appropriate use beyond mere legal requirements, and that they be accountable for any misuse of the information that is in their care.

Accountability does not redefine privacy, nor does it replace existing law or regulation. While mechanisms to achieve privacy goals will remain the concern of both policymakers and organisations, an accountability approach shifts the focus of privacy governance to an organisation's ability to achieve fundamental data protection goals and to demonstrate that capability.

While there is already a greater focus on accountability in recent data protection enactments and discussion, and much can be accomplished within existing frameworks,

there is also a growing awareness that organisations that use personal data need to put in place and ensure compliance with the five essential elements of accountability:

(1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria;

(2) Mechanisms to put privacy policies into effect, including tools, training and education;

(3) Systems for internal, ongoing oversight and assurance reviews and external verification;

(4) Transparency and mechanisms for individual participation; and

(5) Means for remediation and external enforcement.

The path forward is clear, if at times daunting. The promise of an accountability-based approach to international privacy protection presents an opportunity to further the long-standing goal of business, regulators and advocates alike — robust transfer and use of data in a fashion that is responsible and that ensures meaningful protections for individuals. To realise this goal, policymakers and the leaders of organisations must undertake the challenging and necessary work towards greater emphasis on true accountability.

**Appendix**
**Galway Project Participants**

The following lists the participants in the Galway Project. This list indicates participation in the Galway Project deliberations only, and does not imply endorsement of the contents of this document.

Joseph Alhadeff, Oracle Corporation

Rosa Barcelo, Office of the European Data Protection Supervisor

Jennifer Barrett, Acxiom Corporation

Marcus Belke, 2B Advice

Bojana Bellamy, Accenture

Daniel Burton, Salesforce.com

Emma Butler, Information Commissioner's Office, United Kingdom

Fred Cate, Indiana University, Maurer School of Law

Maureen Cooney, TRUSTe

Peter Cullen, Microsoft Corporation

Gary Davis, Office of the Data Protection Commissioner, Ireland

Elizabeth Denham, Office of the Privacy Commissioner, Canada

Michael Donohue, Organisation for Economic Co-operation and Development

Lindsey Finch, Salesforce.com

Giusella Finocchiaro, University of Bologna

Rafael Garcia Gozalo, Data Protection Agency, Spain

Connie Graham, Procter & Gamble Company

Billy Hawkes, Data Protection Commissioner, Ireland

David Hoffman, Intel Corporation

Jane Horvath, Google

Gus Hosein, Privacy International

Peter Hustinx, European Data Protection Supervisor

Takayuki Kato, Consumer Affairs Agency, Japan

Christopher Kuner, The Centre for Information Policy Leadership, Hunton & Williams LLP

Barbara Lawler, Intuit, Inc.

Artemi Rallo Lombarte, Data Protection Commissioner, Spain

Rocco Panetta, Panetta & Associates

Daniel Pradelles, Hewlett Packard Company

Florence Raynal, CNIL

Stéphanie Regnie, CNIL

Manuela Siano, Data Protection Authority, Italy

David Smith, Information Commissioner's Office, United Kingdom

Hugh Stevenson, United States Federal Trade Commission

Scott Taylor, Hewlett Packard Company

Bridget Treacy, The Centre for Information Policy Leadership, Hunton & Williams LLP

K. Krasnow Waterman, Massachusetts Institute of Technology

Armgard von Reden, IBM Corporation

Jonathan Weeks, Intel Corporation

Martin Abrams, The Centre for Information Policy Leadership, Hunton & Williams LLP

Paula J. Bruening, The Centre for Information Policy Leadership, Hunton & Williams LLP

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

# APPENDIX B

ARTICLE 29 Data Protection Working Party

Working Party on Police and Justice

02356/09/EN
WP 168

# The Future of Privacy

## Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data

**Adopted on 01 December 2009**

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190.
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

The Working Party on Police and Justice was set up as a working group of the Conference of the European Data Protection Autorities. It is mandated to monitor and examine the developments in the area of police and law enforcement to face the growing challenges for the protection of individuals with regard to the processing of their personal data.

## Executive Summary

On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

The central message of this contribution is that the main principles of data protection are still valid despite the new technologies and globalisation. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency).
- Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
- Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
- Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

Chapter 1 contains an introduction, with a brief overview of the history and context of data protection in the EU.

Chapter 2 proposes the introduction of one comprehensive legal framework. It recognises the need for specific rules (*leges speciales*), provided that they fit within the notion of a comprehensive framework and comply with the main principles. The main safeguards and principles of data protection should apply to data processing in all sectors.

Chapter 3 and 4 discuss the main challenges to data protection.

Chapter 3 on globalisation states that under EU law, data protection is a fundamental right. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. Individuals should be able to claim protection, also if their data are processed outside the EU. Therefore, the Commission is called upon to take initiatives towards the further development of international global standards regarding the protection of personal data. In addition, it is necessary to redesign the adequacy process. Furthermore, international agreements can be appropriate instruments for the protection of personal data in a global context, and the future legal framework could mention the conditions for agreements with third countries. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs). A provision on BCRs should be further reinforced and included in the new legal framework. Regarding applicable law, the WP29 envisages to advise the Commission on this subject in the course of the upcoming year.

Chapter 4 on the technological changes states that Directive 95/46/EC has stood well the influx of technological developments because of its sound and technologically neutral principles and concepts. These principles and concepts remain equally relevant, valid and applicable in today's networked world. The technological developments have strengthened the risks for individuals' privacy and data protection and to counterbalance these risks, the principle of 'Privacy by Design' should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies. The application of such principle would emphasize the need to implement privacy enhancing technologies, 'privacy by default' settings and the necessary tools to enable users to better protect their personal data. This principle of 'Privacy by Design' should therefore not only be binding for data controllers, but also for technology designers and producers. On top of that, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

Chapters 5, 6 and 7 argue that these main challenges to data protection require a stronger role for the different actors.

The changes in the behaviour and role of the data subject, and the experience with Directive 95/46/EC, require a stronger position for the data subject in the data protection framework. Chapter 5 contains suggestions for empowering the data subject, in order to play a more active role. Empowerment of the data subject requires, among others, the improvement of redress mechanisms: more options for the data subject to execute and enforce his rights, including the introduction of class action procedures, more easily accessible, and more effective and affordable complaints procedures and alternative dispute resolutions. In addition, the new framework should provide alternative solutions in order to enhance transparency and the introduction of a general privacy breach notification. 'Consent' is an important ground for processing which could under certain circumstances empower the data subject. However, at the moment, it is often falsely claimed to be the applicable ground, since the conditions for consent are not fully met. Therefore the new framework should specify the requirements of 'consent'. Furthermore, harmonisation needs to be improved, as the empowerment of the data subject is currently being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Finally, the role of data subjects on the internet is an area of concern and should be further clarified in view of the new legal framework. In any case, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as approriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller.

Chapter 6 aims at strengthening the responsibility of the data controllers. Data protection should first of all be embedded in organizations. It should become part of the shared values and practices of an organization, and responsibilities for it should be expressly assigned. This will also assist national Data Protection Authorities (DPAs) in their supervision and enforcement tasks and therefore strengthen the effectiveness of privacy protections. Data controllers need to take several proactive and reactive measures, mentioned in this chapter. Furthermore, it would be appropriate to introduce in the comprehensive framework an accountability principle, so data controllers are required to carry out the necessary measures to ensure that substantive principles and obligations of the current Directive are observed when processing personal data, and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including DPAs. Notifications of data processing operations with national

DPAs could be simplified or diminished. It should be explored whether and to what extend notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases, and how notification could be streamlined.

Chapter 7a envisages stronger and clearer roles for national DPAs. At the moment, there are large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs. The new challenges to data protection require strong supervision by DPAs, in a more uniform and effective way. The new framework should therefore guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.

Chapter 7b states how the cooperation of the DPAs should be improved. The European DPAs are united in the WP29. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. In addition, the working methods of the WP29 should be further improved. Where needed, it should be insisted on that there is a strong commitment of members of the WP29 to implement the views of the WP29 into national practice. Relations between the WP29 and the Commission, that provides for the Secretariat of the WP29, can be further improved by describing the main roles of both players in a Memorandum of Understanding. The WP29 will enter into consultation with the Commission regarding this Memorandum in 2010.

Finally, Chapter 8 discusses the data protection challenges in the field of police and law enforcement, an area of specific concern. The context of this area within the EU has changed with the entry into force of the Lisbon Treaty. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters can be seen as a first step towards a general framework in the former third pillar, but is far from complete. Over the last years, there has been a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector, due to growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime, and stimulated by the technological developments. Against this background, the challenges for data protection are immense, and should be addressed in the future legal framework. Chapter 8 provides the conditions for law and policy making on data protection in the area of police and law enforcement: basing information exchange on a consistent strategy; a periodic evaluation of existing measures, legal instruments and their application; transparency, and addressing access and rectification rights in a cross border context; transparency and democratic control in the legislative process; the architecture of systems for storage and exchange of personal data; a clear framework as a basis for relations with third states, that is binding on all parties and based on the notion of adequacy; special attention for large scale information systems within the EU; properly addressing independent supervision, judicial oversight and remedies; and strengthening cooperation between DPAs.

## 1. Introduction

*The consultation*

1. On 9 July 2009, the Commission launched a Consultation on the legal framework for the fundamental right to protection of personal data. In its consultation the Commission asks for views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation. It wants to have input on the questions whether the current legal framework meets these challenges and what future action would be needed to address the identified challenges.

2. This paper contains the joint reaction of the Article 29 Working Party (WP29) and the Working Party on Police and Justice (WPPJ) to this consultation.

*History and context*

3. The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[1] can be considered as the first European legal framework for the fundamental right to protection of personal data. The right to data protection is closely related but not identical to the right to private life under Article 8 of the European Convention for Human Rights. The right to data protection is recognised as an autonomous fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union.

4. The principles of Convention 108 were refined in Directive 95/46/EC[2] which forms the main building block of data protection law within the EU. The (future) effectiveness of the directive is the main object of the consultation of the Commission. Other EU legislative instruments for data protection are Regulation (EC) Nr. 45/2001[3] applicable to data processing by EU institutions and bodies, Directive 2002/58/EC[4] on privacy and electronic communications and Framework Decision 2008/977/JHA[5] on data protection in the area of police and judicial cooperation in criminal matters.

5. Under the Lisbon Treaty, data protection has gained significant importance. Not only has the Charter of Fundamental Rights of the European Union become binding but – also Article 16 of the Treaty on the Functioning of the European Union (TFEU) was introduced as a new legal basis for data protection applicable to all processing of personal data, in the private and in the public sector, including the processing in the area of police and judicial cooperation and common foreign and security policy. Article 16 gives an impetus for data protection.

---

1 ETS No. 108, 28.01.1981.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281, p. 31.

3 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001, L 8, p. 1.

4 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37; as revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

5 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ 2008 L 350, p. 60., to be implemented in national law before 27 November 2010.

6. In this context, also the 'Stockholm Programme' must be mentioned. This multi-annual programme of the EU dedicates much attention to data protection in an area of Freedom, Security and Justice protecting the citizen.[6]

*Central message*

7. The consultation by the Commission comes at an appropriate moment, because of the important new challenges provoked by new technologies and globalisation but also in the perspective of the Lisbon Treaty.

8. The central message is that the main principles of data protection are still valid despite these important challenges. The level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:

- Clarify the application of some key rules and principles of data protection (such as consent and transparency).
- Innovate the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
- Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
- Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters.

## 2. One comprehensive framework

*The present legal framework*

9. Data protection was introduced into the legal framework of the European Union as an internal market related issue. Directive 95/46/EC is based on Article 95 EC. The purpose of this directive is twofold. The establishment and functioning of an internal market requires that personal data should be able to flow freely from one Member State to another, while at the same time a high level of protection of fundamental rights of individuals should be safeguarded.

10. Directive 95/46/EC is meant as a general legal framework, which could be complemented by specific regimes for data protection for specific sectors. Until now, only one specific regime has been adopted, for ePrivacy (currently Directive 2002/58/EC). Moreover, several pieces of sectoral legislation also contain specific rules relating to the processing of personal data ([7] on money laundering, customs legislation or VIS, EURODAC or SIS II legislations).

---

[6] The Stockholm Programme: An open and secure Europe serving and protecting the citizen, to be approved by European Council in December 2009.

[7] E.g. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ 2005, L 309, p. 15 and the various legal instruments for the large scale information systems SIS, VIS and EURODAC.

11. The use of Article 95 EC had a consequence for the scope of application of Directive 95/46/EC. Although the Directive was meant as a general framework for data protection and in many aspects functions as such, it does not cover the processing by EU-institutions, nor processing operations that fall outside of the former first pillar (mainly the former third pillar). For the processing by the EU-institutions (as far as they operate within the former first pillar), Regulation 45/2001 was adopted which is to a large extent similar to Directive 95/46/EC. The current situation in the former third pillar can be described as a patchwork of data protection regimes, which are applicable in different situations. Some differences in these regimes stem from the specificities of the area covered, others are merely the consequence of a different legislative history. Framework Decision 2008/977/JHA can be seen as a first step towards a more general framework.

12. The situation is not satisfactory, in particular for the third pillar:

- Data protection is now increasingly recognised as a general concern of the European Union, not necessarily linked to the internal market. This is for instance reflected in Article 8 of the Charter of Fundamental Rights of the European Union.
- In recent years, and certainly after the terrorist attacks in the USA on 11/9/2001, the exchange of personal data between the Member States has become an essential part of police and judicial cooperation which, of course, requires appropriate protection.
- The former division between the pillars does not reflect the reality of data protection where personal data are used in cross pillar situations, as illustrated by the PNR and Data Retention judgements of the European Court of Justice, on cases of use for law enforcement purposes of information collected originally in a business context. .

***The need for a new framework***

13. The shortcomings of the present system require a reflection on 'a comprehensive and consistent data protection framework covering all areas of EU competence'[8]. The Lisbon Treaty foresees a new horizontal approach to data protection and privacy and provides for the necessary legal basis (Art. 16 TFEU)[9] to get rid of the existing differences and divergences which prejudice a seamless, consistent and effective protection of all individuals.

14. The main safeguards and principles should apply to data processing in all sectors, ensuring an integrated approach as well as a seamless, consistent and effective protection.

15. Directive 95/46/EC should serve as a benchmark for the comprehensive framework which has as main goal effectiveness and effective protection of individuals. The existing principles of data protection need to be endorsed, and complemented with

---

[8] Wording used by Commission in COM 262 Final.

[9] Article 16 TFEU does not only extend to the third pillar, but also to the second pillar (common foreign and security policy) as far as EU institutions process personal data. Article 39 TEU provides for a specific legal basis for data processing by the Member States in the second pillar. This all is relevant for instance in relation to the terrorists' lists established by the EU and the Member States, but will not be specifically addressed in this chapter.

measures to execute these principles in a more effective manner (and to ensure a more effective protection of citizens' personal data).

16. The main principles of data protection should be the backbone of a comprehensive framework: key notions (who/data controller - what /personal data) and principles should be reaffirmed, including notably the principles of lawfulness, fairness, proportionality, purpose limitation, transparency, and rights of the data subject, as well as independent supervision by public authorities. Rethinking the framework is also an opportunity to clarify the application of some key concepts, such as:

    - consent: confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis (see also Chapter 5);
    - transparency: it is a pre-condition to fair processing. It must be clear that transparency does not necessarily lead to consent but is a pre-condition for a valid consent and the exercise of the rights of the data subject (see also Chapter 5).

    The objective should be to improve data protection on an international level, in line with the principles and rights defined by Directive 95/46/EC, whilst, at the same time, upholding the current level of protection (see also Chapter 3).

17. The adoption of one comprehensive framework would also allow some useful innovations of the current rules. This might well involve the introduction of the general principle of 'privacy by design' as extension of the current rules on organisational and technical security measures (see also Chapter 4) and the general principle of accountability (see also Chapter 6).

***The architecture of a comprehensive framework***

18. One comprehensive framework - under the Lisbon Treaty based on a single legal basis - does not necessarily mean that there is no room for flexibility and differences between the sectors and between the Member States, within the scope of the general framework. Specific rules (*leges speciales*) could be complementary and enhance the protection, provided that they fit within the notion of a comprehensive framework and comply with the main principles, as mentioned above.

19. Additional sectoral and specific regulations could be envisaged, for example with regard to:

    - Specific sectors, such as for instance public health, employment or intelligent transport systems.
    - Privacy tools and services, such as seals and audits (see also Chapters 4 and 6).
    - Security breaches (as complement of the security principle; see also Chapters 5 and 6).
    - Police and judicial cooperation, as explicitly foreseen in Declaration 21 attached to the Lisbon Treaty (see further Chapter 8).
    - National security policy, as explicitly foreseen in Declaration 20 attached to the Lisbon Treaty.

20. Additional national regulations could be envisaged, taking into account cultural differences and the internal organisation of the Member States, provided that they do not prejudice the harmonisation, needed within a European Union without internal borders.

21. Further harmonisation is needed as part of an unambiguous and unequivocal legal framework, but this does not exclude that some flexibility can have additional value, as is presently recognised under Directive 95/46/EC for instance if needed because of cultural differences. One could also leave room for national law, to determine the allocation of responsibilities and to recognise different roles of the public and private sectors.

## 3. Globalisation

***Context and present legal framework***

22. Under EU law, data protection is a fundamental right, protected under Article 8 of the Charter of Fundamental Rights of the European Union (see also Chapter 1). In other parts of the world, the need for data protection is widely recognised but not necessarily with the status of a fundamental right.

23. The EU and its Member States should guarantee this fundamental right for everybody, in so far as they have jurisdiction. In a globalised world, this means that individuals can claim protection also if their data are processed outside the European Union.

24. Directive 95/46/EC has addressed this need for protection in its Article 4. The directive is applicable to data processing anywhere, and therefore also outside the EU[10] (a) when the controller is established in the EU, and (b) when the controller is established outside the EU but uses equipment in the EU.

25. In addition, Article 25 and 26 of Directive 95/46/EC include a specific regime for the transfer of personal data to third countries. The basic rule of Article 25 is that transfer is only allowed to third countries that ensure an adequate level of protection. Article 26 foresees a number of derogations from this requirement. Well known concepts such as Bindings Corporate Rules (BCRs) and Standard Contractual Clauses implement this provision.

***Applicable law***

26. The exact scope of Directive 95/46/EC however is not sufficiently clear. It is not always clear whether EU law is applicable, which Member State law is applicable, and what would be the law(s) applicable in case of multiple establishments of a multinational in different Member States. Article 4 of the directive, determining when the directive is applicable to data processing, leaves room for different interpretation.

27. Moreover, there are situations which fall outside the scope of application of the directive. This is the case where non-EU established controllers direct their activities to EU residents which result in the collection and further processing of personal data.

[10] In this context, EU should be understood as including the EFTA-countries.

For example, this is the case of on-line vendors and the like using specific advertisement with local flavor, websites that directly target EU citizens (by using local languages, etc). If they do so without using equipment in the EU, then Directive 95/46/EC does not apply.

28. At the moment, the WP29 is writing an opinion on the concept of applicable law. The WP29 envisages advising the European Commission on this topic in the course of the upcoming year. This advice might include further recommendations for a future legal framework.

***International standards and the Madrid Resolution***

29. Global standards regarding data protection are becoming indispensable. Global standards would also facilitate transborder data flows which, due to globalisation, are becoming the rule rather than the exception. As long as global standards do not exist, diversity will remain. Transborder data flows have to be facilitated whilst, at the same time, ensuring a high level of protection of personal data when they are transferred to and processed in third countries.

30. The 'Madrid Resolution', a Joint Proposal on International Standards for the Protection of Privacy which has been adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009, deserves support. The Joint Proposal contains a draft of a global standard and brings together all the approaches possible in the protection of personal data and privacy, integrating legislation from five continents. It includes a series of principles, rights and obligations that should be the basis for data protection in any legal system all over the world, and demonstrates that global standards providing an adequate level of data protection are feasible in due course.

31. The Commission is called upon:

- To take initiatives towards the further development of international global standards regarding the protection of personal data with a view to promote an international framework for data protection and therefore facilitate transborder data flow while ensuring an adequate level of protection of data subjects. These initiatives should include investigating the feasibility of a binding international framework.
- In the absence of global standards, to promote the development of data protection legislation providing an adequate level of protection, and the foundation of independent DPAs, in countries outside the European Union. The basic principles for data protection, as laid down in the 'Madrid Resolution', should be the universal basis for such legislation.

These specific tasks of the Commission should be mentioned in the future legal framework.

***Improving adequacy decisions***

32. Ever more processing operations of personal data take place in a globalised environment. Ensuring the free flow of personal data, while guaranteeing the level of protection of individuals' rights, is an increasing demand. Thus, it is necessary to redesign the adequacy process:

- Defining more precisely the criteria for reaching the legal status of 'adequacy', paying due attention to the approach of the WP29[11] and various other approaches to data protection around the world, and especially to the rights and principles laid down in the Joint Proposal of International Standards on the Protection of Privacy.
- Streamlining the procedures for the analysis of the legal regimes of third countries in order to take more decisions on the adequate level of protection.

The future legal framework should specify these issues.

***International agreements***

33. Note has been taken of the activities of the EU-US High Level Contact Group on information sharing and privacy and personal data protection. These activities might lead to a transatlantic agreement with common principles for privacy and data protection applicable to the exchange of information with the United States for the fight against terrorism and serious transnational crime.[12].

34. International agreements are appropriate instruments for the protection of personal data in a global context, provided that the level of protection afforded is at least equivalent to the global standards mentioned above, that every individual has an easy and effective redress, including judicial redress, and that specific safeguards are included relating to the purpose for which the personal data will be used.

35. Under those conditions the foreseen transatlantic agreement could serve as a model for exchange with other third countries and for other purposes. The future legal framework could mention the conditions for agreements with third countries.

36. Furthermore, the EU should encourage the cooperation between international data protection authorities, for example on a transatlantic level. Such cooperation is a successful means to promote data protection outside the EU.

***Binding Corporate Rules / Accountability***

37. The processing of data outside the EU can also be protected by Binding Corporate Rules (BCRs), international codes of conduct for multinationals, allowing for the worldwide transfer within a multinational corporation. BCRs have been introduced by the WP29 in 2003. Both DPAs and multinationals are of the opinion that BCRs are a good means to facilitate international data flows whilst guaranteeing the protection of personal data. However, Directive 95/46/EC did not expressly take account of BCRs. As a result the process for adoption of BCRs, which is based on Article 26 (2) of Directive 95/46/EC, requires the approval of all Member States concerned by a BCR. As a result, assessing and approving BCRs takes a long time. The WP29 has devoted considerable effort to promote and facilitate the use and the approval of BCRs within the current legal framework. In order to improve the process, so far, nineteen DPAs have agreed to a procedure on the approval of BCRs called 'Mutual Recognition'.

---

[11] See in particular WP 29 Working Document 12: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, adopted on 24 July1998

[12] In this regard, the transatlantic problem regarding redress remains to be solved.

38. Against this background a provision on BCRs should be further reinforced and included in the new legal framework, which would serve several purposes:

- Recognising BCRs as appropriate tool to provide adequate safeguards.
- Defining the main substantive and procedural elements of BCRs, following the WP29 Opinions on the subject.

39. Moreover, from a general point of view, a new provision could be included in the new legislative framework pursuant to which data controllers would remain accountable and responsible for the protection of personal data for which they are controllers, even in the case the data have been transferred to other controllers outside the EU (see on 'accountability' more in general Chapter 6).

***Final remark***

40. This chapter discusses globalisation as such. However, in one way or another, all chapters of this contribution deal with this subject. Often, when one thinks of 'globalisation', one thinks of business. However, increasingly processing operations of personal data take place in a globalised world. Even though the individual often lives a local life, he can more and more be found on line where his data are processed globally. Globalisation therefore is linked to technology (Chapter 4), the position of the data subject (Chapter 5), data controller (Chapter 6), DPAs / WP29 (Chapter 7) and law enforcement (Chapter 8).

## 4. Technological changes; Privacy by Design as a new principle

41. The basic concepts of Directive 95/46/EC were developed in the nineteen seventies, when information processing was characterized by card index boxes, punch cards and mainframe computers. Today computing is ubiquitous, global and networked. Information technology devices are increasingly miniaturized and equipped with network cards, WiFi or other radio interfaces. In almost all offices and family homes users can globally communicate via the Internet. Web 2.0 services and cloud computing are blurring the distinction between data controllers, processors and data subjects.

42. Directive 95/46/EC has stood well the influx of these technological developments because it holds principles and uses concepts that are not only sound but also technologically neutral. Such principles and concepts remain equally relevant, valid and applicable in today's networked world.

43. While it is clear that technological developments described above are generally good for society, nevertheless they have strengthened the risks for individuals' privacy and data protection. To counterbalance these risks, the data protection legal framework should be complemented. First, the principle of 'privacy by design' should be introduced in the new framework; second, as the need arises, regulations for specific technological contexts should be adopted which require embedding data protection and privacy principles into such contexts.

***Privacy by design principle***

44. The idea of incorporating technological data protection safeguards in information and communication technologies ('ICT') is not completely new. Directive 95/46/EC already contains several provisions which expressly call for data controllers to implement technology safeguards in the design and operation of ICT. This is the case of Article 17 which lays down the data controllers' obligation to implement appropriate technical and organizational measures. Recital 46 calls for such measures to be taken, both at the time of the design of the processing system and at the time of the processing itself. Article 16 establishes the confidentiality of processing, a rule which is mirrored and complemented in regulations regarding IT security. Apart from these articles, the principles relating to data quality as contained in Article 6 (lawfulness and fairness, purpose limitation, relevance, accuracy, time limit of storage, responsibility) also apply.

45. Whereas the above provisions of the Directive are helpful towards the promotion of privacy by design, in practice they have not been sufficient in ensuring that privacy is embedded in ICT. Users of ICT services – business, public sector and certainly individuals – are not in a position to take relevant security measures by themselves in order to protect their own or other persons' personal data. Therefore, these services and technologies should be designed with privacy by default settings.

46. It is for these reasons that the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements.

47. Such principle should call for the implementation of data protection in ICT (privacy by design or 'PbD') designated or used for the processing of personal data. It should convey the requirement that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed. This is in line with recent case law in Germany.[13]

48. The application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption). It should be a crucial requirement for products and services provided to third parties and individual customers (eg. WiFi-Routers, social networks and search engines). In turn, it would give DPAs more powers to enforce the effective implementation of such measures.

---

[13] Recently the German Constitutional Court (Judgment of 27 February 2008 – 1 BvR 370/07; 1 BvR 595/07 –) created a constitutional right in the confidentiality and integrity of information technology system. Systems that are able to create, process or store sensitive personal data require special protection. The protective scope of the fundamental right in confidentiality and integrity of information technology system is applied to systems which alone, or in their technical interconnectedness, can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of their personality. These systems are for example personal computers and laptops, mobile phones and electronic calendars.

49. Such principle should be defined in a *technologically neutral* way in order to last for a long period of time in a fast changing technological and social environment. It should also be *flexible* enough so that data controllers and DPAs will, on a case by case basis, be able to translate it in concrete measures for guaranteeing data protection.

50. The principle should emphasize, as current Recital 46 does, the need for such principle to be applied *as early as possible*: 'At the time of the design of the processing system and at the time of the processing itself'. Safeguards implemented at a late stage are inconsistent and insufficient as regards the requirements of an effective protection of the rights and freedoms of the data subjects.

51. Technological standards should be developed and taken into consideration in the phase of system analysis by hardware and software engineers, so that difficulties in defining and specifying requirements deriving from the principle of 'privacy by design' are minimized. Such standards may be general or specific with regard to various processing purposes and technologies.

52. The following examples demonstrate how PbD can contribute to a better data protection:

- Biometric identifiers should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases.
- Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence.
- Patient names and other personal identifiers maintained in hospitals' information systems should be separated from data on the health status and medical treatments. They should be combined only in so far as it is necessary for medical or other reasonable purposes in a secure environment.
- Where appropriate, functionality should be included facilitating the data subjects' right to revoke consent, with subsequent data deletion in all servers involved (including proxies and mirroring).

53. In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be respected:

- Data Minimization: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- Controllability: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
- Transparency: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.

- User Friendly Systems: privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- Data Confidentiality: it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
- Data Quality: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- Use Limitation: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

***Regulations for specific technological contexts***

54. The privacy by design principle may not be sufficient to ensure, in all cases, that the appropriate technological data protection principles are properly included in ICT. There may be cases where a more concrete 'hands on approach' may be necessary. To facilitate the adoption of such measures, a new legal framework should include a provision enabling the adoption of specific regulations for a specific technological context which require embedding the privacy principles in such context.

55. This is not a new concept; Article 14 (3) of the ePrivacy Directive, contains a similar provision: 'Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and communications)'.

56. The above would facilitate the adoption, in specific cases, of specific legislative measures embedding the concept of 'privacy by design' and ensuring that adequate specifications are provided. For example, this may be the case with RFID technology, social networks, behavioral advertisement, etcetera.

***Final remarks***

57. The increasing significance of data protection when creating and operating IT-systems is posing additional requirements to IT-specialists. This causes the need to firmly incorporate data protection into the curricula of IT-professions.

58. The technological data protection principles and the ensuing concrete criteria should be used as a basis for awarding labels of quality (certification schemes) in a framework of a data protection audit.[14]

## 5. Empowering the Data Subject

59. The potential of the position of the data subject in Directive 95/46/EC has not been fully used. In addition, both the behaviour of citizens and the role of data subjects with respect to data protection have changed, amongst others due to sociological

[14] For example, this is the case with the EuroPriSe project.

changes and new ways of data collection (for instance for profiling purposes). Data subjects can be careless with their own privacy, are sometimes willing to trade privacy for perceived benefits. On the other hand, they still have high expectations of those with whom they do business. Also, data subjects themselves more and more play an active role in the processing of personal data, in particular on the internet.

60. Changes in the behaviour and role of the data subject and the experience with Directive 95/46/EC require a stronger position for the data subject in the data protection framework.[15] Further empowerment of the data subject in order to be able to play a more active role is essential.

***Improving redress mechanisms***

61. Empowerment of the data subject requires giving the data subject more options to execute and enforce his rights. As court proceedings can sometimes be very difficult and bear a financial risk, the possibility for class action procedures should be introduced in Directive 95/46/EC.[16]

62. In addition, data controllers should provide for complaints procedures which are more easily accessible and more effective and affordable (see also Chapter 6). If these procedures do not resolve the dispute between data subject and data controller, the data subject should be able to turn to alternative dispute resolutions, primarily provided for by the industry.[17] These options should be included in the new legislative framework.

***Transparency***

63. Transparency is another fundamental condition, as it gives the data subject a say in the processing of personal data, *'ex ante'*, prior to processing. Profiling, data mining, and technological developments which ease the exchangeability of personal data make it even more important for the data subject to be aware by whom, on what grounds, from where, for what purposes and with what technical means data are being processed. It is important that this information is understandable. However, the duty to inform the data subject (Articles 10 and 11 of Directive 95/46/EC) is not always properly put into practice. A new legal framework should provide alternative solutions, in order to enhance transparency. For example, new ways to inform data subjects could be developed in relation to behavioural advertising.

64. In addition, transparency requires that affected individuals should be notified when a privacy breach which is likely to adversely affect their personal data and privacy occurs. That would enable the data subjects to try and control the damage that has been inflicted upon them (in certain cases authorities should be notified as well, see also Chapter 6). A general privacy breach notification should be introduced in the new legal framework (see also Chapter 6).[18]

---

[15] This is especially the case when it concerns children. When taking decisions about their personal data, their best interest needs to be a primary consideration, as stated in the UN Convention on the Rights of the Child (http://www2.ohchr.org/english/law/crc.htm) and other specific international instruments and national law.

[16] Class actions for example exist in environmental law.

[17] This may of course not deprive an individual from a proper redress before a Court or a DPA.

[18] In 'Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)' the WP29 has noted a recommended approach to the issue of the specific privacy breach notifications which are taken on board in the ePrivacy Directive. The same recommendations apply to the introduction of general privacy breach notifications.

***Consent***

65. In the Directive, consent of the data subject is a legitimate ground for data processing (Article 7 and 8 of Directive 95/46/EC). It is and continues to be an important ground for processing, which could under certain circumstances empower the data subject. However, consent needs to be freely given, informed and specific (Article 2 (h) of Directive 95/46/EC).

66. There are many cases in which consent can not be given freely, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities).

67. In addition, the requirement that consent has to be informed starts from the assumption that it needs to be fully understandable to the data subject what will happen if he decides to consent to the processing of his data. However, the complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice.[19]

68. In both hypotheses, consent is an inappropriate ground for processing but nevertheless often falsely claimed to be the applicable ground. The technological developments also ask for a careful consideration of consent. In practice, Article 7 of Directive 95/46/EC is not always properly applied, particularly in the context of the internet, where implicit consent does not always lead to unambiguous consent (as required by Article 7 (a) of the Directive). Giving the data subjects a stronger voice *'ex ante'*, prior to the processing of their personal data by others, however requires explicit consent (and therefore an opt-in) for all processing that is based on consent.[20]

69. The new legal framework should specify the requirement of consent, taking into account the observations made above.

***Harmonisation***

70. Currently the empowerment of data subjects is being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. Several elements of the Directive which are of essence to the position of data subjects, such as the liability provision and the possibility to claim immaterial damages,[21] have not been implemented by all Member States. Besides these differences in the implementation of Directive 95/46/EC, the interpretation of the Directive in the Member States is not always uniform. As globalisation increases, these differences

---

[19] See 'Data Protection Accountability: The essential Elements – A Document for Discussion', Centre for Information Policy Leadership, as Secretariat to the Galway Project, October 2009, p.4.

[20] Regarding consent and opt-in / opt-out, see also chapter 2, where it is stated that confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis.

[21] In the majority of cases in which damage has been inflicted upon the data subject, the damage consists of immaterial damage such as the sense no longer to be able to move through the public and private sector without being watched. This problem increases in the current 'surveillance society'.

more and more weaken the position of the data subject. It is therefore of great importance that harmonisation be improved (see also Chapter 7b), if needed by specifying legislative provisions.

***The role of data subjects on the internet***

71. Increasingly, individuals upload their own personal data into the internet (social networks, cloud computing services, etc). However, Directive 95/46/EC does not apply to the individual who uploads the data for 'purely personal' purposes or 'in the course of a household activity'.[22] Arguably it does not apply either to the organization that provides the service, i.e. hosts and makes available the information uploaded by the individual (unless the service processes data for its own purposes) insofar as the service provider may not be deemed to be a controller.[23] The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations. In this context, whoever offers services to a private individual should be required to provide certain safeguards regarding the security, and as appropriate the confidentiality of the information uploaded by users, regardless of whether their client is a data controller. In addition, thought should be given to the question whether data subjects should be given more means to execute their rights on the internet, including the protection of rights of third parties whose personal data may be object of processing (e.g. social networks). As there are many more unresolved issues in this context,[24] the role of the data subject on the internet should be further clarified, in view of a new legal framework.

## 6. Strengthening Data Controllers' Responsibility

72. Under Directive 95/46/EC, the data controller is the key actor to ensure compliance with the principles and obligations aimed at safeguarding the protection of personal data of individuals. The Directive, implicitly and in many cases explicitly, requires the data controller to respect data protection principles and fulfil certain specific obligations.[25] Examples of the latter include notifying and prior checking of data processing operations with national authorities.[26] Furthermore, ensuring respect for individuals' data protection rights requires the imposition of corresponding duties upon the data controller such as the provision of information.[27]

---

[22] For a better understanding of whether an activity is covered or not by this 'household exemption', see Opinion 5/2009, on online social networking (WP 163).

[23] This problem does not arise where organizations - either in public or private sector - make use of cloud computing applications, since the Directive applies to them and their processing operations where "carried out in the context of the activities of an establishment of the controller" in the EU (see Article 4.1.a). Chapter 5 thus applies to them, regardless of whether the service provider is established in the EU or not.

[24] Regarding, for example, the consent of children and/or their parents, access requests by law enforcement, access rights to internet accounts by heirs of deceased people, and third party applications.

[25] Article 6 (2) explicitly provides that "it shall be for the controller to ensure that paragraph 1(which refers to the main principles relating to data quality) "is complied with".

[26] See Articles 18-21 of Directive 95/46.

[27] Other examples of data subjects' rights include the right to access, rectification, erasure and blocking, and to object to the processing of personal data (Articles 10-12 and 14). These rights entail obligations for the controller to satisfy them.

73. These obligations also apply - directly or indirectly - to data processors when/if data controllers have entrusted all or part of the data processing operations to them. To provide guidance on the concept of data controller and processor, the WP29 is currently engaged in drafting an interpretative opinion. The WP29 envisages to soon advise the Commission on this topic. This advice might include further recommendations for a future legal framework.

***Embedding data protection in organisations***

74. The relevant provisions of Directive 95/46/EC form an undeniably solid base for the protection of personal data and should be maintained. Nonetheless, compliance with existing legal obligations often is not properly embedded in the internal practices of organizations. Frequently, privacy is not embedded in information processing technologies and systems. Furthermore, management, including top level managers, generally are not sufficiently aware of and therefore actively responsible for the data processing practices in their own organizations. The data protection scandals that have taken place in some Member States in the last few years support this concern.

75. Unless data protection becomes part of the shared values and practices of an organization, and unless responsibilities for it are expressly assigned, effective compliance will be at risk and data protection mishaps will continue. In turn, this may undermine public trust and confidence in business and public administrations alike. Moreover, embedding data protection in organizations' cultures will assist national DPAs in their supervision and enforcement tasks, as further developed in Chapter 7, strengthening the effectiveness of privacy protections.

76. The principles and obligations of Directive 95/46/EC should permeate the cultural fabric of organizations, at all levels, rather than being thought of as a series of legal requirements to be ticked off by the legal department. The Directive's requirements should result in concrete data protection arrangements being applied on a day-to-day basis. Privacy controls should be integrated into the design of information technologies and systems (see also Chapter 4). Furthermore, within the organizations, both in public and private sectors, internal responsibility for data protection should be properly recognized, strengthened and specifically assigned.

77. The effectiveness of the provisions of Directive 95/46/EC is dependent on data controllers' effort towards achieving these objectives. This requires the following proactive measures:

- *Adoption by data controllers of internal policies and processes* to implement the requirements of the Directive for the particular processing operations carried out by the controller. Such internal policies and processes should be approved at the highest level within the organization and therefore be binding for all staff members.
- *Putting in place mechanisms executing the internal policies and processes, including complaints procedures (see also Chapter 5),* in order to make such policies effective in practice. This may include creating data protection awareness, staff training and instruction.
- *Drafting compliance reports and carrying out audits, obtaining third-party certification and/or seals* to monitor and assess whether the internal measures adopted to ensure compliance effectively manage, protect, and secure personal data (see also Chapter 4).

- Carrying out *privacy impact assessments*, particularly for certain data processing operations deemed to present specific risks to the rights and freedoms of data subjects, for example, by virtue of their nature, their scope or their purpose.
- *Assignment of responsibility for data protection* to designated persons with direct responsibility for their organizations' compliance with data protection laws.
- *Certification of compliance by top level company executives* confirming that they have implemented appropriate safeguards to protect personal data.
- *Transparency of these adopted measures* vis-à-vis the data subjects and the public in general. Transparency requirements contribute to the accountability of data controllers (e.g. publication of privacy policies on the internet, transparency in regard to internal complaints procedures, and publication in annual reports).

78. Article 17 (1) of Directive 95/46/EC, to some extent, already requires data controllers to implement measures, of both technical and organizational nature (the data controller must *"implement appropriate technical and organizational measures to protect personal data against.... unlawful forms of processing")*. These measures may include some of the above measures. However, in practice Article 17 (1) has not been successful in making data protection sufficiently effective in organizations, also due to different approaches taken in the national implementing measures.

***Accountability principle***[28]

79. To address this problem, it would be appropriate to introduce in the comprehensive framework an accountability principle. Pursuant to this principle, data controllers would be required to carry out the necessary measures to *ensure* that substantive principles and obligations of the current Directive *are observed* when processing personal data. Such provision would reinforce the need to put in place policies and mechanisms to make effective the substantive principles and obligations of the current Directive. It would serve to reinforce the need to take effective steps resulting in an internal effective implementation of the substantive obligations and principles currently embedded in the Directive. In addition, the accountability principle would require data controllers to have the necessary internal mechanisms in place to *demonstrate compliance* to external stakeholders, including national DPAs. The resulting need to provide evidence of adequate measures taken to ensure compliance will greatly facilitate the enforcement of applicable rules.

80. In any event, the measures expected from data controllers should be scalable and take into consideration the type of company, whether large or small, and of limited liability, the type, nature and amount of the personal data by the controller, among other criteria.

***More options: proactive or reactive***

81. Some of the measures described above could be deemed as standard good practice, thus fulfilling the accountability principle if carried out in practice. A built-in reward structure could be foreseen in law to induce organizations to implement them.

---

[28] See on accountability also Par. 39.

82. An alternative solution could be more prescriptive. For example, Article 17 (1) could be elaborated in order to specify additional proactive measures, such as those outlined above, to be implemented by data controllers. These measures should be orientated towards achieving specific outcomes and should be technologically neutral.

83. Other measures would be of a more reactive nature. They would apply when there has been an unlawful processing of personal data and might, inter alia, involve the following:

- *Setting up a mandatory security breach notification obligation* (see also Chapters 2 and 5).
- *Reinforcement of enforcement powers of DPAs*, including the imposition of concrete requirements to ensure an effective protection (see also Chapter 7a).

***Simplification of notifications***

84. Notifications of data processing operations with national DPAs could be simplified or diminished. In this context, the link between compliance with the requirements mentioned above and the possibility to further nuance the administrative requirements, in particular the notification of data processing activities with national DPAs, should be explored.

85. Notification contributes to the awareness of the data processing operations and data protection practices within organizations.[29] It also gives DPAs an overview of data processing activities. However, better data governance and accountability requirements may achieve the same purposes. Those mechanisms might help to carry out the necessary measures to observe the substantive principles and obligations currently embedded in the Directive and to produce evidence of such compliance.

86. It should be explored whether and to what extent notification could be limited to those cases where there is a serious risk to privacy, enabling DPAs to be more selective and concentrate their efforts to such cases. Even in such cases, notification could be streamlined, for example, by providing the results of privacy impact assessments, or the outcome of third-party auditing. This could be combined with a registration system whereby all data controllers would be enrolled in a registry maintained by the DPA, to ensure the easy identification of organizational entities for efficient and effective enforcement when necessary.

## 7. Stronger and clearer roles for DPAs and their cooperation within the EU

### 7a. Data Protection Authorities

87. At the moment, there are big differences regarding the position of the DPAs in the 27 Member States. This is due to the differences in history, case law, culture and the internal organization of the Member States, but also because Article 28 of Directive

[29] These views are further confirmed by the WP's report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union (WP 106), adopted on 18 January 2005.

95/46/EC lacks precision in several aspects. On top of that, the Directive has, to a certain extent, been poorly implemented in some jurisdictions. This has resulted in large divergences between the Member States regarding, amongst others, the position, resources and powers of DPAs.

88. The new challenges to data protection (globalisation and the technological changes, Chapters 3 and 4) require strong supervision by DPAs, in a more uniform and effective way. As a consequence, the new framework should guarantee uniform standards as for independence, effective powers, an advisory role in the legislation making process and the ability to set their own agenda by, in particular, setting priorities regarding the handling of complaints, all on a high and influential level.

89. DPAs need to be fully and truly independent. The current Article 28 (1) of Directive 95/46/EC is unclear in this respect as is demonstrated by Case C-584/07 (Commission v. Germany), currently before the European Court of Justice. In the new legal framework DPAs should have:

- complete institutional independence and not be subordinated to any other government authority.
- functional independence and not be subject to instructions by the controlled, in relation to the contents and extent of its activity.
- material independence. They should have an infrastructure which is suited to the smooth conduct of their activities, in particular adequate funding. Sufficient resources should be allocated to the DPAs.

90. The enforcement role of DPAs is becoming increasingly important. DPAs need to be able to be strong and bold, and strategic on intervention and enforcement. The current wording of article 28 of Directive 95/46/EC has resulted in widely diverse enforcement powers. The new framework should require a more uniform approach from Member States in giving the DPAs the necessary powers and it should be more specific in this regard than Directive 95/46/EC. The necessary powers should, amongst others, include the power to impose financial sanctions on controllers and processors.

91. The advisory role of DPAs in the legislation making process is indispensable, as the knowledge that DPAs acquire from investigation and enforcement actions often is necessary in order to improve (data protection) legislation. The advisory role should involve all measures and regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, not just 'administrative measures and regulations'[30]. DPAs should be asked for advice before the draft legislation is adopted. In addition, the new framework should ensure that DPAs have an advisory role towards their national Parliaments and/or other national competent institutions, at the time when the latter are involved in the drafting process of new EU legislation.

92. DPAs need to be able to fix their own agenda when setting priorities with regard to, inter alia, the handling of complaints, including the manner in which complaints are handled.[31] DPAs should in any case be able to take into account whether the

[30] Article 28 (2) of Directive 95/46/EC.

[31] The possibility to be selective can be put in practice in different ways, e.g. by establishing 'fast track' procedures to deal with minor claims.

handling of a certain complaint will sufficiently contribute to the protection of personal data.[32] The new framework should enable the DPAs to 'be selective to be effective'.

93. On the other hand, DPAs need to be accountable for the way they make use of their stronger supervisory role. They should be transparent in this regard and publicly report on the way they operate and the priorities they set. The current wording of Article 28 (5) of Directive 95/46/EC needs to be specified in this regard in the new framework.

### 7b. Cooperation of Data Protection Authorities

***The present legal framework***

94. Article 29 of Directive 95/46/EC has set up the Working Party on the protection of individuals with regard to the processing of personal data (WP29) as the institutional body for cooperation among national DPAs. The WP29 has an advisory status and acts independently. Its tasks are set forth in Article 30 (1) of the Directive and include contributing to the uniform application of the Directive, by examining questions covering the application of the national measures, giving opinions on the level of protection in the Community and in third countries, as well as advising (also on its own initiative) on proposals for Community legislation having an impact on data protection or any other matters relating to the protection of persons with regard to the processing of personal data in the Community. The Commission is a member of the WP29 and provides for the Secretariat.

95. The WP29 fulfils its task within the scope of Directive 95/46/EC, as specified in its Article 3 (2). In the area of police and judicial cooperation, the European DPAs have established in 2007 the Working Party on Police and Justice (WPPJ) which fulfils a similar role as WP29, but without a legal basis and a secretariat provided for by an EU Institution. Framework Decision 2008/977/JHA, which introduces data protection principles in that area, does not provide for any institutionalised cooperation of DPAs.

***The functioning of the WP29***

96. The WP29 now functions for over 10 years and has significantly contributed to achieve the goals of Article 30 of Directive 95/46/EC. The result of many of its activities can be found on its website.[33]

97. The WP29 has constantly worked on how to improve its effectiveness and should continue to pay attention to its own functioning.
Special points of consideration are:

- how can the WP29 effectively contribute to the uniform implementation of EU legislation in national laws and to the uniform application of national law?

---

[32] Criteria which can be applied to determine whether a complaint should be handled are for example whether the complaint relates to a situation which affects a large number of people, concerns a breach of data protection legislation which is not of little importance and probably not an incidental phenomenon, and whether handling the complaint is likely to be successful and does not require disproportionate efforts.

[33] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm?refer=true&theme=blue

- how can it improve its effectiveness vis-à-vis the EU institutions and in particular the Commission, also taking into account the hybrid role of the Commission as member of the WP29, as its secretariat as well as the addressee of many of the opinions of the WP29?

***Consequences for the future***

98. As a first priority, it should be ensured that all issues relating to the processing of personal data, in particular in the area of police and judicial cooperation in criminal matters, will be included in the activities of the current WP29. A comprehensive legal framework should include a comprehensive advisor and an effective cooperation between supervisory authorities. In a transitional period, before a legislative change is realized, appropriate forms for the WP29 to work closely together with the WPPJ must be found.

99. Other improvements do not require a legislative change.

- The uniform application of national law implementing Directive 95/46 can be achieved within the present legal framework, by further improving the working methods of the Working Party and, where needed, by insisting on a strong commitment by the members of the WP29 to implement the views of the WP29 into national practice.
- In accordance with Article 29 of Directive 95/46/EC, the Secretariat of the WP29 is provided by the Commission. The Secretariat should work in close cooperation with the Presidency of the WP29 and its staff. The tasks of the Secretariat and the Presidency are complementary and they should closely work together in order to enable the WP29 to fulfill its missions in the most efficient manner. While the Secretariat deals with all the logistical aspects of the work of the WP29 and assists the WP29 in preparing its opinions and documents, the Presidency (and the Vice-Presidency) focus mainly on the decision-making process and on the strategy of the WP29.
- Relations with the Commission can be further improved by describing the main roles of both players in a Memorandum of Understanding between the WP29 and the Commission. This Memorandum should also address the resources available for the WP29 so that it can use its full capacity in assuming its assignments. Finally, it should address the functioning of the Secretariat, in order to ensure that both the WP29 and the Secretariat itself have sufficient resources to prepare the opinions and working documents of the WP29. The WP29 will enter into consultation with the Commission on the above in 2010.

## 8. Data protection challenges in the field of police and law enforcement

100. Data protection in the field of police and justice is a specific subject which requires specific attention, taking into account the complex relation between the activities of the State to ensure security and the protection of the personal data of the individual. The specificity of this area is not only the result of the former pillar structure of the previous EU-Treaties, but is more widely recognised (see for instance the exceptions of Article 13 of Directive 95/46/EC and Declaration 21 attached to the Lisbon Treaty).

***Changing context within the EU***

101. With the entry into force of the Lisbon Treaty, new perspectives will be created for law making in the field of data protection. The pillar structure will be abolished and with Article 16 TFEU a single legal basis is created for data protection in almost all areas of EU law (see Chapter 2). This does not necessarily mean that the implementation of data protection principles for police and justice should be the same as the rules in other parts of society. Declaration 21, attached to the Lisbon Treaty claims that specific rules for law enforcement area 'may prove to be necessary'.

102. Data protection and data exchange will be important focuses in the Stockholm Programme. Decision making will be based on the notion of the right balance between the needs of law enforcement and the requirements of data protection. New measures should only be taken after a proper evaluation of the existing legal framework.

103. Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial cooperation in criminal matters must be implemented by the Member States before 27 November 2010. This Framework Decision can be seen as a first step towards a general framework in the former third pillar but is far from complete. It is only applicable in cross border situations. It seems to lack essential elements and tools to effectively deal with the changing working methods in the area of law enforcement.

***Changing emphasis in law enforcement***

104. The last years have shown a shift of emphasis in working methods of the police and the judicial authorities, as far as the use of (personal) information is concerned. This shift was the result of growing needs of the use of information, in order to face new threats resulting from terrorism and organised crime and was stimulated by the technological developments over the last years.

105. The shift of emphasis has several dimensions:

- The use of information focuses on earlier stages in the chain: in addition to the traditional use of information for the investigation and the detection of a specific crime, information is gathered and exchanged in order to prevent possible criminal acts ('preventive policing').
- The use of information focuses on a wider group of persons. Information is gathered and exchanged, not only on persons that are directly related to a crime such as suspects or witnesses, but also on wider groups of the population who are not involved in an investigation (e.g. travellers, users of payment services, etc.).
- The information that is used is more and more technology based. Technology even links disparate factors to predict future behaviour of individuals by means of automated tools (data mining, profiling).
- The information that is used is of a different nature. Information use relies not only on objectively determined information (hard data) but also on information based on evaluation and analysis in the framework of an investigation (soft data). Besides, the distinction between the two may vary depending on the Member States.

- The increased use for preventive purposes of personal information originating from the private sector, like for instance banking/financial data, and passenger data collected by air carriers and CRS.
- Information that is collected for a given, legitimate purpose is increasingly used for different, at times incompatible purposes and tends to growingly converge. Interoperability between systems is an important development but is not a purely technical issue, in particular in view of the risks of interconnection of databases having different purposes.
- More authorities are involved in the use of information, not just police and judicial authorities *strictu sensu* but also other public authorities like authorities responsible for border control and tax authorities, but also national security services.

106. This changing emphasis in law enforcement has led to a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector. The technological possibilities to easily combine information may have a profound impact on the privacy and data protection of all citizens and on the very possibility for them to really enjoy and be able to exercise their fundamental rights, in particular whenever freedom of movement, freedom of speech, and freedom of expression are at issue.

***Challenges for data protection***

107. Against this background, the challenges for data protection are immense. A future legal framework should in any event address the following phenomena:

- Tendencies may lead towards a more or less permanent surveillance of all citizens, often referred to as the surveillance society. An example would be the combined use of intelligent CCTV-camera's and other tools, like an Automatic Number Plate Recognition, registering all cars entering and exiting a certain area.
- Databases may be used for data mining, and risk assessments of individuals can be composed on the basis of profiling of individuals. This might stigmatize persons with certain backgrounds.
- Analyses made on the basis of general criteria run the risk of high inaccuracies, leading to a high number of false negatives and false positives.
- The processing of personal data of non-suspects becomes more important. Specific conditions and safeguards are needed in order to assess their legitimacy and proportionality and to avoid prejudice for persons that are not (actively) involved in a crime.
- There is an increased use of biometric data, including DNA, which presents specific risks.

***Conditions for law and policy making***

108. The growing number of sector-specific initiatives adopted or planned may easily lead to overlapping or even distortion measures. Therefore, there may be added value in basing information exchange on a consistent strategy, provided that data protection is fully considered and is an integrated part of this strategy.[34]

---

[34] A European Information Management Strategy, as currently elaborated by the Council, may - if done correctly - in this context prove to be a useful instrument.

109. The need for evaluation of the existing legal instruments and their application is of utmost importance and should take into account the costs for privacy. Evaluation of existing measures should take place before taking new measures. Additionally, a periodic review of existing measures should take place.

110. Transparency is an essential element. Clear information should be available to data subjects on the use of the information collected and the logic underlying the processing and should only be limited if necessary in individual cases to not jeopardise investigations and for a limited period of time. Access and rectification rights of the data subject should be addressed in a cross border context to avoid that the data subject looses control.

111. Special attention is needed for transparency and democratic control in the legislative process. Privacy impact assessments, appropriate forms of consultation of data protection authorities and an effective parliamentary debate, at national and EU level, should play an important role.

112. The architecture of any system for storage and exchange of personal data should be well elaborated. Some general considerations are:

- Privacy by design and PETS (certification scheme) should determine the architecture. In the area of freedom, security and justice where public authorities are the main actors and every initiative aimed at increasing surveillance of individuals and increasing the collection and use of personal information could have a direct impact on their fundamental right to privacy and data protection, those requirements could be made compulsory.
- Purpose limitation and data minimization should remain guiding principles.
- Access to large databases must be configured in such a way that in general no direct access on line to data stored is allowed, and a hit/no hit system or an index system is in general considered preferable..
- The choice between models with central storage, meaning systems with a central database on EU-level and decentralised storage should be made on transparent criteria and in any event ensure a solid arrangement providing for a clear definition of the role and responsibilities of the controller/s and ensuring the appropriate supervision by the competent data protection authorities.
- Biometric data should only be used if the use of other less intrusive material does not present the same effect.

113. The external dimension. It should be avoided that the stringent regime for the exchange of personal data within the EU will be circumvented. The relations with third states should be based on a clear framework, binding on all parties and on the notion of adequacy. The adequacy regime should be assessed following an evaluation by the national DPAs, if necessary through common mechanisms ensuring consistent implementation and effectiveness.

114. Special attention - including where necessary tailor made safeguards for data protection - is needed for large scale information systems within the EU.

115. Independent supervision, as well as judicial oversight and remedies should be properly addressed. This includes in any event adequate resources and competences for independent supervision.

116. Cooperation between DPAs in charge of ensuring lawfulness of data processing should be strengthened in all matters and integrated in the legal framework, also by envisaging stable mechanisms similar to those currently applying to first pillar matters, in order to foster a harmonised approach across the EU and beyond.

*For the Art 29 Working Party*

The Chairman

Alex Türk

*For the Working Party on Police and Justice*

The Chairman

Francesco PIZZETTI

# APPENDIX C

# Privacy by Design:

## Essential for Organizational Accountability and Strong Business Practices


November 2009


Information and
Privacy Commissioner,
Ontario, Canada

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

## Acknowledgements

The authors wish to acknowledge Fred Carter, Senior Policy and Technology Advisor, Policy Department at the Information and Privacy Commissioner's Office, Ontario, Canada for his input on this paper, as well as Susan Smith, Americas Privacy Officer, Hewlett-Packard Company and staff at The Centre for Information and Policy Leadership at Hunton & Williams LLP.

# Table of Contents

# Foreword

The proposition that "privacy is good for business" is one that is enshrined in all Fair Information Practices (FIPs) around the world and, through them, in the many laws and organizational practices upon which they are based. By setting out universal principles for handling personal data, FIPs seek to ensure the privacy of individuals *and* to promote the free flow of personal data and, through them the growth of commerce.

The enduring confidence of individuals, business partners and regulators in organizations' data-handling practices is a function of their ability to express the FIPs' core requirements. These are: to limit collection, use and disclosure of personal data; to involve individuals in the data lifecycle, and to apply appropriate safeguards in a thoroughgoing manner. These requirements, in turn, are premised upon organizational openness and accountability. The ultimate results – which are highly desirable – include enhanced trust, improved efficiencies, greater innovation, and a heightened competitive advantage. Privacy *is* good for business.

But the early FIPs drafters and adopters had in mind large mainframe computers and centralized electronic databases. They could never have imagined how leapfrogging revolutions in sensors, bandwidth, storage, and processing power would converge into our current hyper-connected "Web 2.0" networked world of ubiquitous data availability.

It has become trite to observe that data is the lifeblood of the new economy, but who today can truly grasp how large the arteries are becoming, how they are multiplying, where they may lead, and to what end? Everywhere we see near-exponential growth of data creation, transmission, use and storage, by an ever-expanding universe of actors, somewhere out there in the opaque "cloud." Most of this data is personally-identifiable. And most of it is now controlled by someone other than the individual himself or herself. Thanks to new information flows, today we enjoy unprecedented and nearly unimaginable new services and benefits, but these have been accompanied by unprecedented and once unimaginable privacy threats and harms. Some say that privacy is effectively dead or dying in the information age. We say that it is not, but it *is* rapidly changing shape.

The need for organizational accountability remains constant – indeed, it has become more urgent today than ever before. What is changing are the *means* by which accountability may be demonstrated, whether to individuals, regulators or to business partners. Beyond policy statements, what is needed now are more innovative and more robust methods for assuring that personal data is, in fact, being managed responsibly.

There are many paths to enhanced accountability and assurance, typically involving a mix of technology, policies and practices, and of law and regulation. More than ever before, a comprehensive and proactive *Privacy by Design* approach to information management is called for – one which assures an end-to-end chain of custody and responsibility right from the very start.


Scott Taylor
Chief Privacy Officer
Hewlett-Packard Company

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Martin E. Abrams
Senior Policy Advisor and Executive Director
Centre for Information Policy Leadership,
Hunton & Williams LLP

# I Introduction

Professor Paul A. Schwartz recently wrote:

> "Companies are now putting internal policies in place, centered on forward looking rules of information management and training of personnel. Such policies are, at the very least, a necessary precondition for an effective accountability regime that develops a high level of privacy protection."[1]

An accountability-based regulatory structure is one where organizations are charged with societal objectives, such as using information in a manner that maintains individual autonomy and protecting the individual from social, financial and physical harms that might come from the mismanagement of information, while leaving the actual mechanisms for achieving those objectives to the organization. One of the best conceptual models for building in the types of controls suggested by Professor Schwartz is *Privacy by Design*. The best in class companies in Schwartz's study, "Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment," are using *Privacy by Design* concepts to build business process that use personal information robustly with clear privacy-protective controls built into every facet of the business process. In other words, *Privacy by Design* and accountability go together in much the same way that innovation and productivity go together.

Accountability is the governance model that is based on organizations taking responsibility for protecting privacy and information security appropriately and protecting individuals from the negative outcomes associated with privacy-protection failures. Accountability was first framed as a privacy principle in the OECD Privacy Guidelines.

The Centre for Information Policy Leadership at Hunton & Williams LLP has recently acted as secretariat for the Galway project that defined the essential elements of accountability.

The conceptual model, *Privacy by Design*, was developed by Ontario Privacy Commissioner Ann Cavoukian in the 1990s to address the development of technologies, but she has since expanded it to include business processes.[2]

Hewlett Packard is in the midst of implementing an accountability tool built on both accountability principles and the key concepts of *Privacy by Design*. HP's accountability tool is an example of the trend described by Professor Schwartz.

This paper discusses the essential elements of accountability, *Privacy by Design* principles, and provides an example of a control process that uses the principles to implement the essential elements.

1 "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment," Paul A Schwartz, a working paper by The Privacy Projects, October 2009.
2 "Privacy by Design," Ann Cavoukian, Ph.D., January 2009.

# II *Convergence of Accountability and Privacy by Design*

Accountability as both a basic privacy implementation and enforcement principle dates to the approval of the OECD Privacy Framework in 1980. But it is only today that the privacy community is beginning to understand what is meant by accountability-based privacy governance, and how it impacts the structuring of a privacy program. The growth of Binding Corporate Rules in the European Union, Cross-Border Privacy Rules in APEC, Safe Guard concepts in the United States, and data transfers compliant with the Personal Information and Electronic Documents Act (PIPEDA) in Canada has made clear direction on accountability crucial. The Galway project published a paper called "Data Protection Accountability: The Essential Elements," in October 2009 that enumerated five essential elements for accountability. The paper was developed with a distinguished group of privacy experts from privacy enforcement agencies, government, academia, civil society and business, and facilitated by the Office of the Irish Data Protection Commissioner, and chaired by the Centre. The essential elements make it clear that accountability comes from privacy protections based on commitment to a program where privacy is built into all business processes.

Over a decade ago Ontario Privacy Commissioner Ann Cavoukian began discussing the virtues of building privacy into technology from the start. She calls that concept "*Privacy by Design*." While *Privacy by Design* began as a technology concept, it has evolved into a conceptual model for building an entire privacy program.

The fact is that *Privacy by Design* and accountability go together like innovation and high productivity. You can have one without the other, but it is hard.

A number of companies have been building programs where privacy is built into core business processes. One can find them in many industries and both business to business and business to consumer industries. Hewlett Packard has spent the last three years building a program called the "Accountability Model Tool" that integrates the technological concepts of *Privacy by Design* with the organizational commitment required for accountability. The accountability tool is now being implemented in the HP businesses that serve customers in 170 countries through 400,000 employees. This paper will describe accountability's essential elements, the components of *Privacy by Design* and will use the HP "Accountability Model Tool" as an example of how leadership companies are building privacy in.

# III The Essential Elements of Accountability

Accountability has a strong basis in privacy law and oversight. The Organization for Economic Cooperation and Development ("OECD") included accountability as principle eight in the Guidelines. Accountability is principle nine in the Asia Pacific Economic Cooperation forum ("APEC") Privacy Framework. It is principle one in the Model Code for the Protection of Personal Information (incorporated into Canadian law), and is a principle in the joint proposal drafted for consideration at the 31st International Conference of Data Protection and Privacy. However, none of those documents defined accountability as it applies to privacy.

The Centre for Information Policy Leadership at Hunton & Williams LLP, in a process facilitated by the Office of the Irish Data Protection Commissioner, brought together a group of experts to consider the essential elements of accountability in a project called the Galway Accountability Project. The Galway project held two experts discussions in Dublin, Ireland, the second sponsored by the OECD and the Business and Industry Advisory Council to the OECD. For the purpose of those discussions the group used the following working definition of accountability:

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.*

For an organization to have the capabilities to demonstrate its willingness to meet expectations based on law and organizational promises, and to have confidence in its ability to be answerable, the organization must have all aspects of privacy and information security under control. This is reflected in the essential elements of accountability:

1. An organization's commitment to accountability and adoption of internal policies consistent with external criteria
2. Mechanisms to put privacy policies into effect, including tools, training, and education
3. Systems for internal ongoing oversight and assurance reviews and external verification
4. Transparency and mechanisms for individual participation
5. The means for remediation and external enforcement.

To be an accountable organization a company must have rules that are based on an external measuring stick such as data protection laws, industry self regulatory guidance, or guidance such as the OECD guidelines or APEC principles. Those policies must then be committed to by the organization at the highest level. The organization must have all the pieces in place to assure that the people who work at (employees) and for the organization (vendors) can be successful in implementing its policies and commitments. Furthermore, the organization must have internal measurement devices in place to assure the actions meet the words, and an external process to verify performance.

*Privacy by Design* is a process map for putting the essential elements of accountability into effect.

# IV *Privacy by Design: 7* Foundational Principles

Ontario Privacy Commissioner Ann Cavoukian has written that *Privacy by Design* is achieved by building fair information practice principles ("FIPs") into information technology, business practices, and physical design and infrastructures. This links with the accountability concepts in two ways. First the essential elements require that policies and practices must be based on external criteria. FIPs are the sum and substance of OECD and APEC privacy guidance, built into the European Union Data Protection Directive, and Canada's PIPEDA. They are examples of the external criteria referenced in the essential elements. Second, is the concept that the FIPs need to be built into all the processes from technology development to the physical structure of facilities. This too is required by the essential elements.

Dr. Cavoukian has also written that *Privacy by Design*'s objectives may be accomplished through adoption of seven foundational principles:

1. Proactive not Reactive; Preventative not Reactive
2. Privacy as the Default
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Lifecycle Protection
6. Visibility and Transparency
7. Respect for User Privacy.

Each of the foundation principles link to the essential elements of accountability.

1. ***Proactive not Reactive; Preventative not Reactive*** Proactive not reactive speaks to the accountability concept of having all the privacy policies as well as mechanisms in place so trained practitioners will see and resolve privacy issues before they turn into problems.
2. ***Privacy as the Default*** Accountability requires clear organizational rules with an explicit commitment to the policies that are the basis for those rules. Those rules will make clear that information should only be collected and used in a manner that is respectful of individual expectations and a safe information environment.
3. ***Privacy Embedded into Design*** Accountable business processes work best when privacy is embedded into design. This would be part of the mechanisms to implement policies.
4. ***Full Functionality – Positive Sum, Not Zero-Sum*** Organizations that understand privacy and bake privacy in have a better understanding of the risks to both the organization and to individuals. Organizations that build privacy in know how to create economic value while protecting individual privacy. The Centre

has being saying that clear privacy rules and methodologies create confident organizations that do not suffer from reticence risk.

5. ***End-to-End Lifecycle Protection*** End-to-end lifecycle protection informs the accountable organization that it must build privacy into every process from the assessment before data is collected to the oversight when data is retired.

6. ***Visibility and Transparency*** Principle six requires an organization to be open and honest with individuals. The accountable organization stands ready to demonstrate that it is open about what it does, stands behind its assertions, and is answerable when questions arise. The accountable organization provides the information necessary for individuals to participate consistent with the OECD individual participation principle. This is echoed in the *Privacy by Design* visibility and transparency principle.

7. ***Respect for User Privacy*** Lastly, the accountable organization must collect, use, store, share and retire information in a manner that is consistent with respect for the individual's privacy.

# V Leadership Companies are Demonstrating *Privacy by Design*

In the course of the Centre's research we looked at leadership companies' information policy policies and practices. We saw information aggregators with excellent assurance review processes, software companies that build privacy protections into processes, and outsourcing companies with excellent checks and balances. "Managing Global Information Privacy: A Study of Cross-Border Data Flows in a Networked Environment" by Paul Schwartz looked at the processes that six companies had for protecting privacy in an application that required data to cross borders. Professor Schwartz found all of the organizations to have very professional processes to assure data is used and protected appropriately.[3]

While there are many corporate examples of *Privacy by Design*, Hewlett Packard makes an interesting case study since they are in online retail, indirect retail, business-to-business, and services.

## *Privacy by Design* – an HP Example

Globalization and new technologies are fundamentally changing how companies communicate and market to customers and prospects. It changes both the opportunities and the risks for individuals and organizations. Many of these technologies, including Web 2.0, user-generated content, and social media are straining traditional frameworks. And as the collection of data becomes more ubiquitous, data mining, analytics and behavioral targeting are growing more and more common and complex.

Laws and regulations often lag behind the practical realities of new technologies. This points to the fact that companies need to develop mechanisms that balance the tensions of using information robustly, yet ensure responsible decision making. Regulators and advocacy organizations are also looking to companies to demonstrate their capacity in upholding obligations and that their use and management of data is under control.

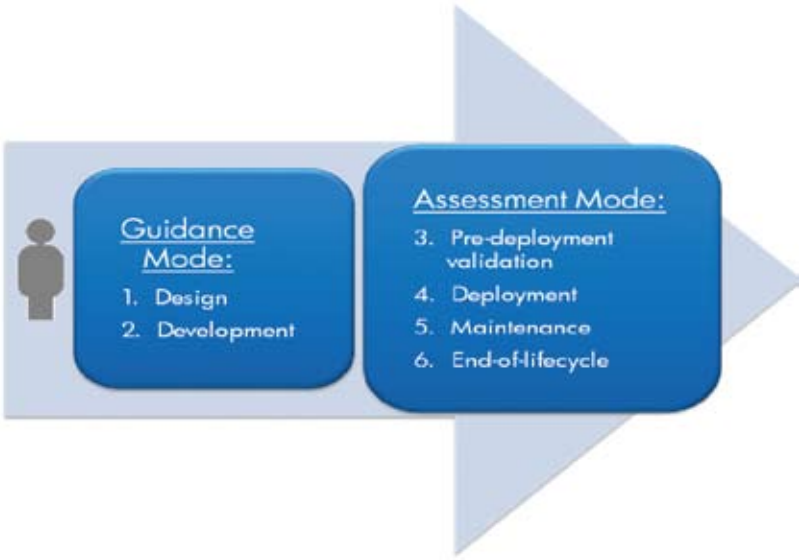
The *Privacy by Design* concepts, originally conceived by Commissioner Cavoukian, can be instantiated within a company in many ways. In an attempt to drive accountability throughout the enterprise, and ensure privacy considerations are taken into account at the earliest stages of a product's lifecycle, HP has developed a tool that guides employees.

3 "Managing Global Information Privacy" is available on the OCED website (www.oecd.org) and The Privacy Projects, a NGO that sponsored the research

As this paper articulates, accountable practices can be broken down into three major categories: 1. Policies and Commitment, 2. Implementation Mechanisms, and 3. Assurance Practices. It is in the development of implementation mechanisms where *Privacy by Design* becomes critical. Employees of an organization must understand how to put policies, obligations, and values into effect. And to minimize business investment, reputation and compliance risks, employees need to consider privacy principles prior to design.


If a product or program is broken down into simple stages, it becomes clear when *Privacy by Design* guidance versus assessment needs to be applied. In the stages of Design and Development, the Privacy Office should provide proactive guidance so that privacy considerations can inform the planning stage. This is often missed and can result in a program being delayed or cancelled based on later privacy concerns.

Early guidance related to privacy becomes a tremendous value added to the organization. If caught early, privacy pitfalls can be avoided and good privacy practices embedded into the design of the program.



In the Pre-deployment, Deployment, Maintenance, and End-of-life stages, the Privacy Office needs to do more than just guide – they need to provide robust assessment mechanisms to ensure compliance with local laws, obligations, policies, and company values.

The assessment results should be documented and reviewed by the Privacy Office, consultation provided as necessary, and ultimately approved prior to deployment. After product or program launch, triggers should exist to ensure deployment was consistent with expectations and that end of life actions are taken when appropriate.

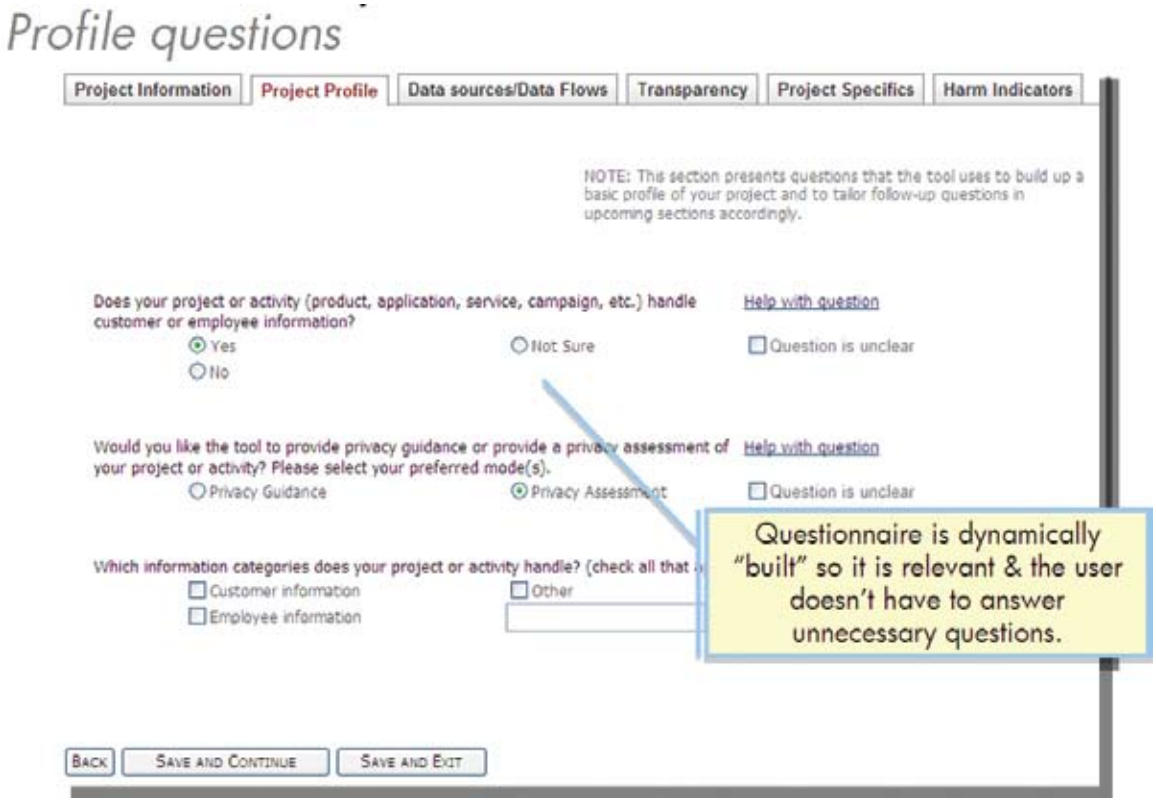
For many years, HP has been managing this *Privacy by Design* lifecycle through education, training, and encouraging employees to engage their privacy account manager at the early stages of design and development. As successful as this can be, it relies on employees thinking about privacy at the right time, knowing who to contact, and not feeling intimidated.

To solve these challenges and take *Privacy by Design* to a new level, the HP Privacy Office partnered with research scientists in HP Labs to develop a solution called the Accountability Model Tool. It combines the guidance in HP's existing Privacy Rulebook with a set of contextual, dynamically-generated questions. These two knowledge bases are connected through a sophisticated rules engine to help guide employees.

It allows employees and teams – working on simple marketing campaigns or complex product solutions – to see what privacy considerations need to be designed into their program. As described above, it works in both a guidance mode and in an assessment mode – depending on the lifecycle stage of the program.

Through company policy, employees who are collecting or using PII are required to assess their programs using this tool. It is easily accessible from the internal Privacy Intranet site. Using their digital badge they are authenticated and their basic contact and organizational information is automatically populated in the tool. All of their past projects are also accessible. This is important if an employee changes jobs or leaves the company so the Privacy Office knows which organization remains accountable for a program.

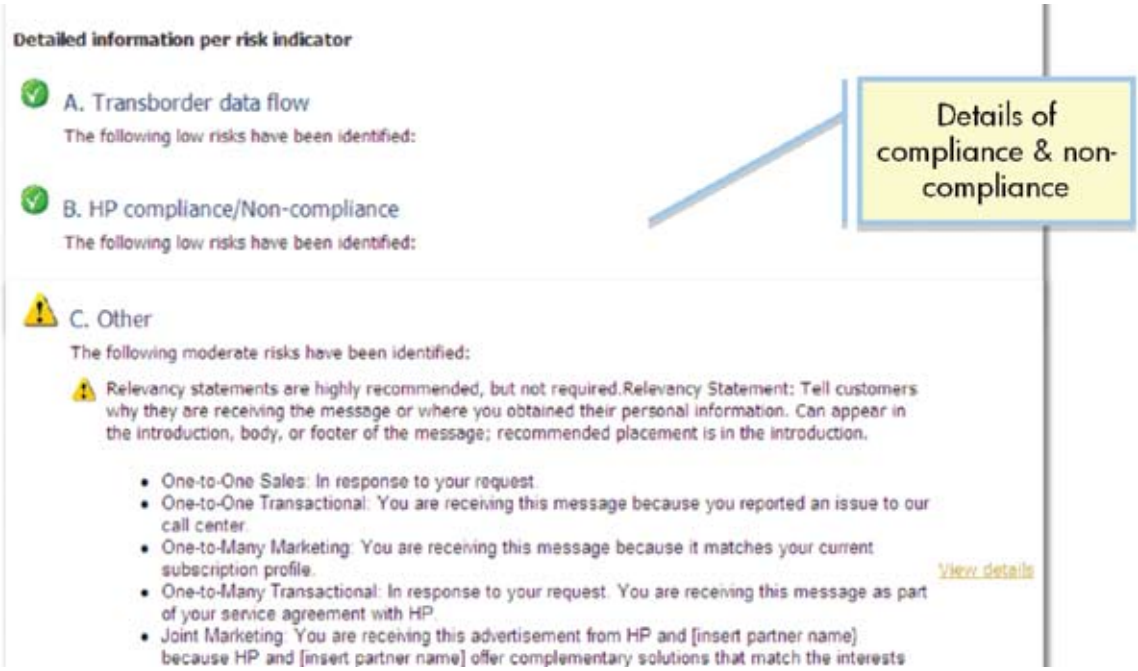
The tool begins by asking simple questions about the nature of their project. If it involves the collection or use of PII, they are presented with further contextual questions. As they answer each question, the next set of questions is dynamically generated based on how they answered prior questions. This is a critical component of success. The Privacy Office has found that each employee understands his or her area of expertise (e.g., e-mail marketing, product development, or employee relations), but when guidance and rules are not contextualized to their area of work, it becomes a daunting task for them to sift through hundreds of pages of rules or guidance and know how to apply them to their program. This tool is meant to narrow the context into exactly what they are doing and provide the associated guidance.



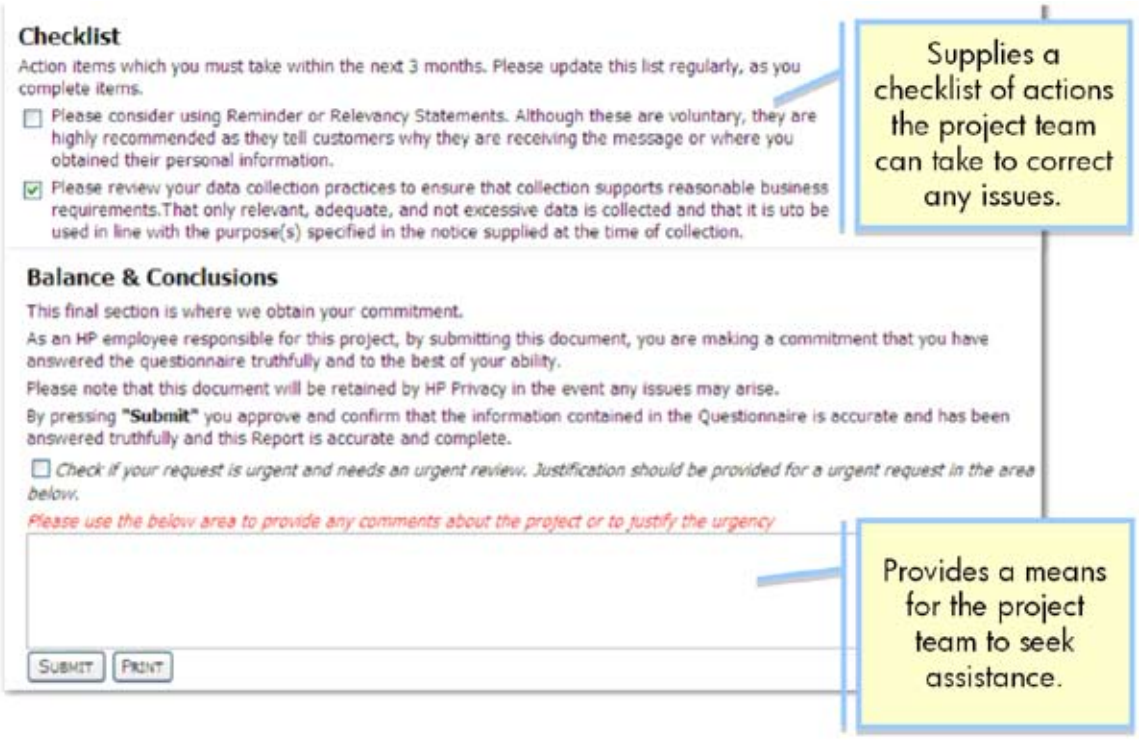

By asking employees contextual questions – and linking their answers immediately against the rules database – the tool not only guides, but educates the employee on good privacy practices. For each question, terms are defined by using text rollovers and help is provided that links the employee directly into the HP Privacy Rulebook. They can also check a box that says "Question is Unclear." This allows the Privacy Office to track trends and improve the delivery of questions if patterns evolve.

The tool takes the employee through a series of questions related to the profile and nature of the project, data sources and flows, transparency, compliance, and indicators of any issues that might arise or surprise the data subject. Once the employee has completed the questions, a report is generated that shows an overall rating, as well as areas of compliance and non-compliance.


For areas of non-compliance, reasons are provided, including links to further information and checklists that can be used to achieve compliance.




Once the employee has made the appropriate modifications, he or she can submit their report to the HP Privacy Office where it will be reviewed and archived.




They are attesting to the truth and accuracy of their statements and will be held accountable. For any areas of concern, the Privacy Office must approve the program prior to deployment.

Once approved, the program information is warehoused in the database. It is maintained for future use as well as a trigger for ongoing assurance monitoring. This database of projects provides a real-time dashboard for the Privacy Office, allows improved ongoing communications and ensures that if laws or regulations in a country change that programs can be modified as appropriate.

This is a new program for HP and has just been deployed. It is a valuable tool along with ongoing efforts in training, implementation standards, compliance management, and audit. It achieves Commissioner Cavoukian's concepts for *Privacy by Design* in a manner that is systematic, predictable and repeatable – and ultimately will drive a richer culture of privacy within the enterprise. It also will enable HP to better demonstrate commitment and capacity in upholding privacy promises and obligations.

# VI Conclusion

In this paper, we have seen an excellent example of how enhanced privacy accountability and assurance can be achieved within an organization by applying *Privacy by Design* principles, in a thoroughgoing manner.

So imperative today are the goals of enhanced accountability and assurance, so universal are the PbD principles, and so diverse are the contexts within which these principles may be applied, that the future of privacy in the 21st century information age may be limited only by our collective imagination and will.

There are virtually infinite ways by which organizations can creatively "build privacy in" to their operations and products, to earn the confidence and trust of customers, business partners and oversight bodies alike, and to be leaders in the global marketplace.

We need to acknowledge and celebrate these innovations and successes, and steadily build upon them.

# About the Authors

**Ann Cavoukian, Ph.D.**, Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of *Privacy by Design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Dr. Cavoukian also serves as the Chair of the Identity, Privacy and Security Institute at the University of Toronto, Canada. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow *Privacy by Design* and hopes to make it go "viral."

**Martin E. Abrams**, Senior Policy Advisor and Executive Director, Centre for Information Policy Leadership, Hunton & Williams LLP

Martin Abrams is Executive Director of the Centre for Information Policy Leadership at Hunton & Williams LLP, a global privacy and information security think tank, and an advisor to the Business Forum for Consumer Privacy. Mr. Abrams brings more than 30 years' experience as a policy innovator to the Centre, where he pursues practical solutions to privacy and security problems. He is a leading theorist on global transfers of data based on accountability, and has led the movement in the U.S. to adopt harms-based approaches to privacy. He was a leader in developing layered privacy notices, and is currently working to bridge cultural differences in privacy. Mr. Abrams has led privacy programs on five continents, and is part of the APEC Data Privacy Subgroup.

**Scott Taylor**, Chief Privacy Officer, Hewlett-Packard Company

As head of HP's privacy and data protection efforts worldwide, Scott Taylor is responsible for global privacy strategy, policy, governance, and operations. In this role, he is a member of HP's Ethics & Compliance Council, Global Citizenship Committee, and chairs HP's Privacy & Data Protection Governance Board. Taylor and his team work with HP business groups, regions and corporate functions to assure the implementation of HP's privacy policies and programs and integrate privacy into product and services development across the company. He serves as HP's global representative with external policy-makers, media, NGOs and customers in the area of privacy and data protection. Taylor serves on the Board of Directors for The Business Forum for Consumer Privacy, as the Chairman of the Executive Council at The Center for Information Policy Leadership, and on the Board of Directors for the Council of Better Business Bureaus. Taylor has been with HP for 22 years. Previously he led HP's global Internet program, part of the Global Operations Organization. In that role, he and his team handled Internet strategy, customer experience, e-business policies, standards, worldwide site management, and operations. Taylor led the team that launched HP's Internet presence in 1994 and managed it for 12 years. Prior to that, Taylor was responsible for HP's direct marketing function, part of the Corporate Marketing & International Services Organization.


Information and Privacy Commissioner of Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario M4W 1A8
Canada
Telephone: 416-326-3333
Fax: 416-325-9195
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

The Centre for Information Policy Leadership
at Hunton & Williams LLP
1900 K Street, NW
Washington, DC 20006
USA
Telephone: 202-955-1500
Fax: 202-778-2201
Website: www.informationpolicycentre.com

Hewlett-Packard (Canada) Co.
5150 Spectrum Way
Mailstop 6H72
Mississauga, Ontario L4W 5G1
Canada
Telephone: 905-206-4725
Fax: 905-206-4739
Website: www.hp.ca



Information and Privacy Commissioner, Ontario, Canada

THE CENTRE FOR INFORMATION POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

C O A L I T I O N  F O R  O N L I N E  A C C O U N T A B I L I T Y

WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP ● 1818 N STREET N.W., 8TH FLOOR ● WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7906 ● FAX: (202) 355-7899 ● E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

Before the United States Department of Commerce
National Telecommunications and Information Administration
International Trade Administration,
National Institute of Standards and Technology

# Response of the Coalition for Online Accountability

to Notice of Inquiry on

# Information Privacy and Innovation in the Internet Economy

(75 Fed. Reg. 21226, Apr. 23, 2010)

[Docket No. 100402174–0175–01]

Submitted by
Steven J. Metalitz
Mitchell Silberberg & Knupp LLP

Counsel to Coalition for Online Accountability

June 14, 2010

American Society of Composers Authors & Publishers (ASCAP)
Broadcast Music Inc. (BMI)
Recording Industry Association of America (RIAA)
Entertainment Software Association (ESA)
Motion Picture Association of America (MPAA)
Software & Information Industry Association (SIIA)
Time Warner Inc.
The Walt Disney Company

*Counsel: Steven J. Metalitz (met@msk.com)*

The Coalition for Online Accountability (COA) appreciates this opportunity to respond to the Notice of Inquiry on Information Privacy and Innovation in the Internet Economy ("NOI"). 75 Fed. Reg. 21226 (Apr. 23, 2010).

About COA

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners, all of them deeply engaged in the use of the Internet to disseminate creative works. These are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. The Coalition's main goal since its founding a decade ago (as the Copyright Coalition on Domain Names) has been to preserve and enhance online transparency and accountability. A predominant focus has been to ensure that data concerning domain name registrations and IP address allocations remain publicly accessible, accurate and reliable, as key tools against online infringement of copyright. This data is also essential in combating trademark infringement, cybersquatting, phishing, and other fraudulent acts online.

Introduction

The focus of the NOI appears to be on (1) businesses that collect information from or about individual consumers in the course of engaging in e-commerce activities, and (2) the individuals themselves, whose data could be manipulated or abused by those collecting businesses. The perspective of COA participants is somewhat different: the protection of the legal rights of creators and distributors of copyrighted material in the e-commerce environment. Not surprisingly, this perspective does not correspond directly to the topic areas specifically identified in the NOI. Our perspective is, however, directly responsive to the question posed by the NOI: "whether current privacy frameworks, or frameworks that are in development, create barriers to innovation on the Internet." NOI at 21228.

COA and its members fully support the NOI's goal, "to identify policies that will enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy." Id. at 21227. The online environment offers exciting opportunities for new ways to create, deliver and disseminate creative works. Through this medium, works such as musical compositions, recordings, movies, and videogames are reaching ever wider audiences through ever more diverse distribution and performance channels. We believe that developing and safeguarding a thriving online marketplace for such works is a key element of the innovation that a healthy information economy requires.

Widespread infringement of copyright has been a pervasive feature of the online environment in recent years. This represents a clear threat to a healthy information economy and to the innovation that underpins it. The substantial investments in innovation that copyright owners undertake in order to develop a legitimate online marketplace in their works cannot be sustained without adequate protections against copyright theft. We appreciate the consistent and strong support voiced by the leadership of the Department of Commerce and its constituent

agencies for the central role of intellectual property enforcement in promoting innovation in the Internet economy. See, e.g., remarks of Under Secretary Kappos before Center for American Progress (June 2,2010) at http://www.uspto.gov/news/speeches/2010/Kappos_CAP_speech.jsp ("strong intellectual property protection and its effective enforcement will fuel innovation and jump-start our economy"); remarks of Assistant Secretary Strickling before the Media Institute (Feb. 24, 2010) at http://www.ntia.doc.gov/presentations/2010/MediaInstitute_02242010.html (enumerating as a key challenge "How do we protect against illegal piracy of copyrighted works and intellectual property on the Internet while preserving the rights of users to access lawful content?").

COA participants are strongly committed to the goal of clear and enforceable privacy protections in the online environment. Without such protections, the necessary public confidence in the information economy can be jeopardized. But widespread disrespect for intellectual property rights online could have the same deleterious effects. If the online marketplace comes to resemble a thieves' bazaar, both legitimate merchants and prudent customers will be reluctant to enter it.

All COA participants, like others in the copyright sector, actively engage in efforts to detect and to prevent online copyright theft, and have invested heavily in programs to do so. These efforts depend upon our continued ability to access and process publicly available information concerning illegal online activities, and to share this information as appropriate with other key stakeholders in the Internet environment, including Internet service providers, e-commerce marketplaces, and law enforcement agencies. Maintaining access to this information, and taking steps to ensure that it is accurate, reliable, and current, will not threaten the privacy interests of consumers. Rather, it will enhance their online experience and encourage greater participation in the information economy.

In this submission, COA wishes to emphasize that privacy policies must be carefully calibrated to minimize adverse impacts on legitimate activities carried out to protect copyright and other intellectual property rights online, through the use of this publicly available data. We are confident that this calibration is fully consistent with robust privacy protections for the personal information of consumers and their legitimate online activities. We urge NTIA and the other DOC agencies participating in the Task Force to keep in mind the need for such calibration, both in the context of developing improved privacy policies under U.S. law, and in engaging with our trading partners on these issues.

Two brief examples of the needed calibration can be provided. The first involves data on registrants of domain names, while the second concerns Internet Protocol addresses.

Domain Name Whois

Domain name registration information has been publicly accessible through a service labeled Whois since the earliest days of the domain name system, even predating the World Wide Web. Public access to Whois data is essential to the investigation and prompt resolution of instances of copyright piracy and trademark counterfeiting online. The investigation of virtually every such case involves the use of Whois data. For example, when an investigator seeks to

determine who is responsible for a website where infringing activity is taking place, a review of the Whois data for the domain name which resolves to that site is usually the first step. Once the responsible party has been identified, the copyright owner or its agent is in a position to request that the party obtain a license or cease the infringing activity, or, where appropriate, to begin enforcement action.

But Whois data's valuable uses are by no means limited to the sphere of intellectual property protection. Access to Whois data is critical to dealing with instances of phishing, distribution of malware, network attacks, and online frauds of all kinds. This data is essential to law enforcement, of course, but also to private parties such as copyright and trademark owners, whose independent enforcement of their rights allows law enforcement to conserve scarce resources. Indeed, virtually every Internet user benefits from public accessible Whois. Whois provides greater transparency, so that end users know more about the parties with whom they – or their children – are interacting online. This is a fundamental prerequisite to building public confidence in the information economy.

For these reasons, COA urges the Commerce Department to maintain and redouble its long-standing efforts to preserve public access to Whois data, and to improve its quality, reliability, and timeliness. The locus for such efforts includes, though it is by no means limited to, the Internet Corporation for Assigned Names and Numbers (ICANN), where binding policy on these issues for the generic Top Level Domains is hammered out, and where continued U.S. leadership within the ICANN Governmental Advisory Committee is especially critical.

While many other national governments share this perspective on the importance of maintaining public access to Whois, some commentators insist that the long-standing system of publicly accessible Whois is incompatible with the privacy laws of some countries. It is claimed that these laws require restrictions on what data about domain name registrants is made available through Whois, and/or that these laws demand that public access to Whois be wholly or substantially suppressed. Such an expansive interpretation of privacy laws threatens to cloud the transparency needed for a sound information economy. As such issues arise, we urge the Commerce Department to engage with our trading partners to ensure that the implementation of their national privacy laws accommodates continued unfettered access to Whois data for the valuable purposes summarized above.

IP Address Information

The label "Whois" also refers to information about the allocation of blocks of Internet Protocol (IP) addresses, which are the numeric addresses for all resources connected to the Internet. Access to this information is extremely important for enforcement against copyright piracy, trademark infringement, and other forms of misconduct carried out online. When such misconduct is associated with a particular IP address, Whois enables the investigator to identify the Internet service provider or other entity to which the IP address was initially assigned, and also to learn of sub-allocations to other providers, though rarely, if ever, to the end-user. Accessibility and reliability of IP address Whois data, including ensuring that all sub-allocations are entered into the database and kept up to date, are also critical issues for attention from the U.S. government.

Since IP address information travels routinely and visibly with many communications over the Internet, and since even the Whois information associated with such addresses generally cannot, by itself, identify any end-user, public access to and use of such data should have little if any impact on privacy or free expression concerns. However, under expansive interpretations of their national privacy laws, government agencies and courts in some countries have erected obstacles to the collection and use of IP address information in private sector efforts to enforce copyright in the online environment.[1]

These interpretations are particularly problematic to the extent that they impede cooperative efforts of right holders, ISPs and other information economy stakeholders against copyright theft. For instance, when an investigator acting on behalf of a copyright owner observes high-volume copyright infringements by a user of an illicit peer-to-peer (p2p) service, questions have been raised under some national privacy laws about the collection of the user's IP address by the investigator; the furnishing of that address to the ISP to which the address has been allocated; and the linking of that address by the ISP to a particular subscriber, for the purpose of forwarding a warning notice regarding the infringing activity. In this example, expansive interpretations of privacy laws clearly disserve the goal of promoting innovation in the information economy. Such a privacy law framework could make it virtually impossible for responsible parties to work together to address illegal activity that, left unchecked, could easily inundate the legitimate online marketplace in copyrighted works.

To a considerable extent, the impediments to collecting and using IP address data in online copyright enforcement efforts flow from the classification of such information as "personal data," the collection or processing of which is extensively regulated under the privacy laws of a number of countries. Legislation to regulate collection and use of IP addresses as "personally identifiable data" under US law has also been proposed. See, e.g., Staff Discussion Draft of House legislation "to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual," May 3, 2010, available at http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf. Such proposals risk erecting unintended obstacles to the robust enforcement of copyright that is essential to promoting innovation in the Internet economy. COA urges the Department of Commerce to engage actively on these issues, both in the development of U.S. privacy law and policy, and in consultations with our trading partners, to ensure that that the "personal data" rubric is not counterproductively extended to impede responsible use of IP address data to detect and deal with instances of online copyright infringement.

---

[1] See, for example, the legal analyses of the situation in several European Union member states in the reports found at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf and http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf. But see EMI Records v. Eircom Ltd, [2010] IEHC 108 (Republic of Ireland High Court, Apr. 16, 2010), available at http://www.bailii.org/ie/cases/IEHC/2010/H108.html, finding such uses fully compatible with Irish data protection law. See also Arista Records LLC v. Doe 3, No. 09-0905, (2d. Cir., April 29, 2010), slip op. at 16 ("to the extent that [online] anonymity is used to mask copyright infringement or to facilitate such infringement by other persons, it is unprotected by the First Amendment.").

Conclusion

COA appreciates your consideration of our views and would be glad to respond to any questions concerning this submission.

Respectfully submitted,

Steven J. Metalitz, counsel to COA
Mitchell Silberberg & Knupp LLP
1818 N Street, NW, 8th Floor
Washington, DC 20036 USA
Tel: +1 (202) 355-7902
Fax: +1 (202) 355-7899
E-mail: met@msk.com

*Before the*
**Department of Commerce**
Washington, DC

| | | |
|---|---|---|
| *In re* | : | |
| Information Privacy and Innovation in the Internet Economy | : | Docket No. 100402174-0175-01 |

**COMMENTS OF**
**COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION**

The Computer and Communications Industry Association ("CCIA") respectfully submits these comments in response to the U.S. Department of Commerce ("DOC"), National Telecommunications and Information Administration's ("NTIA"), Notice of Inquiry in the matter of Information Privacy and Innovation in the Internet Economy.[1] Although the DOC raises numerous important issues, CCIA does not seek to address them all. Instead, these comments address: (1) revising the Electronic Communications Privacy Act[2] ("ECPA") in order to create a clear set of working standards for both individuals and businesses; (2) distinguishing between tracking by applications and websites and tracking by network operators offering Internet access, and the potentially harmful effects of the use of deep-packet inspection ("DPI") by internet access providers ("IAPs") for uninvited intrusions at the network level; (3) ensuring that privacy policy adequately addresses the continuing advancement in technologies, including the rise of remote computing services ("cloud computing") which may recognize no geographical boundary, and the widespread availability of geolocation data.

1 "Information Privacy and Innovation in the Internet Economy; Notice of Inquiry," 75 Fed. Reg. 78 (April 2010), pp. 21226-21231.
2 The Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510, *et seq.*

CCIA is a non-profit international trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly one million people and generate annual revenues exceeding $250 billion.[3]

## I. Introduction

The U.S. possesses a unique opportunity to lead the world in safeguarding civil liberties, but in order to display sufficient credibility to do so, our own privacy policy must do more than merely mitigate perceived intrusions. Instead, the U.S. should adopt policies that broadly protect Internet users' free speech and privacy rights from overreaching law enforcement as digital information moves into contexts different from those in which traditional privacy protections were formed. Inquiries into the current state of privacy policy should go beyond examining potential online commercial abuses to look at hidden telecommunications network surveillance and undue government intrusions.

CCIA commends the DOC for taking another step in that direction by raising the increasingly important issue of privacy in initiating its Information Privacy and Innovation in the Internet Economy proceeding. CCIA urges the DOC to cooperate with other interested bodies, including the U.S. Department of Justice ("DOJ"), the U.S. Office of Science and Technology Policy ("OSTP"), the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), and other foreign governments in reviewing the current state of U.S. privacy law and policy.

[3] A complete list of CCIA's members is available online at http://www.ccianet.org/members.

Concerns over privacy continue to rise as innovation and technological developments advance at a rapid pace. The Internet's expansion brings consumers new and exciting ways to communicate and engage with one another, the government, potential employers, and society as a whole. However, in doing so, more and more consumers are sharing sensitive and personal information, data, and communications online. U.S. privacy policy should be crafted in a way that allows businesses and consumers to understand the ramifications of this shift to sharing more private information online.

Even when no actual privacy loss occurs, the mere perception of privacy loss in personal and/or business matters can spur widespread damage in consumer confidence. When data security is lacking, business users also lose confidence in online transactions. In March 2010 the FCC released its National Broadband Plan ("NBP") calling for nearly ubiquitous access to broadband.[4] If consumers fear that their private information is at risk, adoption of broadband will be slowed, thus hindering the goals set forth by the FCC's NBP.

## II. Revision of ECPA will help clear the air of uncertainty surrounding privacy laws and allow individuals and businesses to better understand their privacy rights and how to comply with and invoke the protection of U.S. privacy laws.

Technologies are not immune from governmental overreaching and any review of U.S. privacy policy must take into account governmental intrusions. As a general proposition, CCIA supports the application of basic Forth Amendment protections against undue search and seizure to electronic communications. CCIA also supports the ECPA revisions advanced by the Digital Due Process Coalition ("DDP"), of which CCIA is a member.

[4] Omnibus Broadband Initiative, Federal Communications Commission, Connecting America: The National Broadband Plan (2010).

### A. As it stands, Courts treat harshly the concept of Fourth Amendment protections in the Internet realm.

Historically, the Fourth Amendment protected postal mail from governmental inspection during delivery. This privacy right in one's mail extended to mail carried by the U.S. Postal Service ("USPS"), as well as private carriers such as United Parcel Service and Federal Express. While some minimal exceptions applied,[5] people generally held privacy rights in mail sent by or delivered to them. As e-mail becomes the more dominant form of communicating, U.S. courts have been hostile to the idea of extending these postal mail Fourth Amendment protections to electronic communications.

A recent decision by the U.S. District Court for the District of Oregon highlights the potential troublesome outcome for Fourth Amendment protection in the context of ECPA. In *In re Application of U.S. for Search Warrant*, the District Court concluded that law enforcement officials did not have to inform an e-mail account holder of a warrant to search the contents of his or her e-mail account.[6] Instead, the court found sufficient notice served only to the IAP and not the account holder. The court premised its decision on the theory that a person must access the Internet through an IAP and, in doing so, the user's information passes through, or may even be stored on, servers owned by the IAP. By means of this process, the Court concluded that the information was no longer private information contained in the home and, thus, not protected by ECPA.

Similarly, the Eleventh Circuit recently rejected extension of Fourth Amendment protection to e-mails. In *Rehberg v. Paulk*, the Eleventh Circuit held that, "a person…loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a

---

[5] No privacy right extended to USPS mail sent as "fourth class," which reserved for the USPS the right to inspect the mail. Further, the protection applied only to the *content* of the mailing, not to anything on the outside of the envelope or the package (i.e. addresses and names).

[6] *In re Application of U.S. for Search Warrant*, ___ F.Supp.2d ___, 2009 WL 3416240 (D. Or. 2009)

third party."[7] The Court found the government's subpoenaing of defendant's e-mails from an IAP to not violate the defendant's Fourth Amendment rights as the e-mails were subpoenaed directly from the IAP and not, "an illegal [search of defendant's] home computer for e-mails."[8]

The courts' unwillingness to extend Fourth Amendment protections to electronic communications, in a world where e-mail serves as a dominant form of communication, will continue to shake consumer confidence in adoption of broadband as an efficient tool for daily communications. Protection from governmental intrusion must evolve as technology evolves. In order for the pervasiveness of e-mail to continue, it is vital that consumers can expect to receive the same protection for an e-mail that they receive in a handwritten letter. E-mail users have established an expectation of privacy in their communications and, as e-mail becomes more and more commonly used, this expectation will only deepen.

Since the Fourth Amendment should extend to anywhere "a reasonable expectation of privacy" exists,[9] the protections prescribed by the Fourth Amendment should be extended to electronic communications in order to preserve consumer confidence. At least two courts have recognized this and found, unlike the Eleventh Circuit's later *Rehberg* decision, that e-mails stored in a web-based e-mail account[10] and text messages stored with a service provider[11] to be protected by the Fourth Amendment. These decisions better develop U.S. privacy policy in accordance with technological advancements.

---

7 *Rehberg v. Paulk*, ___ F.3d ___, 2010 WL 816832 (11th Cir. Mar. 11, 2010).
8 *Id.*
9 *Katz v. U.S.*, 389 U.S. 347, 361 (1967).
10 *Warshak v. U.S.*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc on other grounds*, 532 F.3d 521 (6th Cir. 2008).
11 *Quon v. Arch Wireless*, 529 F.3d 892 (9th Cir. 2008), *cert. granted sub nom. City of Ontario v. Quon*, 78 U.S.L.W. 3395 (U.S. Dec. 14, 2009) (No. 08-1332).

### B. DDP's proposed ECPA revisions help clarify privacy standards for both individuals and businesses and effectively accommodate technological advancements, including the tracking and collection of geolocational data.

DDP advocates four specific ECPA revisions that seek better protection for data shared or stored online.[12] These revisions will also allow for better protection from governmental bulk data requests. CCIA agrees with DDP's assessment that such revisions are necessary to better ensure clarity for both individuals and businesses in what ECPA standards apply to information and data online.

The first recommended ECPA revision would require law enforcement to obtain a search warrant based on probable cause before obtaining private communications or documents stored remotely.[13] Such a revision merely extends the traditional privacy protections provided to documents physically held in the home to the Internet realm. The second revision would require law enforcement to obtain a search warrant before tracking people's location via cell phones or other devices.[14] The third revision would require law enforcement to submit proof that the information sought is relevant to a criminal investigation before electronic surveillance begins.[15] The fourth revision would require law enforcement to submit proof the information sought is not only relevant to a criminal investigation, but is in fact needed, before it may obtain bulk information about broad categories of unknown telephone or internet users.[16]

Additionally, DDP's proposed ECPA revisions would help companies and individuals better understand the privacy concerns of an increasingly important technological development:

---

[12] "Specific Background on ECPA Reform Principles," Digital Due Process Coalition, available online at http://www.digitalddueprocess.org/index.cfm?objectid= C00D74C0-3C03-11DF-84C7000C296BA163.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

the tracking and collection of geolocational data. Mobile phone service providers are being bombarded with law enforcement requests for both real-time tracking of mobile devices and collected geolocational data of mobile devices in connection with searches and surveillance. Meanwhile, privacy advocates' argue that disclosure of such information violates the subscriber's privacy. Geolocational data may also be collected by social networking websites based on the user's location, often through a global positioning system ("GPS") on the user's mobile device or triangulating the device's signal via cell towers. DDP's proposed ECPA revisions help solidify standards of when telecommunications companies can and cannot hand over users' geolocational data to law enforcement authorities.

Revision of ECPA would help tech companies better draft policies that strike a balance between operational needs and user privacy and security. As it stands now, certain law enforcement legislation requires tech companies to keep large databases of retained consumer information. These requirements not only place onerous burdens on the tech companies themselves, but also result in a weakened consumer trust in both the companies and Internet technology itself. Although companies are trying to draft such balanced data retention policies right now, the current state of ECPA results in companies being stuck between privacy advocates demanding less retention and law enforcement favoring increased retention, with ECPA providing little-to-no clarity on how to proceed.

## III. U.S. privacy policy should recognize a distinction between tracking by websites and Internet services at the application level and intrusions by IAPs at the network level, and prohibit any use of DPI by IAPs to track user activity, gather user information, inspect the content of user's messages, or for any other illegitimate purpose.

The differing level of user choice calls for a distinction between technologies used at the application level and technologies used at the network level. At the application level, consumers

may not only have the ability to control what information is collected about them, but also have a better ability to respond to any inappropriate behavior by the service provider. These options often do not exist at the network level.

Users have a greater amount of control at the application level as a result of competition among service providers. Multiple companies often offer the same or a similar product allowing a user of one application to leave that service provider without penalty or inconvenience, if and when it acts inappropriately, and fairly easily migrate to another application offering the same or similar services. As a result, companies acting at the application level know they must implement and act according to pro-consumer policies, or risk losing customers to a competitor.

Users generally do not have the same ability to control and respond to IAP behavior at the network level because the network operators/IAPs lack the competition found at the application level. The high barriers to entry into the Internet access business leads to fewer companies within a given area providing service choice for consumers. Thus, fewer choices leave consumers unable to switch from one IAP to another service.

Additionally, IAPs often engage in practices that make departure from their service even more difficult. For instance, IAPs will often offer a significantly lower monthly rate when the consumer signs a contract agreeing to utilize that IAP's services for some period of time, sometimes upwards of two years. This results in more consumers binding themselves to that IAP for an extended period of time in order to receive the lower, more affordable, rate. Further, IAPs often provide other telecommunications services, such as cable television and/or telephone. Those multi-faceted companies will often bundle their Internet access service with the other television and/or telephone services, further locking in the consumer.

The consumer's lack of control at the network level is of even greater concern because the use of DPI technology at the network level allows IAPs access to a great amount of consumer personal data and a greater ability to engage in end-user tracking of all activity online. Such access and the potential for illegitimate uses highlights why the use of DPI by IAPs at the network level should be prohibited where the IAP fails to give full disclosure to the consumer of its DPI activity and/or the IAP fails to receive express consent to engage in such DPI activity from the user.

The disclosure and consent requirements for use of DPI should be subject to certain standards. Informing the consumer should require the IAP's disclosure to the consumer of:

(1) The purpose of the inspection;

(2) What will be inspected and how it will be inspected;

(3) All uses that will be made of the information gleaned from the monitoring; and

(4) The fact that consent means waiver of all privacy rights, other civil privileges and confidentiality protections.

In explaining any claimed waiver of rights, the IAP should ensure that customers completely understand when their terms of service claim to forfeit any legal privilege, including attorney-client, priest-penitent, doctor-patient, or trade secret privileges. Further, any such term of service is problematic and should be subjected to federal review. Lastly, IAPs should not be permitted to make consent to DPI a mandatory term of the service contract.

CCIA recognizes that DPI may prove valuable in an IAP's attempts to control network integrity and security. As such, DPI should be permitted for those limited purposes only. Any illegitimate use of DPI by IAPs, including the gathering of user-specific information and end-user tracking, should be prohibited without disclosure to the user and the user's express consent.

## IV. An updated U.S. privacy policy should address where privacy stands in continually advancing technologies which may recognize no geographical boundary, such as cloud computing.

Uncertainty abounds for both consumers and businesses in understanding what privacy standards apply to new online applications and cloud computing due to the patchwork nature of current federal laws. Further complicating matters, new technologies such as cloud computing may recognize no geographical boundary. The current sector-specific laws result in consumers having more protection in one area than in another, making consumers unsure what level of protection will apply where. Instead, both businesses and consumers need a modernized and clear set of baseline rules taking into account these continually advancing technologies that necessarily have a multijurisdictional existence.

### A. The rise in popularity of cloud computing requires clarification of what privacy standards will apply to information held in the cloud.

Cloud computing becomes more and more widely used as IAPs provide faster Internet speeds and data storage fees drop.[17] A 2008 Pew Internet study reports that approximately 40% of U.S. Internet customers have engaged in cloud computing, with approximately 59% of those people being between the ages of 18 and 29.[18] While cloud computing offers invaluable tools for cooperation and co-creation, the storage of documents and files on third party servers raises critical privacy questions.

---

[17] "Cloud Computing: Storm Warning for Privacy?," at 1, ACLU of Northern California ("ACLU Report"), available online at http://www.dotrights.org/cloud-computing-storm-warning-privacy-issue-paper (last accessed on June 1, 2010).

[18] "Use of Cloud Computing Applications and Services," Pew Internet and American Life Project ("Pew Report"), available online at http://www.pewinternet.org/Reports/2008/ Use-of-Cloud-Computing-Applications-and-Services.aspx?r=1 (Sep. 2008) (last accessed on June 1, 2010).

### i. Applicability of Fourth Amendment protections to cloud computing requires clarification.

Currently, both the businesses that hold consumer data and the individuals whose data is held face uncertainty in whether the Fourth Amendment protections against unreasonable search and seizure apply to the cloud. The *Katz* case extended Fourth Amendment protections to any "reasonable expectation of privacy,"[19] and a subsequent line of cases extended the protections to items such as personal containers (even if left with another person or in a common area)[20], safety deposit boxes,[21] rented storage lockers,[22] personal computers (even if completely under the control of another),[23] and files on networked computers.[24] Meanwhile, the "business record exception," created by the Supreme Court before the Internet age, says no reasonable expectation of privacy can be had when a person turns over information to a third-party business.[25]

In order for certainty to prevail, this conflict must be resolved. Fourth Amendment protections should be extended to cloud computing in order to match consumer expectations, the promotion of innovation, and the continued prevalence of the Internet. Doing so will not only prompt further adoption of such valuable technologies and spur business development, but will also promote further innovation on the Internet as a whole.

---

[19] *Katz*, 389 U.S. at 361 (1967).

[20] *See* ACLU Report, at 5, *citing U.S. v. Most*, 876 F.2d 191 (D.C. Cir. 1989) (finding a plastic bag inadvertently left with a grocery clerk protectable) and *U.S. v. Block*, 590 F.2d 535 (4th Cir. 1978) (finding a locked footlocker in a common area to be protected).

[21] *See* ACLU Report, at 5, *citing U.S. v. Spilotro*, 800 F.2d 959 (9th Cir. 1985).

[22] *See* ACLU Report, at 5, *citing U.S. v. Karo*, 468 U.S. 705(1984).

[23] *See* ACLU Report, at 5, *citing U.S. v. Barth*, 26 F.Supp.2d 929 (W.D. Tex. 1998).

[24] Protection may not attach if "there is a clear policy of monitoring network use." *See* ACLU Report, at 5, *citing U.S. v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007) and *U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000).

[25] *See* ACLU Report, at 6, *citing U.S. v. Miller*, 425 U.S. 435 (1976) (finding banking records not protectable) and *Smith v. Maryland*, 442 U.S. 735 (1979) (finding phone records of numbers dialed unprotectable).

### ii. The current federal statutory regime creates a climate of uncertainty around cloud computing and must be modernized to accommodate cloud computing.

Current federal privacy statutes require updating in order to address cloud computing. For instance, cloud computing post-dates ECPA and, thus, unsurprisingly is not defined by it. Updating laws to extend privacy coverage to cloud computing services will not only preserve consumer privacy but also encourage loyalty and trust in new beneficial technologies like cloud computing.

In addition to DDP's proposed ECPA revisions discussed above, Microsoft proposed privacy legislation directly addressing cloud computing in January 2010.[26] The proposed legislation followed a Microsoft-sponsored survey reflecting a significant excitement surrounding cloud computing.[27] However, that same study showed that 90 percent of those excited about cloud computing are also concerned about data security within the cloud.[28]

Microsoft's proposed legislation seeks four things:[29]

(1) "Improve[d]…privacy protection and data access rules to ensure users' privacy," specifically calling for revision of ECPA to "clearly define and provide stronger protections for consumers and businesses;"

(2) "Modernization of the Computer Fraud and Abuse Act" giving law enforcement the tools necessary to go after hackers and prevent online crime;

(3) Establishing "truth-in-cloud-computing principles" so that businesses and individuals will know how their data is accessed and used and how their data will be protected online; and

---

[26] *See* "Microsoft Urges Government and Industry to Work Together to Build Confidence in the Cloud," Microsoft press release, Jan. 20, 2010, available online at http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx (last accessed on June 1, 2010).

[27] *See Id.* (reporting, "58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing…").

[28] *See Id.*

[29] *Id.*

(4) Creation of a multilateral agreement addressing data access issues across national borders.

Implementation of these four measures will help businesses and individuals to better understand privacy concerns in the cloud. With more certainty will come more investment and innovation in this new and exciting technology. In fact, an adequate update of the current legislative framework to accommodate technological advancements could spur investment and innovation in not just cloud computing, but across the Internet as a whole.

## V. Conclusion

Modernizing the current state of U.S. privacy policy would go a long way toward promotion of innovation and investment across the Internet. With the current veil of uncertainty surrounding privacy online, individuals and businesses may have reservations about fully embracing all the possibilities the Internet has to offer.

Respectfully Submitted,

/s/ Ed Black
Ed Black, President & CEO
Catherine Sloan, Vice President Government Relations
Gregory Egan, Law Clerk
Computer & Communications Industry Association
900 Seventeenth Street NW, 11th Floor
Washington, D.C. 20006
(202) 783-0070


June 13, 2010

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, D.C. 20230

RE: Information Privacy and Innovation in the Internet Economy
[Docket No. 100402174-0175-01]
RIN 0660-XA12

These comments are submitted on behalf of the more than 200 corporate members of the Consumer Data Industry Association (CDIA). CDIA is an international trade association representing a wide array of technology companies that build market-leading information products based on consumer data which enable businesses in the United States and around the globe to manage risk, comply with legal requirements, protect consumers and enable consumers to access a fair, safe and open free market of products and services delivered over the Internet and through bricks-and-mortar companies. CDIA estimates that its members' products are used more than 9 billion times a year in the United States alone.

CDIA and its members applaud the Department of Commerce's efforts to ensure that as it explores the nexus between privacy policy and innovation in the Internet economy it has a full and complete understanding of the Internet and its fundamental contribution to "U.S. innovation, prosperity, education, and political and cultural life."[1] We agree with the DOC's decision to make sure that "the Internet remains open for innovation."[2] Further, the DOC is correct when it states that the "proper use of personal information can play a critical, value-added role" in preserving what is best about the U.S. approach to the Internet.[3]

**Risk Management – Third-party Databases and Analytical Innovations**

CDIA's members own, operate, manage and develop the world's most sophisticated

[1] NTIA/ITA notice of its May 7, 2010 meeting published in the Federal Register, Vol. 75, No. 73/Friday, April 16, 2010.
[2] Ibid.
[3] NTIA/ITA/NIST notice published in the Federal Register, Vol. 75, No. 78/Friday, April 23, 2010.

third-party databases of consumer data used for risk management purposes both online and offline... They are also the leading providers of decision sciences tools which help users to evaluate data in order to manage risk. It is our members' innovative database designs and analytical tools which lower risk and ensure that citizens' expectations are met and that they continue their full participation in the Internet.

For example, consumers expect to be protected from the crime of identity theft. Our members' identity verification and management tools help Internet businesses to ensure that the persons with whom they are dealing are in fact the true consumers and not fraudsters. Out-of-wallet test questions based on credit reports, databases of names associated with previous fraudulent applications and an array of other data and analytical tools can be deployed to test an online applicant's identity on a real-time basis.

Consumers also expect to be treated fairly and given a price which reflects their hard work and care in managing their finances. Internet delivery of financial services is wholly dependent on our members' data in order to meet these expectations. U.S. credit reporting databases, which contain files on more than 200 million credit-active consumers and which are updated 3 billion times each month are studied the world over due to their sophistication, completeness and timeliness. Perhaps the most effective method for price comparison is Internet-based shopping and consumers can be confident that their data is the key to accessing low-cost credit for their small businesses, their children's college loans and for household credit of all types.

Victims of natural disasters find themselves in the unusual position of asking the government for help and they have an expectation that governmental services will be delivered quickly during their times of need. Often consumers who have moved out of the disaster area will seek such help via the Internet. The government turns to our members for identity verification tools which ensure consumers are served quickly and also that entitlement fraud is greatly reduced.

Consumers and the government expect U.S. businesses to obey the law. Laws such as the U.S.A. Patriot Act, Section 326 require financial institutions to properly verify the identity of their customers in order to prevent foreign and domestic terrorists from accessing and using our country's financial systems against it. Some may think that online applications for credit are a lower-risk method of attempting to work around identity verification. However, our members' innovative systems ensure that Internet transactions are as safe as an in-person application process. Similar systems help Internet orders for age-restricted products such as wine to not be shipped to minors. Age verification tools are critical for companies that must comply with the Children's Online Privacy Protection Act

As a result of the financial crisis Congress has imposed new, stricter statutory underwriting requirements on lenders. For example, the Credit Card Act of 2009 requires credit card issuers to restrict certain types of credit card offers to individuals under the age of 21. Credit card issuers, for example, must engage in a more probative underwriting process to ensure a consumer has "the ability to pay" the loan. Card issuers

must also ensure that certain credit card offers are not made to those under the age of 21 which requires that age verification tools be available for Internet transactions. This concept of measuring a consumer's ability to pay is also embedded in the financial services regulatory reform which states that a lender must "assure that consumers are offered and receive residential mortgage loans on terms that reasonably reflect their ability to repay the loans."[4] This reasonable assurance is a broad mandate that requires verification of income, assets as well as use of credit reports. Assessing a consumer's ability to pay assumes the existence of sophisticated, third-party databases and analytical tools which can be deployed instantly in an Internet transaction.

**How U.S. Laws, Consumer Choice and Third-Party Data Infrastructure Used to Manage Risk**

Congress has recognized the importance of ensuring that an infrastructure of third-party data used for risk management is preserved. Laws such as the federal Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) regulate a range of data used for a set of permissible uses. The FCRA, which pre-dates the U.S. Privacy Act, the OECD's establishment of Fair Information Practices and Europe's Privacy Directive, is an excellent example of a law which provides consumers with rights necessary to balance against the fact that the data flows regulated under the act are generally not tied to consumer consent. See Appendix I for the FTC's summary of consumer rights under the FCRA.

Were consumers able to choose the data that went into their credit reports, such reports would be inherently at risk of being incomplete and inaccurate. Some consumer would simply choose to hide their nonpayment of debts. Clearly our country's financial crises has demonstrated definitively that full, complete and accurate data is necessary in every lending transaction if our financial institutions are to remain stable and so that securities backed by consumer loans are stable and perform as expected. In a different example, criminals, such as pedophiles who want to work in a daycare center or DUI-convicted bus drivers applying for a job driving a school bus, could, if given a right to chose whether or not an FCRA-regulated consumer reporting agency can compile their data, choose to not have their criminal records compiled and used by employers.

It is our view that the U.S. has distinguished itself in the world by recognizing that the principle of consumer choice cannot be applied monolithically and that risk-management is impaired where consumers are given choices to hide data that is necessary to prevent crimes, to predict risk and to ensure compliance with laws. For example, when enacting the Gramm-Leach-Bliley Act (GLBA), Title V, Congress made sure that the consumer's right to opt out of the transfer of nonpublic personal information to nonaffiliated third parties was limited. GLBA Title V, Section 502(e) stipulates that a range of third-parties can and must have access to data without the impairment of consumer choice including ensuring the transfer of data to existing laws which protect consumer data such as the

[4] Conference Base Text (H.R. 4173), "Restoring American Financial Stability Act of 2010", , Pg. 1786, lines 19-22

FCRA. GLBA also ensures that data can be used, for example, to prevent fraud (including identity verification), for public safety purposes, for law enforcement and to complete transactions. A full accounting of the exceptions to consumer choice can be found in Appendix II of this letter.

Laws which govern how Internet data flows involving consumer data must account for the necessity of ensuring continued innovation in the construction of risk-management systems. An inappropriate application of consumer choice to Internet data flows could choke off the innovative risk-management data systems which are created in this country only because of the careful balancing of individual protections with important societal benefits which U.S. law strikes. Third-party risk management databases are designed to comply with a plethora of legal regimes including, to name just a few, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Health Insurance Portability and Privacy Act, the Gramm-Leach-Bliley Act, Title V, the Children's Online Privacy Protection Act, and also Section 5 of the Federal Trade Commission Act. Internet privacy laws will prevent flows of data that are critical to our

**International Privacy Laws and Trans-border Data Flows**

While today risk-management data is often compiled and maintained on a country-specific it is CDIA's view that the arbitrary harmonizing of legal regimes which regulate the free flow of consumer data used for risk management would be the wrong approach. As the DOC's own Federal Register notice suggests, our U.S. privacy framework is multi-faceted and "[i]n many, though not all cases, this has been a formula for success to build on."

CDIA and its members regularly participate in international dialogues regarding data flows. These include many of the ones discussed in the DOC notice such as the Safe Harbor Framework between the European Union and the United States, the Asia Pacific Economic Cooperation Privacy Framework discussions for implementation of trans-border data flows, various International Standards Organization discussions of privacy as well as World Bank-hosted Task Forces on international standards for credit reporting. Such discussions should continue and the role of the United States should be to ensure that the nature and success of U.S. laws and their operation is fully understood in these dialogues.

**Conclusion**

Consumer data which flows from the Internet will continue to increase as consumers shift their lives to this medium. CDIA's members will continue to serve as the vanguard when it comes to ensuring that risk management priorities are central to this mode of commerce. The DOC should make every effort to ensure that regulation of data flows does not impair in any way the construction of data bases and the ensuring innovative products which protect consumers and ensure their fair treatment.

Sincerely,

Stuart K. Pratt
President & CEO

# APPENDIX I

**A Summary of Your Rights Under the Fair Credit Reporting Act**

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. **For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.**

C **You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.

C **You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

C a person has taken adverse action against you because of information in your credit report;

C you are the victim of identify theft and place a fraud alert in your file;

C your file contains inaccurate information as a result of fraud;

C you are on public assistance;

C you are unemployed but expect to apply for employment within 60 days.

In addition, by September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.ftc.gov/credit for additional information.

C **You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

C **You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.ftc.gov/credit for an explanation of dispute procedures.

C **Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

C **Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

C **Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need -- usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

C **You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.ftc.gov/credit.

C **You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the

lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).

C **You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

C **Identity theft victims and active duty military personnel have additional rights.** For more information, visit www.ftc.gov/credit.

**States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.**

APPENDIX II

(e) GENERAL EXCEPTIONS.—Subsections (a) and (b)
14 shall not prohibit the disclosure of nonpublic personal
15 information—
16 (1) as necessary to effect, administer, or en17
force a transaction requested or authorized by the
18 consumer, or in connection with—
19 (A) servicing or processing a financial
20 product or service requested or authorized by
21 the consumer;
22 (B) maintaining or servicing the con23
sumer's account with the financial institution,
24 or with another entity as part of a private label
1 credit card program or other extension of credit
2 on behalf of such entity; or
3 (C) a proposed or actual securitization,
4 secondary market sale (including sales of serv5
icing rights), or similar transaction related to a
6 transaction of the consumer;
7 (2) with the consent or at the direction of the
8 consumer;
9 (3)(A) to protect the confidentiality or security
10 of the financial institution's records pertaining to
11 the consumer, the service or product, or the trans12
action therein; (B) to protect against or prevent ac13
tual or potential fraud, unauthorized transactions,
14 claims, or other liability; (C) for required institu15
tional risk control, or for resolving customer disputes
16 or inquiries; (D) to persons holding a legal or bene17
ficial interest relating to the consumer; or (E) to
18 persons acting in a fiduciary or representative capac19
ity on behalf of the consumer;
20 (4) to provide information to insurance rate ad21
visory organizations, guaranty funds or agencies, ap22
plicable rating agencies of the financial institution,
23 persons assessing the institution's compliance with
24 industry standards, and the institution's attorneys,
25 accountants, and auditors;
1 (5) to the extent specifically permitted or re2
quired under other provisions of law and in accord3
ance with the Right to Financial Privacy Act of
4 1978, to law enforcement agencies (including a Fed5
eral functional regulator, the Secretary of the Treas6
ury with respect to subchapter II of chapter 53 of
7 title 31, United States Code, and chapter 2 of title
8 I of Public Law 91–508 (12 U.S.C. 1951–1959), a
9 State insurance authority, or the Federal Trade
10 Commission), self-regulatory organizations, or for an
11 investigation on a matter related to public safety;
12 (6)(A) to a consumer reporting agency in ac13
cordance with the Fair Credit Reporting Act, or (B)
14 from a consumer report reported by a consumer re15
porting agency;
16 (7) in connection with a proposed or actual
17 sale, merger, transfer, or exchange of all or a por18

tion of a business or operating unit if the disclosure
19 of nonpublic personal information concerns solely
20 consumers of such business or unit; or
21 (8) to comply with Federal, State, or local laws,
22 rules, and other applicable legal requirements; to
23 comply with a properly authorized civil, criminal, or
24 regulatory investigation or subpoena or summons by
25 Federal, State, or local authorities; or to respond to
1 judicial process or government regulatory authorities
2 having jurisdiction over the financial institution for
3 examination, compliance, or other purposes as au
thorized by law.

June 14, 2010

Office of the Secretary;
National Telecommunications and
Information Administration;
International Trade Administration
US Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

*Filed by email at privacy-noi-2010@ntia.doc.gov*

Re: Department of Commerce Notice of Inquiry
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174–0175–01; RIN 0660–XA12

The Council of Better Business Bureaus (CBBB) appreciates the opportunity to provide these comments in response to the US Department of Commerce's ("the Department") "Notice of Inquiry on Information Privacy and Innovation in the Internet Economy," 75 FR 21226, issued April 23, 2010.

The NOI seeks comments on the efficacy of current privacy laws and self regulatory initiatives in the United States and worldwide in supporting internet commerce and innovation, while maintaining fundamental privacy principles and taking account of evolving consumer expectations regarding online privacy. These issues were explored during panel discussions at the Department's related Symposium on Privacy and Innovation held May 7, 2010, in which CBBB was pleased to participate.

We applaud the Department's initiative in launching this fact finding effort, and in providing a forum for dialogue around approaches to privacy accountability that

foster continued innovation across the internet ecosystem, while respecting and protecting consumer privacy

We note two recurring themes that emerged during the Symposium. First, in the global internet economy, privacy accountability for the collection, transfer and use of personal data does not simply implicate individual rights within one jurisdiction, but also affects the flow of international trade. Many individual privacy complaints arising from online commerce cannot be readily handled in the cross border environment, where varying legal privacy frameworks may provide few traditional options for resolution of consumer disputes. Even in countries with well-developed privacy rules, regulatory intervention is unlikely to occur until a critical mass of complaints has been received against a single perpetrator, and the vast majority of consumer privacy disputes are unlikely to be adjudicated within traditional judicial systems, given the barriers of expense, language, access and procedural complexities and the low monetary value of most disputes.

In our comments we will reference CBBB's experience and belief that these issues may be addressed most effectively and economically by flexible self-regulatory frameworks for handling complaints and adjudicating privacy disputes against mutually agreed principles. A key element of such frameworks is the inclusion of independent third party accountability mechanisms to support and enforce industry compliance and to resolve consumer privacy disputes that might otherwise go unaddressed.

Our comments will also touch on a second theme of the Symposium – how the evolving privacy expectations of internet users regarding the passive collection and use of their personal data in certain contexts have exposed the limitations of traditional notice and choice in the privacy policy. CBBB recognizes the need for innovative approaches to consumer awareness and participation in authorizing the collection, transfer and use of personal data and other unique identifiers in contexts such as online marketing. To this end, CBBB has participated in the development of the first cross-industry Self-Regulatory Principles for Online Behavioral Advertising, released in July 2009 and discussed below.

## I. CBBB Background

The Council of Better Business Bureaus, a non-profit 501(c) (6) membership organization, is the umbrella organization for local Better Business Bureaus, which are grassroots organizations that foster a fair and honest marketplace and an ethical business environment. The mission of the BBB system is to advance marketplace trust by promoting the highest ethical relationship between businesses and the public through self-regulation, consumer and business education, and service excellence.

The CBBB has administered self regulatory programs in the advertising industry for almost 40 years, and has created innovative compliance and dispute resolution programs to address other emerging issues, including the highly regarded *BBB AUTOLINE* and *BBB Online* programs. The CBBB also has demonstrated leadership in online advertising and privacy issues. Its *Children's Advertising Review Unit (CARU)* administers the first FTC-granted safe harbor under the Children's Online Privacy Protection Act. The CBBB developed one of the earliest online privacy seal programs, and its *BBB EU Safe Harbor* program remains a prominent dispute resolution mechanism under the US-EU Safe Harbor Framework. Most recently, CBBB and a coalition of advertising industry associations spearheaded the development and release in July 2009 of the *Self Regulatory Principles for Online Behavioral Advertising.*

## II. Self Regulation and International Privacy Frameworks

A. Key Concepts in Self Regulation

While business self-regulation is well recognized in the United States, it is less understood in other parts of the world. CBBB has long argued that the term "self" in self-regulation should not be understood as industry acting unilaterally, but rather as a process driven by the enlightened self-interest of industry, supported in limited, but critical, ways by government to the ultimate benefit of consumers. The Better Business Bureau system has many years of highly successful experience with self-regulation in the U.S. and Canada. Based on that experience, we believe that successful self-regulatory frameworks include performance and voluntary compliance standards that are developed by industry, recognized and complemented by objective third party oversight, and credible to the public.

Any self-regulatory process that lacks substance or fails to deal firmly and openly with conduct at variance with the voluntary guidelines will lose the confidence of both consumers and regulators, resulting in often sweeping regulation that can strangle innovation and discourage competition.

Industry can play a pivotal role in developing international self-regulatory privacy frameworks by encouraging the development of standards for online commerce, and funding the development of the technology infrastructure needed to ensure dispute resolution mechanisms are both cost-effective and provided at low or no cost to consumers. It can develop private sector funding to support independent "accountability agents" such as trustmark organizations and other third party monitoring mechanisms. It can also encourage effective partnering across borders among consumer groups, dispute resolution programs and self-regulatory organizations.

National governments can play an equally vital role by adopting cross border principles that complement and encourage the development of national privacy laws; establishing standards for accountability agents and dispute resolution mechanisms; and taking action under national laws and regulations when certified companies fail to honor their commitments under international frameworks. The CBBB believes that self-regulatory frameworks meeting these criteria provide the best model for consumer privacy protection in the global e-commerce environment.

Two international initiatives spearheaded by the Department of Commerce incorporate these self-regulatory elements: the US-EU Safe Harbor Privacy Framework, now in its tenth year of operation; and the APEC Privacy Pathfinder Projects, dedicated to developing a Cross Border Privacy Rules system for cross border data transfers across the APEC economies.

B. US-EU Safe Harbor Privacy Framework

After a decade in operation, the US-EU Privacy Framework has seen a rapid expansion in participation over the last two years by US companies doing business in the European Union, who choose to self-certify their compliance with the Safe Harbor Principles as a mechanism to facilitate transfers of personal data from the European

Union member states. We understand that around 2,000 companies are registered on the Department's Safe Harbor List, with up to 50 new companies filing initial self-certifications each month.[1]

Alternative data transfer mechanisms are available, including Model Contracts pre-approved by the European Commission for transfers to both the US and other destinations, and Binding Corporate Rules, enabling affiliated companies operating in multiple jurisdictions to obtain approval from the DPAs to use internal privacy rules based on EU data privacy principles for cross border data flows within affiliate groups. However, for most US businesses, and particularly for smaller concerns doing business online with non-affiliated entities in the EU, the Safe Harbor Framework appears to offer a more practical, less burdensome option.

Equally importantly, participation in the Safe Harbor Framework creates a level of public accountability for US companies within the United States. Participants must self-certify to the Commerce Department and in published privacy statements that their privacy practices conform to the seven Safe Harbor Privacy Principles, and must verify that compliance during annual recertification. Verification may be performed in-house and certified by senior management, or may be provided by a commercial seal program or other independent verifier. Participating companies also are required to designate an affordable, accessible independent dispute resolution mechanism to handle complaints by EU data subjects. In addition, the Federal Trade Commission ("FTC") has enforcement authority over both the Framework participants and over commercial trustmarks who may verify their compliance.

We note two developments in 2009 that will likely bolster the Framework's effectiveness: the FTC's first two enforcement actions against a total of seven companies that had falsely represented their self-certification to the Safe Harbor Program in their online privacy statements (one had never certified; six others had allowed their certifications to lapse); and the imposition of certification fees for participation, providing the Department of Commerce with additional resources to keep the Safe Harbor List of certified participants updated and accurate. These actions can be expected to refocus participating companies on the substantive

[1] *See* Brian Hengesbaugh, Michael Mensik, Amy de La Lama, *Why Are More Companies Joining the US-EU Safe Harbor Framework?* IAPP Privacy Advisor, Vol. 10, No. 1 (January –February 2010).

commitments they have made to privacy protection, and to increase public confidence in the efficacy of the Framework.

C. The APEC CBPR System

We wish to commend the Department for its continuing leadership in the APEC Data Pathfinder Projects, which seek to bring together all stakeholders – governments, regulators, industry, consumer representatives and accountability agents – in a consultative process to create and test the elements of the cross border privacy rules (CBPR) system to enable cross border data flows across the APEC economies under the guidance of the APEC Privacy Principles. The system is intended to provide a mechanism for certification by accredited accountability agents of a business's internal 'privacy rules' as compliant with the Principles. Such certifications are to have mutual recognition among participating economies. The system is also expected to guarantee backstop enforcement by a public sector enforcement authority with jurisdiction to enforce domestic privacy laws. The CBPR system is intended to promote a minimum standard of privacy protection for data transfers across participating economies, while maintaining the obligations of participating companies to comply with all applicable domestic laws.

Given that the proposed CPBR certification system will subject the business processes and privacy practices of participating companies to an intensive process of self-assessment and external review, the qualifications and roles of accountability agents have received well deserved scrutiny. At present, the proposed system provides some flexibility as to which entities may perform the accountability tasks of certifying businesses, monitoring compliance, dispute resolution and enforcement. Certain private sector accountability agents – including established trustmark or seal programs – may assert their ability to play all of these roles. Other entities that are well qualified to evaluate and certify privacy compliance, such as law or accounting firms or public sector agencies, may be unable to demonstrate sufficient 'independence' in their relationships with certified businesses to also offer dispute resolution services. Such entities may elect to provide only certification and limited compliance monitoring, while partnering with qualified entities to provide independent dispute resolution and enforcement. As discussions progress, we expect that the eligibility standards for accountability agents – including, but not limited to, independence and freedom from conflicts of interest – will be critical to maintaining

the confidence of businesses, consumers and governments in the ability of the CBPR system to protect consumer privacy while maintaining information flows across the APEC economies and preserving the vitality of internet commerce.

## III. Self-Regulation of Online Behavioral Advertising (OBA)

In July 2009, following months of collaborative efforts by associations and individual companies representing the entire online advertising ecosystem, a coalition of trade associations including the CBBB, together with the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, and Direct Marketing Association released the cross-sector *Self-Regulatory Principles for Online Behavioral Advertising*[2], the first self regulatory framework designed to apply broadly to all of the actors engaged in online behavioral advertising activities. The seven Principles include commitments to consumer education; new consumer notice and choice mechanisms; data security; increased protection for sensitive data categories such as medical and financial information and children's data; affirmative consent for material changes to online behavioral advertising data collection and use policies; and strong enforcement mechanisms.[6]

### A. Transparency and Choice

Key elements of the Principles provide both for more transparent notice of how consumer data is collected and used and for simple and effective processes for consumers to choose whether to receive behaviorally targeted ads. Companies engaged in behavioral advertising are directed to explain their activities on the relevant websites outside the privacy policy, by placing a consistent icon and common notice language in proximity to behaviorally targeted online ads or in another prominent location on web pages where behavioral data is collected. Web site operators hosting behavioral advertising, as well as the third party ad networks, behavioral data providers and others collecting behavioral data or serving ads on their sites are called on to provide links from this enhanced notice to consumer preference pages or choice mechanisms. In addition to these innovative solutions, the Principles include specific commitments to provide consumer education on

[2] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available* at http://www/bbb.org/us/behavioral-advertising-principles/

behavioral advertising practices and on the significance and functionality of the icon and the enhanced notice and choice mechanisms. They also call for the creation of accountability mechanisms – now under development by CBBB and by the Direct Marketing Association –that will police and enforce industry compliance with the Principles, handle consumer complaints, help bring entities into compliance, publicly report instances of noncompliance, and refer persistent violators to the appropriate government agencies.

B. Accountability

The CBBB believes that a robust and independent accountability mechanism is critical to the success of self-regulatory programs. Accordingly, with support from the industry Coalition, the CBBB is currently developing an accountability mechanism to monitor compliance with the OBA Principles, to be modeled loosely on the highly successful Children's Advertising Review Unit or CARU, a CBBB-administered program whose operational policies are set by the National Advertising Review Council (NARC).[3] Like CARU, CBBB's OBA accountability mechanism will engage in widespread monitoring of web sites and companies known or believed likely to be engaged in behavioral advertising activities. To facilitate consumer complaint handling and to avoid duplication of effort, CBBB will coordinate its activities with those of the DMA, whose own accountability mechanism will ensure its members' compliance with the Principles as implemented in the DMA's Code of Ethical Guidelines.

## IV. Conclusion

CBBB is proud of the progress that self-regulation has made toward protecting consumers while maintaining the dynamic, innovative environment of the internet, and we look forward to continuing our participation in both domestic and international self regulatory privacy programs. CBBB believes that sustained efforts by all interested groups to build alliances and relationships remain essential to the goal of fostering global online commerce to the benefit of consumers and merchants in every country.

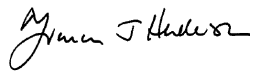
[3] NARC is a strategic alliance of the advertising industry and the BBB.

*  *  *

The CBBB thanks the Department of Commerce for the opportunity to submit these comments, and we look forward to working with the Department as it continues to evaluate the important issue of online privacy in the global internet economy.

Respectfully submitted,

C. Lee Peeler
Executive Vice-President
Council of Better Business Bureaus



Frances J. Henderson
Associate General Counsel and Director, Privacy Initiatives
Council of Better Business Bureaus

**Before the**
**DEPARTMENT OF COMMERCE**
**Washington, D.C. 20230**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | Docket No. 100402174-0175-01 |
| Information Privacy and Innovation in the Internet | ) | |
| Age | ) | RIN 0660-XA12 |

**COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®**

## I. INTRODUCTION

CTIA – The Wireless Association® ("CTIA")[1] hereby submits these comments in response to the Department of Commerce Internet Policy Task Force's Notice of Inquiry seeking information on the effect of privacy law and policy on the Internet economy.[2] As CTIA's recently revised location-based services ("LBS") guidelines and best practices demonstrate, industry self-regulation is more capable of moving at Internet speeds and adapting to the ever-evolving digital world than government rulemaking and regulation in the fight to safeguard consumers' privacy. In issuing its report, CTIA urges the Department of Commerce to recognize that proactive industry self-regulation, which is responsive to consumer demands and marketplace evolution, is more nimble and effective at protecting consumer privacy in the age of the Internet than government regulation.

Few could fully anticipate a mere two decades ago the crucial role the Internet would play in the lives of Americans. In addition to the explosion of commerce and content on the Internet, Americans' increasingly are migrating to web-based services, including education,

---

[1] CTIA-The Wireless Association® (www.ctia.org) is an international organization representing the wireless communications industry. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products.

[2] Information Privacy and Innovation in the Internet Age, 75 Fed. Reg. 21226 (Apr. 23, 2010).

healthcare and government services. With the aggregation of personal information on the Internet, great diligence is necessary to prevent fraud and unwanted dissemination of personally identifying information ("PII"). CTIA and the wireless industry have been leaders in privacy policy, especially with respect to LBS associated with mobile users. LBS, which rely on, use or incorporate the location of a device to provide or enhance a service, have raised privacy questions from their start, more than fifteen years ago. In response, the wireless industry has crafted LBS best practices and guidelines to address consumers' concerns regarding their services. These guidelines, which CTIA recently updated to reflect changes in the technology, the market, and consumers' demands, are an example of how self-regulation has the flexibility and the speed to adapt to the rapidly evolving wireless ecosystem.

## II. BACKGROUND

Even when LBS was just an idea, CTIA and the wireless industry recognized the importance of balancing the need for access to customers' location information in emergencies and legitimate law enforcement purposes with wireless users' privacy expectation. The industry's efforts to balance these expectations with consumers' demand for innovative services and devices began fifteen years ago when CTIA and Public Safety proposed a "Consensus Solution" for providing location information to Public Safety Answering Points to the Federal Communications Commission ("FCC" or "Commission") in the agency's wireless E-911 rulemaking proceeding.[3]

[3] *See* In the Matter of Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 18676, 18687-88, 18770 (1996) (Full text of *Consensus Agreement Between CTIA and Public Safety Groups Regarding Wireless E911* available at Appendix D, Table B).

In the late 1990s, CTIA supported *The Wireless Communications and Public Safety Act of 1999* ("WCPSA").[4] The Act addressed some of the issues that arose from the FCC's E-911 rulemaking, including a provision that specifically authorized carriers to provide call location information concerning a user of a commercial mobile service to: (1) emergency dispatchers and emergency service personnel in order to respond to the user's call; (2) the user's legal guardian or family member in an emergency situation that involves the risk of death or serious physical harm; or (3) providers of information or database management services solely for purposes of assisting in the delivery of emergency services.[5] The WCPSA also amended Section 222 of the Communications Act of 1934, as amended ("Communications Act"), to require "the express prior authorization of the customer" for the disclosure of the wireless customer's location information for any other purpose, thus keeping consumers in control and better protecting their private location information.[6]

CTIA continued its privacy efforts in 2000 by petitioning the FCC to adopt a set of Fair Location Information Practices for wireless LBS.[7] Embracing the Federal Trade Commission's ("FTC") "belief that greater protection of personal privacy . . . will benefit businesses as well as consumers by increasing consumer confidence and participation in the . . . marketplace," CTIA modeled its proposal on the familiar FTC Fair Information Practice Principles, which espoused notice, consent, security and integrity of information,

---

[4] The Wireless Communications and Public Safety Act of 1999, Public Law 106-81, 113 Stat. 1286 (codified at 47 U.S.C. § 222 (2006)).

[5] *Id*.

[6] 47 U.S.C. § 222.

[7] Wireless Telecommunications Bureau Seeks Comment On Request to Commence Rulemaking To Establish Fair Location Information Practices, *Public Notice*, 16 FCC Rcd 5599 (2001).

and technology neutral rules.[8] Although the FCC declined to adopt CTIA's proposal at the time,[9] the fundamental principles of customer "notice" and "consent" have been widely adopted in numerous cross-industry privacy policies and principles, and have provided the basis for the wireless industry's approach to protecting the privacy of wireless users who use LBS.

## III. CTIA'S LBS BEST PRACTICES AND GUIDELINES ARE ADAPTING IN LIGHT OF RAPIDLY-EVOLVING TECHNOLOGY AND CONSUMER DEMAND FOR PROMOTING AND PROTECTING THE PRIVACY OF LOCATION INFORMATION.

### A. CTIA's 2008 LBS Guidelines Sought and Achieved Consensus to Establish an Effective Framework and a Strong Foundation

In 2008, as the development and deployment of LBS began occurring in earnest for non-E-911 applications, CTIA commenced work with its members and other interested parties on developing a set of industry "Best Practices and Guidelines" to promote and protect the privacy of wireless customers' location information. As part of the development process, CTIA reached out to privacy experts from over 90 entities, including telecommunications companies, non-profit privacy groups and government agencies, and examined numerous privacy agreements from various LBS companies.

---

[8] *See* Federal Trade Commission *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, 34 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[9] *See* In the Matter of Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, 17 FCC Rcd 14832 (2002). In declining to commence a rulemaking to adopt rules to implement the wireless location information privacy amendments to Section 222 of the Communications Act, the Commission stated that it "[does] not wish to artificially constrain the still-developing market for location-based services," and that it will "initiate a rulemaking proceeding only when the need to do so has been clearly demonstrated." *Id*. at 14832.

After extensive work and consultation, CTIA unveiled its Best Practices and Guidelines for Location-Based Services ("2008 Guidelines") on April 2, 2008.[10]

The 2008 Guidelines, built on the now familiar foundation of "Notice-and-Consent," directed entities that provide LBS to inform consumers about how their location information will be used, disclosed, and protected so that consumers can make an informed decision about whether or not to use a particular LBS or authorize disclosure of their location to others. Importantly, the 2008 Guidelines were expansive in scope by applying to *all* LBS providers, including application developers and equipment providers, and not simply limited to wireless carriers. Once a user has opted to use an LBS, or authorized disclosure of his or her location, the 2008 Guidelines contemplated that the user should have the ability to decide when or whether location information may be disclosed to third parties, as well as providing that the user should have the ability to revoke such authorization at any time. Furthermore, the guidelines incorporated the Notice-and-Consent structure utilized by the FTC.[11] In constructing the 2008 Guidelines, CTIA also recognized that user privacy must be balanced with legitimate law enforcement and emergency or other needs – consistent with Section 222 of the Communications Act and the FCC's rules governing Customer Proprietary Network Information.[12] Accordingly, the Guidelines do not apply to location information used or disclosed: (1) as authorized or required by applicable law (*e.g.*, to respond to emergencies, E911, or legal process); (2) to protect the rights and property of LBS

[10] News Release, CTIA – The Wireless Association®, CTIA – The Wireless Association® Announces Best Practices for Location-Based Services (Apr. 2, 2008).

[11] *See* Federal Trade Commission, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited May 27, 2010).

[12] *See* 47 U.S.C. § 222.

providers, users or other providers of location information; (3) for testing or maintenance in the operation of any network or LBS; or (4) in the form of aggregate or anonymous data. With a base of broad industry support, the 2008 Guidelines presented LBS providers with a clear path forward in the development of LBS, while giving consumers the information and tools they need to control the use of their location information.

### B. CTIA's LBS Best Practices and Guidelines Are Adapting to Technological and Market Changes

Reflecting the rapid innovation and introduction of new technologies that characterize the wireless industry, CTIA's LBS Best Practices and Guidelines are not carved in stone. In fact, its framers anticipated that, as technology and applications advanced, so must the Guidelines. Accordingly, a little more than a year after publication of the 2008 Guidelines, CTIA proactively initiated efforts to update the LBS Guidelines to keep pace with the rapid advance of LBS technologies and services. These efforts produced revised Guidelines that maintain the Notice-and-Consent format while adding greater protections for LBS consumers. Of particular significance to this proceeding is the wireless industry's willingness and ability to adopt and modify best practices at the pace of Moore's Law,[13] which demonstrates the superior speed and flexibility of industry self-regulation versus government intervention.

Until recently, LBS relied on a wireless carrier having access to a user's location information and then using or sharing that information with a third party to provide an LBS. This is the model Congress contemplated when it enacted the LBS amendments to Section 222 in 1999, and even the model CTIA, commenters and participating entities contemplated when drafting the 2008 Guidelines. However, in just two years the

[13] *See* Intel, *Moore's Law: Raising the Bar* (2005), *available at* http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_Backgrounder.pdf

wireless industry and LBS technology have undergone profound changes that extend the provision of LBS well beyond a carrier-centric approach.

Smartphones are rapidly taking over the market - in the fourth quarter of 2009, thirty-one percent of all handsets sold were smartphones compared to just eleven percent during the first half of 2007.[14] Leading smartphone operating systems are open for application development spurred by Android, iPhone and other application development kits, which has led to an exponential rise in applications. In late 2009, a CTIA filing with the FCC observed that consumers had access to more than 100,000 apps.[15] That number has more than doubled to 240,000, and it is projected that worldwide downloads from mobile application stores will exceed 21 billion by 2013.[16]

With increased functionality of handsets and the ease of mobile application development, LBS-based applications are on the rise and can now be downloaded to a handset and operated without the wireless carrier's involvement or knowledge. LBS technology that resides in the handset, not the carrier's network, has led to applications such as Loopt, Foursquare, Yowza!!, and Gowalla, and offers consumers

---

[14] *See* Press Release, The NPD Group, The NPD Group: Smartphones Drive More Handset Sales Overall, But Lower Prices Stall Total Handset Revenue Growth (Mar. 17, 2010), *available at* http://www.npd.com/press/releases/press_100317.html; Press Release, The NPD Group, The NPD Group: Year-Over-Year U.S. Mobile Phone Sales Increased 14 Percent in Second Quarter (Aug. 15, 2007), *available at* http://www.npd.com/press/releases/press_070815.html.

[15] In the Matter of Fostering Innovation and Investment in the Wireless Communications Market, A National Broadband Plan For Our Future, GN Docket Nos. 09-157, 09-51, Comments of CTIA (Sept. 30, 2009).

[16] *Consumers Will Spend $6.2 Billion in Mobile Application Stores in 2010*, CELLULAR-NEWS (Jan. 18, 2010), http://www.cellular-news.com/story/41491.php.

location-specific driving directions, mobile search, coupons, reviews, and social networking. Loopt alone has reached over three million registered users.[17]

At the same time, the past two years have seen increased consumer consciousness and demand for privacy. From Facebook and Google, and their use of consumer data, to the forthcoming Supreme Court decision in *City of Ontario, CA v. Quon*, which examines the expectation of privacy in an employer-provided wireless device, privacy policies and frameworks are on the front pages of newspapers and web sites, and in the minds of consumers.[18]

In 2009, CTIA and its members began the process of revising the LBS Guidelines to ensure consumers that when they use an LBS, a clearly identified LBS provider will inform them about how their location information will be used and disclosed, and the LBS provider also will obtain their consent before initiating services. The revised Guidelines, released in March 2010, merge the familiar Notice-and-Consent requirements with protections for account holders and device users alike.[19]

As stated in the revised Guidelines, LBS providers will use written, electronic or oral notice that will ensure that users have an opportunity to be fully informed of the providers' information practices. Notice must be provided in plain, easily understood language; it must not be misleading and, if combined with other terms or conditions, the portion pertaining to the LBS must be conspicuous. If, after having obtained consent, an LBS provider wants to use location information for a new or materially different purpose

---

[17] Claire Cain Miller, *Cellphone in New Role: Loyalty Card*, NEW YORK TIMES (May 31, 2010), *available at* http://www.nytimes.com/2010/06/01/technology/01loopt.html (last visited June 1, 2010).

[18] Quon v. Arch Wireless Operating Co., 529 F.3d. 892 (9th Cir. 2008) *cert. granted*, 130 S.Ct. 1011 (U.S. Dec. 14, 2009) (No. 08-1332).

[19] *See* 2010 Revised Guidelines, attached hereto at Attachment A.

not disclosed in the original notice, the provider must inform the user with further notice and obtain the user's consent to the new or other use. LBS providers must inform users how long any location information will be retained, if at all. The Guidelines require that, as a general matter, providers should retain user location information only as long as business needs require, after which such information should be destroyed or rendered unusable. The Guidelines also direct LBS providers to periodically remind users when their location information may be shared with others and of the users' location privacy options. A significant change from the 2008 Guidelines is the clear requirement that every *user*, not just account holders, be informed whenever an LBS is installed and used on their device, reducing the risk of surreptitious or unauthorized tracking.

The revised Guidelines require that consent be informed and based on a notice consistent with the notice requirements set forth by the Guidelines. Consent may be implicit, such as when users request a service that obviously relies on the location of their device – such as seeking information on the nearest gas station. Notice may be contained in the terms and conditions of service for a location-based service to which users subscribe. Users may manifest consent to those terms and conditions electronically by clicking "I accept;" verbally by authorizing the disclosure to a customer service representative; through an interactive voice response system or any other system reasonably calculated to confirm consent. The Guidelines expressly reject pre-checked boxes that cause a user to be automatically opted-in to location information disclosure or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement. Such an approach would be insufficient to express user consent under the CTIA Guidelines.

The revised Guidelines offer a framework for the protection of user privacy. The industry's willingness to develop meaningful and effective best practices, and to nimbly revise those guidelines as circumstances warrant, represents the best way to balance the need to promote and protect user privacy while also facilitating the deployment of new and innovative products and services. Industry self-regulatory efforts have the flexibility to address privacy issues in the ever-changing wireless space much faster than government regulation.

### C. Data Retention Requirements Adversely Affect Carriers, Consumers, and the Internet Economy

Data retention requirements currently under consideration have real economic and privacy implications for providers. The "Internet Economy" – as used by NTIA in this proceeding – will be adversely affected by data retention laws that require carriers not only to store large quantities of data for law enforcement purposes, but also to implement additional costly measures in order to ensure the safety of consumers' private information. While complying with such data retention regulations, carriers are often exposed to privacy and Fourth Amendment lawsuits. The ultimate result is a stifling of innovation and investment in the Internet.

A balance between law enforcement's legitimate need to investigate and prosecute crimes carried out or facilitated by the Internet, consumers' legitimate expectations of privacy and free speech, and carriers' costs of retention and its effect on innovation and creativity on the Internet must be sought at the Federal level. As a recent NTIA report stated, "[i]f states are allowed to set their own data retention standards, this would burden the [Internet service providers] with as many as 54 different sets of

requirements, creating even more uncertainty for law enforcement."[20] Government, privacy advocates and industry must work together to develop a technologically feasible and economically reasonable solution with careful attention to constitutional and legal protections.

[20] National Telecommunications and Information Administration, Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group (June 4, 2010), *available at* http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf

## IV. CONCLUSION

With the emergence of new technology and applications, today's wireless ecosystem is vastly different from just a few years ago. Advances in wireless technology are being driven by Moore's Law, and when innovative new technologies and applications upset old paradigms, consumer privacy must keep pace. As CTIA and the wireless industry have shown, proactive industry self-regulation that is responsive to consumer demands and marketplace evolution will be more nimble and effective at protecting consumer privacy in the age of the Internet than government regulation.

Respectfully submitted,

By: */s/ Brian Josef*
Brian Josef
Director, Regulatory Affairs

Michael F. Altschul
Senior Vice President, General Counsel

Christopher Guttman-McCabe
Vice President, Regulatory Affairs

**CTIA–The Wireless Association®**
1400 16th Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org

**Before the**
**United States Department of Commerce**
**National Telecommunications and Information Administration**
**Washington, D.C.**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | Docket No. 100402174-0175-01 |
| Information Privacy and | ) | |
| | ) | RIN 0660-XA12 |
| Innovation in the Internet Economy | ) | |

## COMMENTS OF DATA FOUNDRY

Data Foundry, Inc. ("Data Foundry") respectfully submits these comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("NOI") released April 23, 2010.

### Introduction

Data Foundry is a global provider of managed Internet, enterprise data center, collocation and disaster recovery services. Data Foundry is headquartered in Austin, Texas. We have long been an advocate for Internet privacy and we welcome the opportunity to comment in this proceeding. In the NOI, the NTIA specifically posed a number of Internet privacy questions and requested comments that address the most impending dangers to Internet users' privacy.

These comments will address with particularity the looming threat to users' privacy rights posed by deep packet inspection ("DPI") and the wholesale monitoring of Internet communications by broadband providers. Monitoring through DPI is today imposed upon Americans as a mandatory condition of broadband service. These terms are offered on a take it or leave it basis and users must consent to DPI in order to obtain service. But as a matter of law, users waive all expectations of privacy when they knowingly submit their communications to the inspection of the third party broadband provider.

Data Foundry requests the NTIA and the Internet Policy Task Force establish a public policy against the compulsory waiver of privacy as a condition of receiving broadband service. This policy would be privately enforceable in courts of law and would empower Internet users to protect their own privacy. A public policy against terms of service that impose monitoring would set a default rule of privacy for the Internet, rather than the current default of no-privacy. A declaration of public policy would provide meaningful protection for user privacy and security that is neither overly regulatory nor dependent upon unaccountable self regulation.

## Comments

### I. The Monitored Internet

The Internet is quickly turning into a monitored network as the use of DPI has become widespread and pervasive. Over 20 broadband providers in the United States have acknowledged either current or past use of DPI. DPI vendors Sandvine and Arbor Networks alone claim over 300 worldwide customers, including 13 of the 20 largest American broadband providers. Using the same technology that forms the Great Firewall of China, broadband providers are peering into the packets that traverse their networks and are monitoring American Internet users' online activities.

Few broadband providers will freely admit to the use of DPI because the technology is highly controversial. Generally, broadband providers mask their DPI-facilitated capabilities under the euphemism of "network management." Only when faced with public outrage and political scrutiny for certain contentious network practices, such as BitTorrent throttling and behavioral advertising, have broadband providers acknowledged their use of DPI. And while those highly-publicized practices supposedly stopped, the monitoring equipment almost certainly remains in place and Data Foundry believes it is still being used to invade Americans' privacy.

DPI constitutes the wholesale monitoring of Internet users' communications. As the Federal Communications Commission has previously noted, "DPI involves examining the contents of Web browsing session, email, instant message, or whatever data the packet contains."[1] Essentially, DPI allows broadband providers to see everything that their users do on the Internet in real-time and provides the capability of acting on that information.

While offensive to many Internet users, this highly-invasive form of monitoring presents a lucrative opportunity for broadband providers to monetize the content and various forms of traffic that touch their networks. This presents a clear conflict between the business interests of the broadband providers and the privacy interests of Internet users. For the broadband providers, it is all too easy to sacrifice the privacy of their customers for the additional revenues created by DPI. This conflict between user privacy and broadband providers' profits came to a head in the NebuAd scandal. In that instance, it took a Congressional inquiry to force a number of broadband providers to stop selling private information about their users' Internet activities and Web whereabouts.

## II. With Monitoring, Traditional Expectations of Online Privacy Are Lost

Packet monitoring is anathema to an Internet that has traditionally maintained users' reasonable expectations of privacy. Courts have long recognized the confidentiality of users' online communications and their associated rights of privilege.[2] These privacy rights, however, have always depended upon the assumption that Internet communications travel from party to party – and network to network – without inspection by the carriera. The Internet and online privacy law have developed in conjunction under the premise that tools like DPI are *not* used to

[1] *See* Notice of Inquiry, *In the Matter of A National Broadband Plan for Our Future*, FCC 09-31 (rel. Apr. 8, 2009) at fn 89.

[2] *See e.g. United States v. Maxwell*, 45 M.J. 406 (1996).

invade the privacy of users' traffic. This recognition of online privacy has facilitated many of the most important features of today's Internet, such as free expression and e-commerce.

Internet users today expect and depend on having privacy in their online communications. In the NOI, the NTIA explained that, "consumers must be able to trust that their personal information is protected online and securely maintained." Users communicate in confidence with their doctors and attorneys, they shop and bank online, and business users communicate trade secrets and proprietary information over the Internet. These expectations of privacy have become engrained in Internet users and have provided Americans with the confidence to embrace the Internet with great enthusiasm.

One noteworthy exception to users' traditional expectations of privacy, however, has been in situations of workplace monitoring of employees' online communications. American courts have reasoned that employees cannot reasonably expect any confidentiality when they know that their employer is monitoring their communications.[3] There can be no privacy in such an instance and any information placed on a monitored work network will be deemed to have been knowingly disclosed. This is a commonsense rule of privacy law that applies identically to other forms of communication.[4] DPI now threatens to expand the application of this rule to the Internet at large.

In an online environment of wholesale DPI, Internet users cannot maintain reasonable expectations of privacy. Just as with monitored work networks, monitored broadband provider networks are not confidential and any communications placed on such networks are public by

[3] *See e.g. Scott v. Beth Israel Medical Center, Inc. et.al.*, 17 Misc. 3d 934 (Sup. Crt. NY 2007).

[4] See Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & Tech. 2 (2007) ("The third party doctrine provides that information 'knowingly exposed' to a third party is not subject to Fourth Amendment protection because one 'assumes the risk' that the third party will disclose that information to the government. Under this test, constitutional privacy interests in information are both bright and binary. It does not matter if the information is exposed for a limited purpose, or in confidence; it matters only whether the individual should know the information was made available to another party.").

nature. Broadband providers' mandatory terms of service clearly put users on notice of monitoring, and, by consenting to these terms, users have waived their privacy rights.[5] By merely accessing these networks and subjecting their communications to DPI, users have made a knowing disclosure of their information and all privacy rights that once applied have vanished. With DPI, the traditionally confidential Internet is replaced with one that is persistently monitored and totally without privacy.

## III. The Implications of an Internet Without Privacy

An online environment that is subject to monitoring through DPI and without any expectations of privacy is a fundamental change to the nature of the Internet. Whereas users could previously expect confidentiality in their personal communications, such as financial transactions and Web surfing, this information is now public and in the hands of a third party broadband provider. This is an Internet with a default *no*-privacy rule. Whatever users do online, their activities are being watched and potentially recorded. And without the traditional safeguards associated with private information, broadband providers are under no duty to protect this information and keep it out of the hands of others.

While broadband providers may reassure their customers that their private information will be used for only a limited purpose and will remain safe with the company,[6] such promises

---

[5] *See e.g.* Verizon Online Terms of Service, http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=TOS (last visited Jun 8, 2009) ("Verizon may, but is not required to, monitor your compliance, or the compliance of other subscribers, with the terms, conditions or policies of this Agreement and AUP. You acknowledge that Verizon shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Service, including but not limited to content that violates the law or this Agreement.").

[6] *See e.g.* AT&T Privacy Policy for AT&T Yahoo! and Video Services, http://helpme.att.net/article.php?item=8620 (last visited Jun 8 2009) ("Conducting business ethically and ensuring privacy is critical to maintaining the public's trust and achieving success in a dynamic and competitive business climate. Privacy responsibility extends not only to protection of customer account information but to the privacy of conversations and to the flow of information in data form. Subsidiaries and affiliates of AT&T Inc. (the "AT&T family of companies") understand that the trust of our customers necessitates vigilant, responsible privacy protections.").

are hollow and legally ineffective.[7] This is because privacy is binary – information is either wholly private or wholly public[8] – and once that information has been inspected by a third party broadband provider, that data becomes public to all and can never again be deemed private. Thus, as with all public information, the records of users' online communications would not be subject to the protection of privacy laws and could be permissibly sold or released by the broadband provider.

A monitored Internet, without reasonable expectations of privacy, would profoundly change the way that Americans communicate. Consumers' need to maintain the confidentiality of their private information would not change and many, particularly businesses, would be left searching for other means of sending sensitive communications, such as by mail or facsimile. Data Foundry has already witnessed this effect first hand, as a number of our customers have inquired into the security of their data as it travels the Internet to our data centers. In response, we can only guarantee the security of their information once it has arrived at our facilities and are forced to admit that our customers' data is almost certainly not private and secure on the public Internet. One customer, a law firm that needs to maintain the confidentiality of its attorney-client privileged communications, has stopped using the Internet to transmit its sensitive materials altogether. The customer now burns large amounts of data to disk, which it sends by overnight delivery to our data centers. Unfortunately, as more businesses and users come to the

---

[7] *See e.g. United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities...").

[8] *See* Daniel J. Solove, *The Digital Person*¸ 143 (2004) ("The secrecy paradigm … is deeply entrenched in information privacy law. In addition to focusing on whether information is completely secret or not, the paradigm categorizes information as either public or private. When information is private, it is hidden, and as long as it is kept secret, it remains private. When it is public, it is in the public domain available for any use. Information is seen in the black-and-white manner; either it is wholly private or wholly public.").

same realization about the public nature of online communications, abandoning the efficiency and benefits of the Internet will become more common.

## IV. Solution: The Protection of Privacy As a Public Policy

The destruction of all users' online expectations of privacy through widespread DPI should not be a part of America's broadband future. In helping to establish policies to protect Internet privacy, the NTIA and the Internet Policy Task Force should recognize the critical role that traditional expectations of privacy have played in the development and success of the Internet to this point. Maintaining users' privacy rights will be imperative in ensuring an open and prosperous Internet into the future. Users that want and require privacy should not be forced to submit to DPI as a mandatory condition of service and should have the opportunity to remain free from monitoring. DPI must only occur with the user's informed consent (opt-in) and actual knowledge that the result will be the total waiver of all expectations of privacy in their inspected communications. This standard of voluntary monitoring – rather than mandatory monitoring – would set privacy as the default rule for American broadband.

Data Foundry recommends that the Department of Commerce, the NTIA, and the Internet Policy Task Force mandate this rule through a simple declaration of public policy against the forced waiver of privacy as a compulsory condition of service. Such a declaration would be enforceable in courts, under traditional contract and consumer protection laws. This would empower Internet users to protect their own privacy rights by ensuring that broadband Internet access is never offered on a monitored-only basis. Should broadband providers violate this public policy and offer Internet access without a clear opt-in requirement for monitoring, it would be the consumers themselves and their state attorneys general that would bring broadband providers back into compliance.

A declaration of public policy against the non-consensual monitoring of Internet users' communications would be neither overly regulatory nor totally dependent upon faithful and honest self-regulation. The NTIA and the Internet Policy Task Force could essentially announce the policy and leave the role of enforcement with private citizens. This would relieve the federal government of the burden of *ex post* enforcement on a case by case basis and would avoid the dangers of political arbitrariness or regulatory capture. Private enforcement, rather than continuous federal regulation at multiple agencies would ensure that broadband Internet privacy is safeguarded for the future with the least administrative entanglement and the most accountability.

**Conclusion**

The traditional expectations of privacy associated with Internet communications have been one of the most important factors in the success of the Internet as a democratic medium. Privacy is not an end, but a means for the most fundamental of individual rights. On the Internet, privacy facilitates free expression, free exploration of ideas, free worship, and free communication with others.

Traditional expectations of online privacy have also helped to facilitate the explosion of e-commerce and the transition to a digital marketplace. It is critical for businesses that their transactions and communications remain private and free from third party purview. With reasonable expectations of privacy, businesses and consumers have learned to trust the Internet with their secret and proprietary information. With the Internet's inherent advantages of efficiency and availability of near limitless information, the online marketplace has become an integral part of America's economy.

All of these benefits of online privacy are now threatened by DPI and broadband monitoring. Unfair terms of service, offered on a take it leave it basis, require users to consent to the inspection of their communications and effectively waive their expectations of privacy. Data Foundry requests that the NTIA and the Internet Policy Task Force establish a clear public policy against broadband contracts that unfairly impose Internet monitoring upon Americans. Doing so would set a default rule of privacy for the Internet and require informed opt-in consent before users can be forced to submit to DPI. Such a public policy would provide meaningful protection for online privacy that is neither overly regulatory nor dependent upon unaccountable self regulation.

Respectfully Submitted

Matthew A. Henry
1250 South Capital of Texas Highway
Building 2, Suite 235
West Lake Hills, Texas 78746
512.888.1114
henry@dotlaw.biz
*Counsel for Data Foundry, Inc.*

June 14, 2010

**COMMENTS OF**

# DATRAN MEDIA LLC

**TO THE**
**UNITED STATES DEPARTMENT OF COMMERCE**
**REQUEST FOR COMMENTS ON**

# INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY

Steven Vine
Associate General Counsel &
Chief Privacy Officer
Datran Media, LLC
345 Hudson St.
5th Floor
New York, NY 10014
(212) 706-4866

June 14, 2010

# TABLE OF CONTENTS

Datran Media LLC ("Datran") appreciates the opportunity to provide these comments regarding the Department of Commerce Notice of Inquiry dated April 23, 2010 ("NOI") on information privacy and innovation in the Internet economy.[1] As a leading digital marketing technology company, we are pleased to offer our company's unique perspectives.

## I. ABOUT DATRAN MEDIA

Datran uses innovative technology to provide digital advertising solutions, audience measurement and analytics, email marketing services, and to otherwise help online companies to market their products and services in the digital space. (This, in turn, allows consumers to receive free online content.) More than 1,000 top consumer brands have relied on Datran to deliver campaigns to achieve their customer branding, acquisition, and retention goals. Moreover, as explained in these comments, Datran will soon be introducing a service that will empower consumers by enabling them to exercise clear and meaningful choices regarding their advertising preferences, including to opt out or opt in to tailored advertising, at the brand level or more broadly from advertising networks.

A bedrock principle followed at Datran is that of "Privacy by Design." Privacy is built into all of our products and services. Datran, of course, complies with all privacy laws and legal obligations. But beyond that, Datran is deeply committed to protecting consumer privacy. To that end, our company is an active member of many self-regulatory organizations including the Better Business Bureau, the Interactive Advertising Bureau (IAB), the Direct Marketing Association, the International Association of Privacy Professionals, the Online Trust Alliance (OTA), the Email Sender and Provider Coalition (ESPC), and others. As addressed below, we are adopting, embracing, and helping to develop best practices for our industry.

---

[1] *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 Fed. Reg. 21,226 (Apr. 3, 2010).

## II. INTRODUCTION

Because Datran's business focuses on online marketing and related activities, our comments are limited to the ongoing debate over privacy and online behavioral advertising. That debate has focused primarily on whether the current self-regulatory model as endorsed by the Federal Trade Commission ("FTC") and implemented by various industry organizations is working or whether new legislation is needed. The FTC, legislators, and even some privacy advocates recognize that any regulatory model governing consumer online advertising and privacy, whether industry self-regulation, new legislation, or ad hoc enforcement by the FTC under its Section 5 authority, must take into account the vital role that advertising dollars play in supporting the widely available, free, and quality content that makes the Internet valuable to consumers.[2]

---

[2] *See, e.g.*, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 6 (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf (describing online behavioral advertising's potential benefits to consumers and businesses, including "delivering more relevant ads to consumers, subsidizing free online content, and allowing businesses to market more precisely and spend their advertising dollars more effectively"); Jon Eggerton, *Leibowitz: FTC Not Interested in Regulating Behavioral Ads if Industry Can Do Job*, Broadcasting & Cable (May 12, 2010), http://broadcastingcable.com/article/452590-Leibowitz_FTC_Not_Interested_in_Regulating_Behavioral_Ads_If_Industry_Can_Do_Job.php (quoting FTC Chairman Jon Leibowitz as stating that behavioral advertising is "good for the Internet, where online advertising helps support the free content everyone enjoys and expects"); Boucher, Stearns Release Discussion Draft of Privacy Legislation (May 4, 2010), http://boucher.house.gov/index.php?view=article&id=1957 (quoting Representative Rick Boucher (D–VA), who stated: "Online advertising supports much of the commercial content, applications and services that are available on the Internet today without charge . . . ."); CTR. FOR DEMOCRACY & TECH., ONLINE BEHAVIORAL ADVERTISING: INDUSTRY'S CURRENT SELF-REGULATORY FRAMEWORK IS NECESSARY, BUT STILL INSUFFICIENT ON ITS OWN TO PROTECT CONSUMERS 3 (2009), *available at* http://cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf ("The Center for Democracy & Technology (CDT) recognizes that advertising is an important engine of Internet growth. Consumers clearly benefit from a rich diversity of content, services and applications that are provided without charge and are supported by advertising revenue."); *see*

Some privacy advocates and consumer groups, however, argue that the current self-regulatory model has failed. Datran disagrees with this assessment. Datran believes that if consumers are provided with appropriate tools to choose how their personal information is used online and to control the types of advertising targeted to them in a manner that does not disrupt the online advertising ecosystem and its subsidization of free content, then any need for far-reaching legislation or regulation is negated. Industry groups have been developing such tools,[3] but other marketplace solutions are also developing, including a tool that will soon be available from Datran.

Specifically, as we explain in Part III below, Datran is proud to be developing a first-of-its-kind privacy-enhancing technology that will allow consumers to customize the targeted advertisements they receive, even down to the advertiser or the type of product or service offered. This technology, developed in accordance with self-regulatory principles, is a prime example of how self-regulation is transforming the online marketing industry to incorporate transparency and choice into every advertisement offered to consumers. Recent research demonstrates that Datran's privacy-enhancing technology tools will be welcomed by consumers.

In addition, Datran is concerned that calls for legislation and regulation may result in a regime that unduly restricts advertising and commerce.[4] However, as explained in Part IV below,

---

*also infra* Part IV.C (describing recent study that indicated that only 10% of Internet users would prefer to pay for a majority of the information and services they access online in exchange for no online advertising).

[3] *See, e.g.*, IAB & NETWORK ADVERTISING INITIATIVE, CLEAR AD NOTICE: TECHNICAL SPECIFICATIONS FOR THE IMPLEMENTATION OF THE INTERACTIVE ADVERTISING SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (Apr. 2010), *available at* http://iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf.

[4] For example, there have been numerous critiques of proposals like the draft legislation Representatives Rick Boucher (D–VA) and Cliff Stearns (R–FL) circulated in April, *see* Boucher, Stearns Release Discussion Draft of Privacy Legislation (May 4, 2010),

Datran does not oppose limited, smart legislation or regulation that provides a level playing field and regulatory certainty, provided it does not unduly burden online marketing. Moreover, any legislation or formal regulation should not interfere with the development of consumer-friendly privacy-enhancing technologies. In addition to these comments, Datran fully supports the comments being submitted by the OTA.

---

http://boucher.house.gov/index.php?view=article&id=1957, and Datran agrees with the criticisms addressed by groups such as OTA. *See, e.g.*, Letter from Craig Spiezle, Executive Dir., OTA, to The Hon. Rick Boucher & The Hon. Cliff Stearns, Chairman & Ranking Member, Comm. on Energy & Commerce, Subcomm. on Commc'ns, Tech. & the Internet, U.S. House of Representatives (June 4, 2010), *available at* https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf.

## III. DATRAN'S PREFERENCECENTRAL WILL GREATLY ENHANCE CONSUMER TRUST IN INTERNET COMMERCE BY PROVIDING CONSUMERS WITH EXTENSIVE CONTROL

As the Department acknowledged in the NOI, companies are developing privacy-enhancing technologies to create enhanced notification to consumers about privacy policies and to manage the information they are sharing.[5] The Department's Internet Policy Task Force is seeking input on these technologies and their potential to enhance consumer trust in Internet commerce.[6] Datran is currently developing a first-of-its-kind privacy-enhancing technology that will revolutionize online behavioral advertising and enhance consumer trust in Internet commerce by incorporating transparency and choice into every advertisement offered to consumers. Empirical research demonstrates that consumers are willing to adopt this technology when introduced, and that doing so will increase their trust in online behavioral advertising.

Datran's new tool, PreferenceCentral,[7] will accomplish this goal by respecting consumer choice and providing consumers with access to profile data where they can exercise clear and meaningful control. Offered as a free service to consumers, PreferenceCentral will be accessible whenever a consumer clicks an icon accompanying a tailored advertisement served by a participating ad network or advertiser. Consumers will then see an intuitive interface that enables consumers to learn about, control, and improve the quality and relevance of advertising they receive. Consumers will be able to customize their advertising preferences by advertiser, publisher,[8] and ad network,[9] even down to the specific types of products and services for which

[5] NOI at 21,230.
[6] *Id.* at 21,230-31.
[7] http://preferencecentral.com. Datran is developing PreferenceCentral.com through its subsidiary, UnsubCentral.
[8] The publisher is the website where an ad appears.

they wish to receive or decline to receive ads. PreferenceCentral will also allow consumers to easily and intuitively opt out of targeted advertising altogether. These preferences will be persistent – upheld whenever consumers access a website served by participating networks regardless of the browser or device they are using in subsequent sessions. Consumers will also be able to access their preferences and make changes at any time through participating marketers' preference centers. By enabling consumers to grant permissions to specific merchants across various media channels and networks, PreferenceCentral is the first and only product that delivers a control solution that is consumer-centric.

For marketers, including individual brands, the consumer-reported preferences will make offline and online marketing more efficient and effective by reducing wasted ad impressions and increasing the likelihood of generating a favorable response from marketing campaigns. PreferenceCentral offers marketers, including individual brands, a turn-key, easy-to-deploy preference center solution to help manage consumer choices, whether they be opt-in or opt-out. Therefore, PreferenceCentral will create value for both consumers and advertisers, ensuring consumers are not targeted against their wishes while still supporting the basis for free content on the Internet.

### A. How PreferenceCentral Will Work

The following is a description of how PreferenceCentral will work along with some visual samples of PreferenceCentral interfaces. Each ad served by participating networks will be accompanied by a link comprised of an explanatory phrase along with the "Power I"[10] icon to

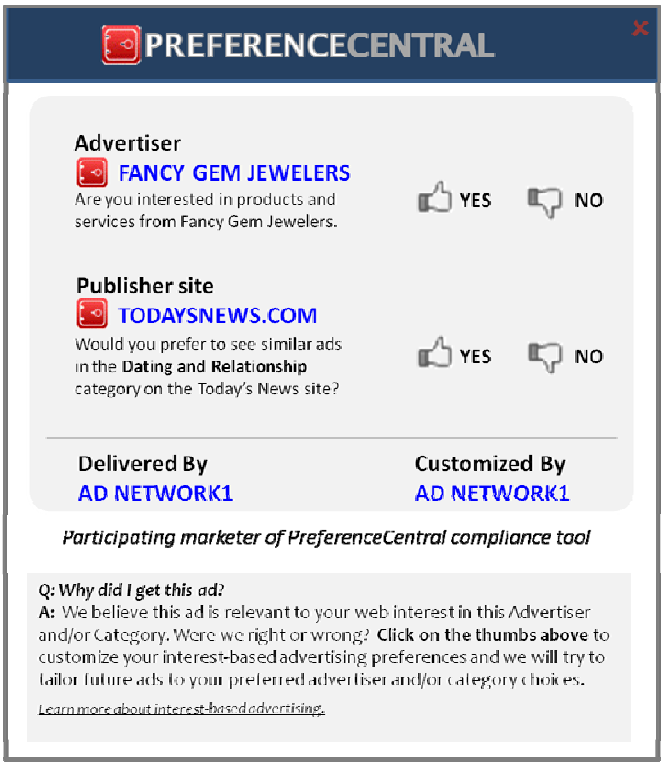
---

[9] An ad network is a company that matches ads and advertisers with numerous, unrelated publishers that will display the ads, and that facilitates the display of the ads on the publishers' websites.

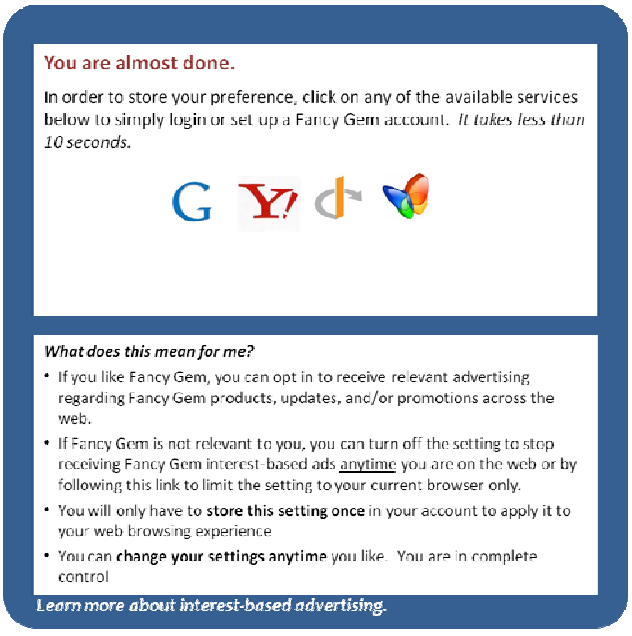
[10] *See* Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, *available at* http://nytimes.com/2010/01/27/business/media/27adco.html.

alert users to the existence of the behavioral ad. For example, the following ad for a jewelry brand could appear on a newspaper's website:

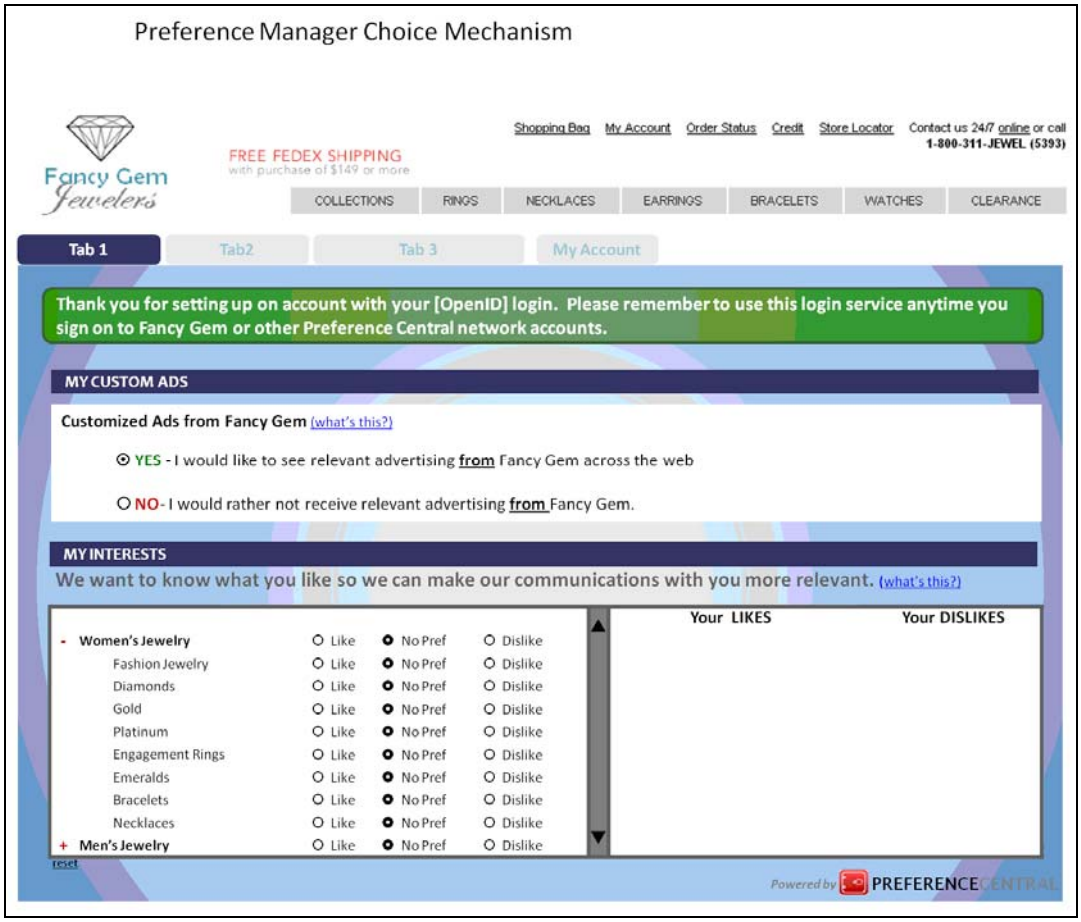

When a user clicks on the link, a box will be displayed on the screen that lists the advertiser, the publisher, the ad network, and the reason the consumer was delivered the ad. Users will be able to opt in or out of targeted ads of this kind or from that particular website by clicking on a "thumbs up" or "thumbs down" icon as shown here:



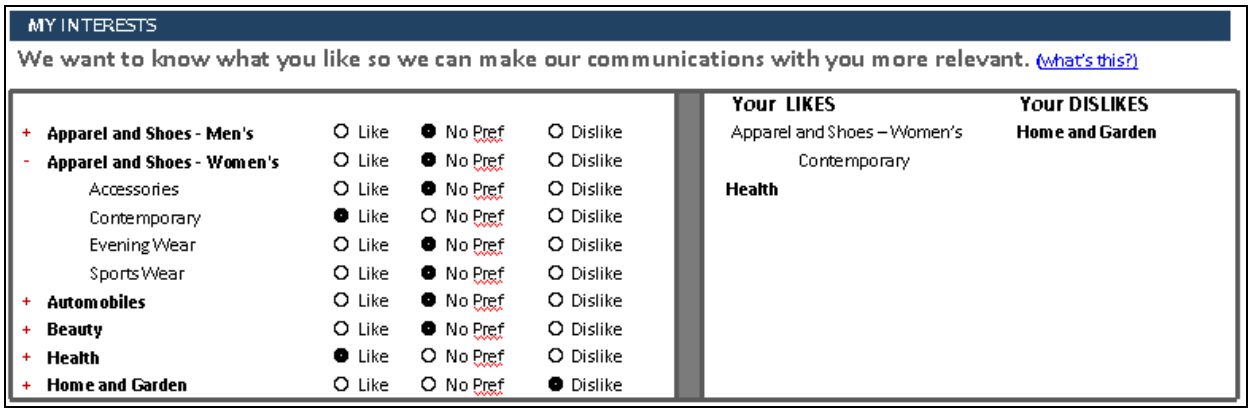

If they are not already logged in, they will be taken to the marketer's preference center powered by PreferenceCentral. Users can set up PreferenceCentral accounts through any a number of login services including Google, Yahoo, OpenID, and MSN by clicking on the corresponding icons. This screen will look like the following:



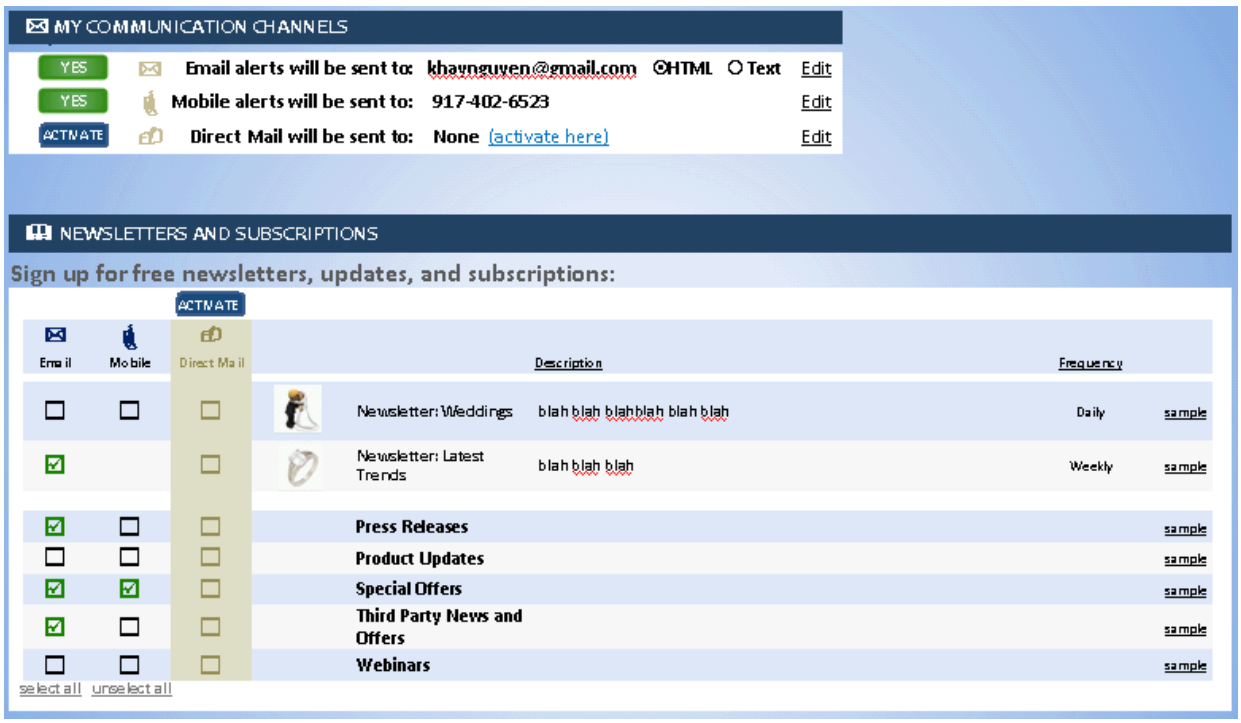
Once the login is authenticated via the provided login service, users will be taken to the main page of the user's PreferenceCentral account, which will look like the following:




From this interface, users can save within their PreferenceCentral account their preferences regarding whether they wish to receive customized ads from a particular publisher, from a particular advertiser, or even about particular products and services. In this example, where the user has indicated a desire to express preferences about an *advertiser*, users can further customize the specific products and services associated with their tailored advertising (in this case diamonds, gold, platinum, etc). When the user wants to customize ads on a specific *publisher site*, the range of possible advertisements is broader so the categories displayed are more generic, as shown below:




There will be additional options to further allow consumers to manage their direct communications with the given brand. Among some of the features will be the ability for consumers to opt in to newsletters, updates, and other subscriptions via specified channels like email, mobile devices, and direct mail.




Users will also be able to log into their PreferenceCentral account(s) at any time to change or update these preferences.

These and other options available through PreferenceCentral will ensure that advertising is tailored to users' interests and that the serving ad network will exclude advertisements for unwanted products and services. By notifying users more clearly that an advertisement is served based on a behavioral profile and granting users more control over the ads they are served, privacy-enhancing technologies like PreferenceCentral will help demystify online behavioral advertising and greatly enhance consumer trust with participating brands, and eventually with the industry and Internet commerce in general.

### B. Empirical Research Demonstrates That Consumers Are Willing to Adopt PreferenceCentral, and That Doing So Will Increase Trust in Targeted Advertising

In the NOI, the Department asked whether consumers have readily accepted or used privacy-enhancing technologies when made available, and whether current available privacy-enhancing technologies have increased user trust.[11] While PreferenceCentral has not yet been released, empirical consumer research demonstrates that consumers are willing to adopt PreferenceCentral for its privacy-enhancing capabilities, and that doing so will increase those consumers' trust in customized advertising.

Just last month, Datran, with support from Survey Sampling International, surveyed 1,050 randomly selected Internet users to answer questions designed in part to gauge the potential adoption and effectiveness of PreferenceCentral.[12] The survey provided some context to consumers about the trade-offs involved with online behavioral advertising. The survey also revealed important information about consumers' willingness to receive customized ads when they could exercise control over the customization.

---

[11] NOI at 21,231.

[12] While the formal survey results have not yet been released, we are pleased to provide preliminary results with relevant slides that we are attaching as an Appendix.

For example, when consumers were informed that online ads are commonly tailored for specific consumers based on their online behavior, 70% of those surveyed indicated an interest in using PreferenceCentral, with a third of all respondents indicating that they were either "extremely" or "very" interested.[13] Of those that indicated an interest, 59% indicated that they were driven by the promise of control – that they would have the power to control which ads they wanted to receive or eliminate, or that they would have control over how their information would be used by advertisers.[14] The responses also indicated that PreferenceCentral would markedly diminish consumers' concerns about behavioral advertising, as 41% of respondents stated that they would be "more comfortable" about the use of targeted ads due to the availability of PreferenceCentral.[15]

This study presents important information about the prospects for consumer adoption of PreferenceCentral and its potential to enhance transparency and consumer choice regarding online behavioral advertising. The survey results indicate that self-regulatory efforts to encourage the development of privacy-enhancing technologies such as PreferenceCentral are succeeding. After implementation of PreferenceCentral, Datran intends to conduct further consumer surveys and research to examine the actual operational impact PreferenceCentral and similar tools have for consumers. It is important that any consumer survey attempting to accurately capture consumer sentiment be conducted in a manner that promotes consumer awareness of the trade-offs between customized advertising (and with it, free and high-quality content) and generic advertising (usually entailing lower-quality content or even an imposed fee

[13] *See* Appendix at A-6.
[14] *See* Appendix at A-7. Interestingly, the respondents' primary aversion to tailored advertising was not an invasion of privacy (only 10% of respondents indicated that this was their primary concern), but instead was an aversion to advertisements in general (61%). *See* Appendix at A-5.
[15] *See* Appendix at A-8.

for content access).[16] Datran is confident that PreferenceCentral and other privacy-enhancing technologies borne of self-regulatory efforts will demonstrably enhance consumers' trust in online advertising and enable the Internet to flourish for consumers.

[16] *Cf.* Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214 (describing a study stating that a majority of Americans did not want tailored advertising, but failing to consider the trade-off between receiving tailored advertising and receiving free content versus not receiving tailored advertising and having to pay for content). Although not addressed in Datran's most recent study, consumers should also be aware when surveyed that online behavioral advertising does not necessarily mean greater amounts of advertising.

## IV. DATRAN SUPPORTS APPROPRIATE FEDERAL LEGISLATION OR FORMAL REGULATION TO PROTECT CONSUMERS AND SET EXPECTATIONS

Unlike some in our industry, Datran is not opposed to narrowly tailored federal legislation or formal regulation that extends certain fundamental privacy protections to consumers, including legal requirements that foster transparent practices and that empower consumers with the choice of how companies can collect and use their personal information. Appropriate legislation would reduce regulatory uncertainty, providing a level playing field for businesses involved in online behavioral advertising, allowing firms like Datran to plan their business operations around established modes of conduct, as well as offering consumers a fundamental level of protection from advertising abuse. It is important though that legislation or regulation not unduly restrict commerce because consumers' welfare could potentially be negatively affected due to a loss in advertising revenue. Furthermore, certain proposals that purport to protect consumers can be counterproductive especially if they hinder mechanisms and products that are in place to allow consumers to control their advertising experience.

### A. Smart Legislation and Regulation Can Provide a Level Playing Field

Datran welcomes appropriate legislation or formal regulation that would level the playing field for the many companies such as Datran and others that already abide by self-regulatory principles and that operate in a manner respectful of consumer privacy. Some companies in the online marketing arena may gain a competitive advantage by not following, or even intentionally disregarding, transparency and choice. In the current self-regulatory environment, these actors can simply choose to ignore the existing regimes in an effort to maximize profit. Datran supports legislative or formal regulatory efforts in this area to curtail these questionable practices, to better inform consumers of how their personal information is collected and shared for

marketing purposes, and to provide a baseline set of standards that all members of the online advertising ecosystem must follow to ensure that these goals are met.

### B. Appropriate Regulation and Legislation Can Reduce Regulatory Uncertainty

The lack of appropriate legislation or formal regulation makes business planning difficult for companies like Datran. Legislation or formal regulation would also help create certainty about Datran's compliance obligations as it continues to be a leading innovator in the online marketplace. Through laws designed to prevent unfair or deceptive trade practices, online privacy currently is regulated on an *ad hoc* basis by the federal government and the states. In addition, there are regular calls and proposals for additional legislation and regulation, which make it difficult to predict the path of regulation. The piecemeal approach to the regulation of privacy means that companies like Datran must constantly monitor for legislative and regulatory developments in different jurisdictions. It also means that in designing its services to be consistent with the latest legal and industry standards, it is difficult to design and implement innovative marketing tools that have the potential of unpredictably being declared out of bounds. Therefore, Datran welcomes federal legislation or formal regulation that would preempt state law, which would allow companies to focus on a single, comprehensive, and fair legislative or regulatory regime.

### C. Federal Legislation or Formal Regulation Should Not Harm Commerce by Unduly Burdening Online Marketing

Online advertising supports much of the commercial content, applications, and services that are available on the Internet today without charge.[17] Datran is proud to help support free content by contributing to this online advertising ecosystem, and staunchly supports allowing

[17] *See supra* note 2.

consumers to make informed choices regarding whether to share their information for advertising purposes.

Any prospective federal privacy legislation or regulation must consider its effect on the viability of online marketers that subsidize free content on the Internet. If legislation or regulation unduly burdens online marketers, websites may soon have to resort to charging fees to consumers to access their websites. In addition, since targeted online advertisements result in 2.68 times more revenue than non-targeted advertisements,[18] any legislation or regulation that affects the profitability of targeted advertisements, or their ability to link profile information to a user or computer, will cause a corresponding precipitous drop in the revenues earned by websites, increasing the likelihood that more websites will need to charge consumers for access. This is a scenario overwhelmingly rejected by consumers. Datran's recent consumer research indicates that when given a choice between content subsidized by advertising and ad-free content with a charged fee, only 10% of Internet users would prefer the latter.[19] A large number of consumers would seemingly be ill-affected if ad revenue could not supply them with the abundant and free content they have grown accustomed to accessing.

Legislation and regulation must take into account these benefits and weigh them against the potential harm to consumers. When companies engage in online advertising consistent with current, robust self-regulatory principles with transparency and choice for consumers, particularly opt-out choice where non-personally identifiable information is used in online advertising, consumers benefit.

---

[18] Press Release, Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More than Twice as Valuable, Twice as Effective as Non-Targeted Online Ads (Mar. 24, 2010), *available at* http://networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

[19] *See* Appendix at A-9.

## V. CONCLUSION

Datran appreciates this opportunity to submit its comments. Through privacy-enhancing technologies like PreferenceCentral designed to comply with self-regulatory principles in the online advertising industry, Datran and others are giving consumers greater control over the advertisements they receive, which will ultimately lead to increased consumer trust in Internet commerce. Moreover, the country is at a historical moment in the development of the Internet, and the Department, through its report on information privacy and innovation in the Internet economy, can help spur online commerce by recommending that the Administration support limited, narrowly tailored legislation or formal regulation that would establish a level playing field and certainty about compliance without unduly burdening commerce. As long as the online marketplace is transparent about how its uses consumer information, and consumers are afforded control over this information, it is important to have the ability to share information with others in the online advertising ecosystem to ensure that advertising can support the availability of free, robust content for consumers.

PREFERENCECENTRAL

# *Appendix*

## *Consumer Perspectives on Online Audience Measurement & Advertising Relevance – 2010*

***PreferenceCentral Benchmark Research Study,***
***with support from Survey Sampling International***

# Research Plan

## Concept Statement

**PreferenceCentral** is a free service that provides consumers with complete control of what targeted advertising they receive online and complete visibility into what information advertisers use to target the advertisements. More specifically, **PreferenceCentral** provides consumers:

- **Complete Control**: Consumers will now be able to select what online advertising they will get – Selecting the categories, brands, or advertisers in which they are interested AND those from which they do not want to receive advertisements;
- **Complete Transparency**: Consumers will now know what information is being used by specific advertisers to target advertising to them AND have that specific advertiser stop use of that information for targeting. This will happen through a notification in every targeted ad that links to an account where a consumer can exercise control;
- **Monitoring & Enforcement**: PreferenceCentral will also monitor online advertising to assure that consumers' preferences and industry best practices are being used by advertisers.



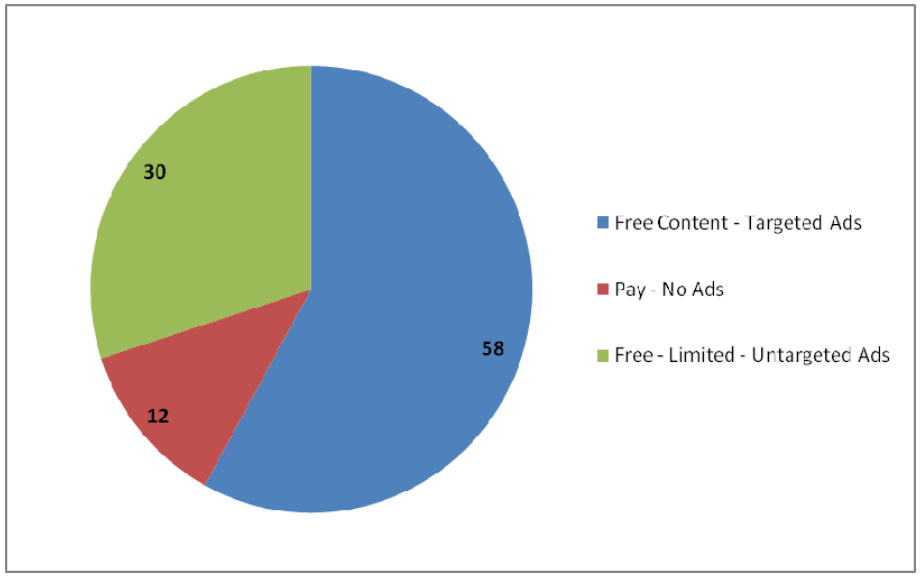
PREFERENCECENTRAL

# Research Plan – Sampling Frame

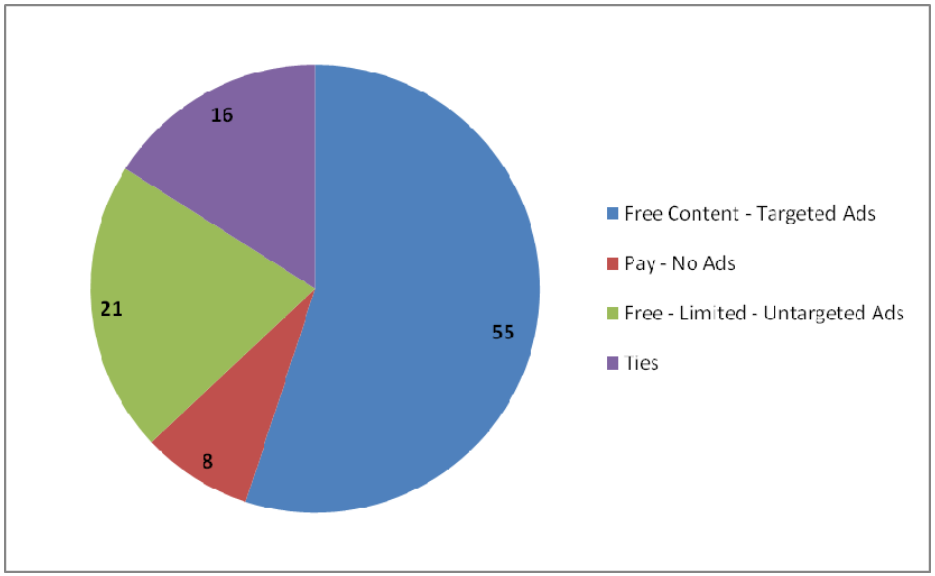
- Online questionnaires completed by 1,050 Internet Users 18 to 64 years of age
- Survey Sampling International (SSI) selected Internet Users using their Dynamix Platform:
  - Randomly selecting 50% panel & 50% online "real-time" recruited
  - Screened for age and gender to assure proportionally-representative sample
  - Sampling across days-of-week and day-parts to minimize DOW-TOD biases
  - Fieldwork started May 21 and was completed May 28
  - Completion rate of 85%
  - Average duration: 10 minutes
- Error estimates at 95%-confidence level are +/- 3% (with P = .5)

# Current-State – Trade-Off Favors "Free Content with Targeted Ads"

- **In trade-off, a majority of consumers (55%) prefer free content-targeted ads**




**Average Allocation**




**% Internet Users**

*Q: What proportion of your time would you prefer to spend among each of the options below?*
*Base total = 1050 (Error estimate = +/- 3% at 95% CL )*

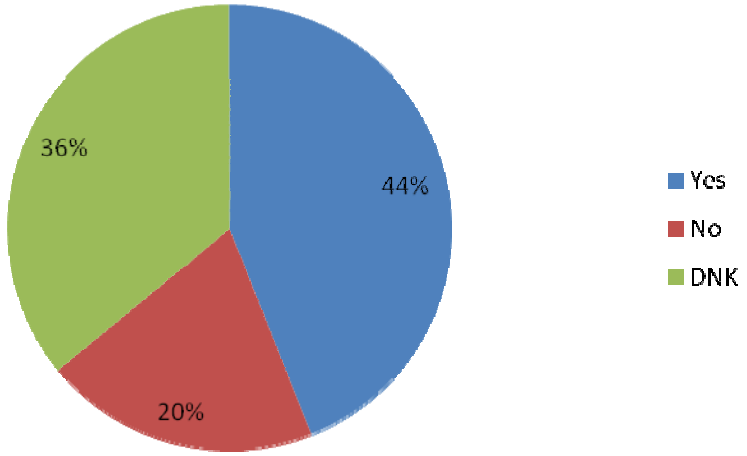


PREFERENCECENTRAL

# Desire for Websites Visited to Show Tailored Ads

- With this wording, now a minority of consumers express a desire for tailored ads
  - This corroborates the result obtained in the recent Annenberg study (2010)
- However, the primary reasons reflect a dislike for online ads, not a concern for privacy

**Q: Would you want the websites you visit to show you ads that are tailored to your interests?**




| Key Reasons | Not Interested |
|---|---|
| - Not Interested in As | 16% |
| - Hate Ads | 16 |
| - Ads Annoying | 13 |
| - Interrupt | 10 |
| - Invasion of Privacy | 10 |
| - Don't Pay Attention | 7 |
| - If Need a Product | 7 |
| - Waste of Time | 6 |

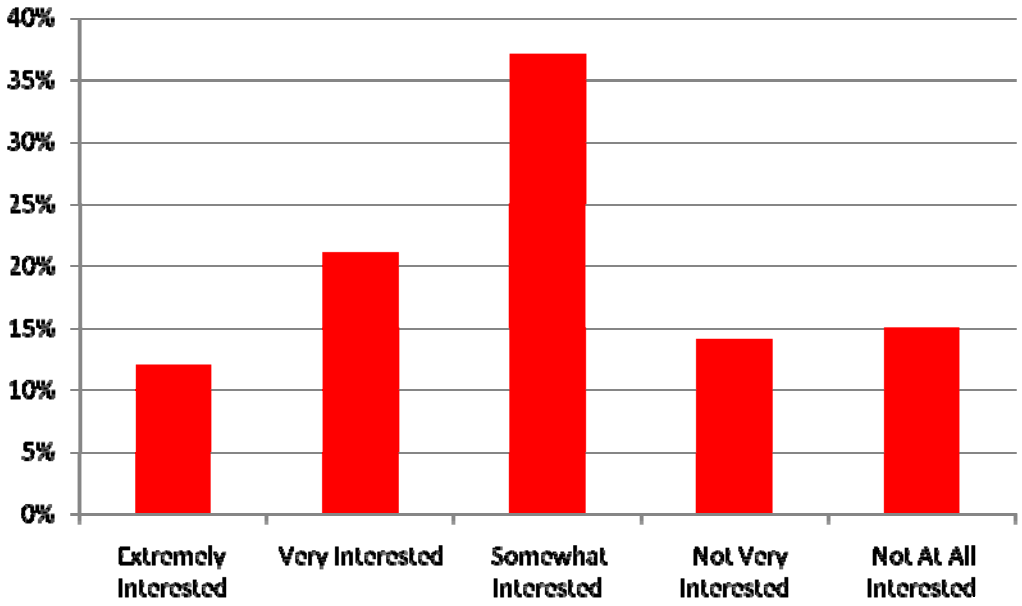
*Base total = 1050 (Error estimate = +/- 3% at 95% CL )*



PREFERENCECENTRAL

# Interest in Using PreferenceCentral

- **70%** of internet users are interested in using PreferenceCentral
  - A third are either extremely or very interested




**Q: Based on this description of PreferenceCentral, how interested would you be in using this free service?**

***Base Total = 1050 (Error estimate = +/- 3% at 95% CL )***



PREFERENCECENTRAL

# Reasons for Interest in PreferenceCentral

- Interested consumers are primarily driven by the promise of control
  - First in terms of the ads seen and not seen
  - Secondarily in their information
- Those not interested do not feel a need and/or just ignore ads
  - A few cite concerns that PreferenceCentral may itself present a threat to their privacy and safety – A recognized "seal of approval" will facilitate consumer acceptance

| Key Reasons | Interested | Not Interested |
|---|---|---|
| - Control of What I See | 34% | |
| - Interesting Idea | 15 | |
| - Wanted Ads/Eliminate Unwanted Ads | 14 | |
| - Control Over Information/Protection | 11 | |
| - Free | 10 | |
| - Don't Need | | 29% |
| - Don't Like Ads/Ignore Ads | | 26 |
| - Invasion of Privacy | | 5 |
| - Not Sure Safe/Trustworthy | | 3 |
| - Seems Like a Lot of Work | | 4 |

*Q: Why are you "interested/not interested" in PreferenceCentral?*

*Base total = 1050 (Error estimate = +/- 3% at 95% CL )*

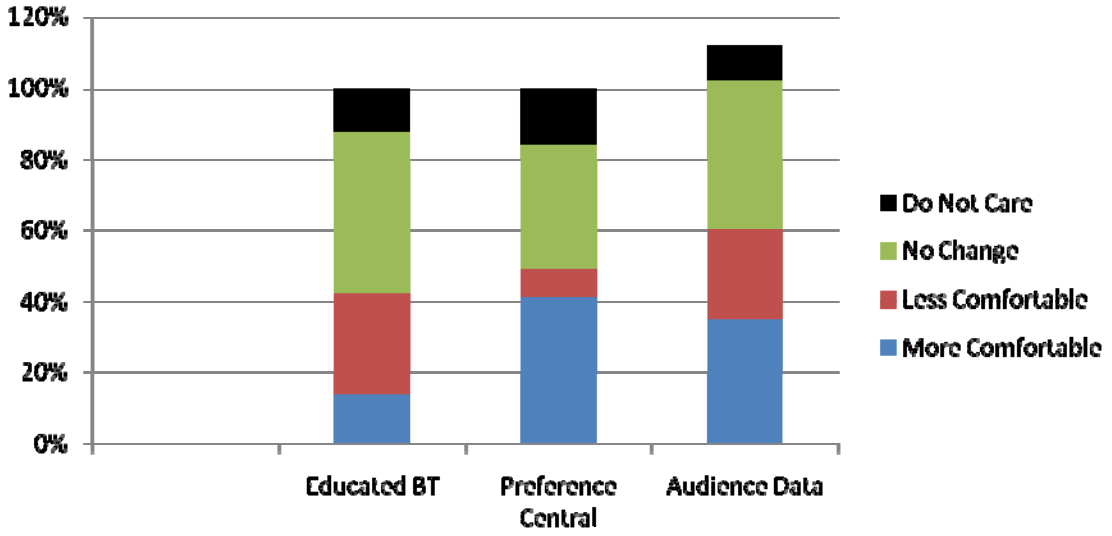


PREFERENCECENTRAL

# PreferenceCentral Provides Assurance Over Behavioral Targeting

- Availability of PreferenceCentral diminishes consumers' concerns about behavioral targeting – There is a pronounced shift towards more comfortable

***Q: Does the availability of PreferenceCentral change your attitude towards the use of behavioral information to target relevant online ads?***




| | More Comfortable | Less Comfortable | No Change | Do Not Know |
|---|---|---|---|---|
| | | | | |
| Educated BT | 13.5% | 28.6% | 45.1% | 12.6% |
| Preference Central | 40.9% | 7.9% | 34.8% | 16.2% |
| Audience Data | 34.8% | 25.5% | 41.4% | 9.8% |

*Base Total = 1050 (Error estimate = +/- 3% at 95% CL )*

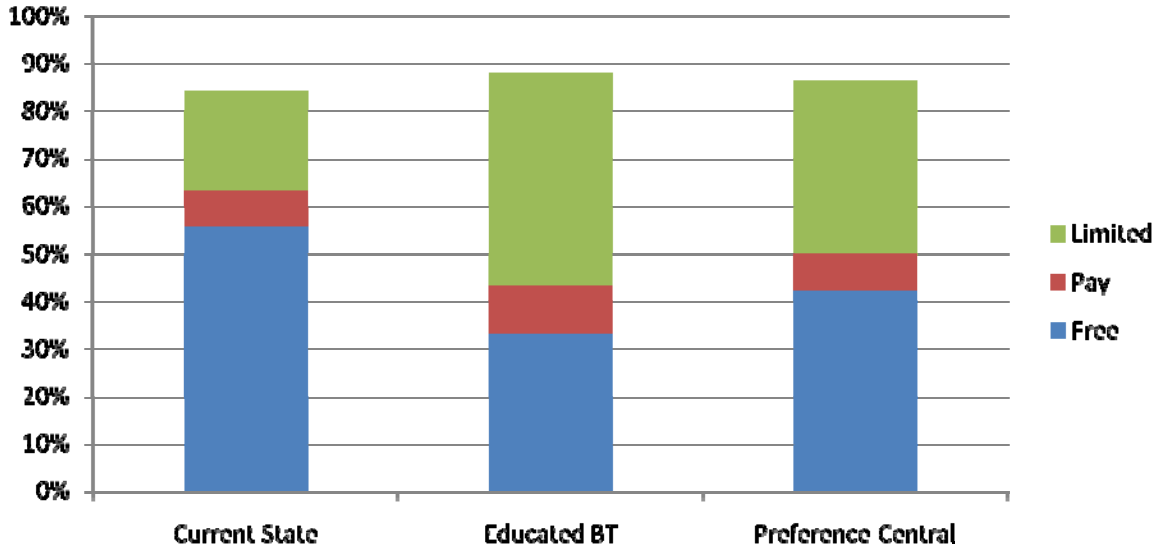


PREFERENCECENTRAL

# Content-Ad Trade-Off – Preference for "Free Content with Tailored Ads"

- PreferenceCentral generates interest and for some restores their "free-tailored" preference
- A steady minority of consumers state a preference for paying for ad-free content

***Q: What proportion of your time would you prefer to spend among each of the options below?***




| | Free | Pay | Limited |
|---|---|---|---|
| Current State | 55.4% | 7.5% | 21.2% |
| Educated BT | 32.8% | 10% | 44.7% |
| Preference Central | 42% | 7.9% | 36.3% |

*Base Total = 1050 – Classification based on highest-point allocation*



PREFERENCECENTRAL

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

SCHOOL OF INFORMATION
102 SOUTH HALL # 4600
BERKELEY, CALIFORNIA 94720-4600
(510) 642-1464
(510) 642-5814 Fax

**UNITED STATES DEPARTMENT OF COMMERCE**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**

**In the Matter of**

***Information Privacy and Innovation in the Internet Economy*** **Docket No. 100402174-0175-01**

**COMMENTS OF Deirdre K. Mulligan**

**June 14, 2010**

Thank you for the opportunity to offer comments on this important inquiry. It continues a long tradition of thoughtful inquiry into the resilience of regulatory, market, and self-regulatory mechanisms of privacy protection in the face of disruptive technological change. While continuing this long-standing U.S. tradition, it is distinct in its emphasis on the connections between privacy and innovation. This comment, therefore, seeks to highlight a set of issues where innovation and privacy are inextricably intertwined. Below, I set out three new concepts that are necessary to buttress privacy frameworks (represented in existing and international privacy laws and self-regulatory initiatives reflecting Fair Information Practice Princiles) that are undergirded, to varying extents, by assumptions of market competition and innovation on privacy terms; I discuss the inefficient and counterproductive effect of the current U.S. legal framework governing law enforcement access to personal information, email and private files stored in the Internet; and conclude with a discussion of some perhaps unexpected or unanticipated benefits of the Federal Trade Commission's defacto status as the regulator of privacy in the commercial marketplace, and the importance of transparency-forcing laws, such as the state security breach notification laws, in fostering improved stewardship of personal information.

**Competition, innovation and privacy**

The belief that competition and consumer trust would foster robust privacy practices in the private sector was a bedrock assumption of, *"A Framework for Global Electronic Commerce,"* issued by the Clinton Administration in 1997, and strongly influences today's dialogue about the necessity of new privacy legislation to govern the private sector. Companies routinely tout the ability of consumers to vote with their feet about privacy in comments such as "competition is a click away"[1] as a market mechanism that protects consumer privacy. On the flip-side the lack of mass exodus after publicized privacy failures has

[1] Miguel Helft, "Google Makes a Case That It Isn't So Big", *The New York Times*, June 28, 2009. http://www.nytimes.com/2009/06/29/technology/companies/29google.html
E.B. Boyd, "Google Privacy Chief: 'We Absolutely Compete on Privacy'", *BayNewser*, January 29, 2010 http://www.mediabistro.com/baynewser/privacy/google_privacy_chief_we_absolutely_compete_on_privacy_150406.asp

been used to defend companies privacy-corrosive actions after the fact. For example, in responding to journalists questions about changes to Facebook's privacy settings CEO Zuckerberg said, "We look at how many people leave the service and deactivate their accounts. Privacy was not a major meme among Facebook users…We have seen no meaningful uptick in the number of people who deleted their accounts."[2]

Surely, there is no doubt that a market for privacy, whether undergirded by a regulatory floor or not, would be beneficial to consumers: For at least some consumers will desire and seek out privacy in excess of whatever regulatory minimum is established. Yet, given the rather heated public outcry about shifts in privacy practices by entities such as Google and Facebook—who both trumpet consumer's ability to exit as an important check on their behavior—followed by limited actual consumer exit, it appears that the threat of exit may be empty, or at best limited.

I submit that for the threat of exit, fueled by robust competition on privacy, to inhibit over-reaching corporate behavior, the following additional market conditions must exist: 1) consumers must be able to easily port their information to alternate providers and services through the use of technical tools supported by open interfaces and data formats; 2) services and products that comprise part of the communication infrastructure of the Internet must be interoperable; and 3) data practices, including those that impact privacy and security, must be accessible in standard formats, using standard terms. The absence of these conditions in today's marketplace undermines privacy and innovation by allowing early market entrants to exploit users' sunk costs and network effects. Companies exploit users' sunk costs, represented in the Web 2.0 environment largely in reams of user-generated content (personal information, contact lists, copyrighted works, etc.), through the standard use of Terms of Service provisions that forbid the use of automated tools by users to interact with their own data. These provisions are buttressed by the deployment of technical protection mechanisms to thwart consumer use of such automated tools. They are then further hardened by background legal rules (including but not limited to the anti-circumvention provisions of the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act) that chill the provision and use of such tools. Companies limit the ability of consumers to interact with individuals using other services in a manner that substantially magnifies the benefit of network effects the company enjoys and further reduces the capacity of consumers to take the value they and their network add to a given service with them. Collectively, the lack of data portability and interoperability stifle innovation and competition on privacy as well as other terms in the current Web 2.0 marketplace.

Data portability and service interoperability must be touchstones of a privacy framework that relies, at any degree, on market competition to advance privacy. Regardless of what additional privacy regulatory constraints or requirements do these market conditions must be considered an integral component of the U.S. privacy framework.

Yet, even if such conditions exist, the difficulty consumers face in parsing and understanding an ever-growing list of privacy policies make privacy concerns difficult to act upon in today's marketplace. For that reason, efforts should be taken to revitalize the work begun at the World Wide Web Consortium in the Platform for Privacy Preferences initiative, and continued in activities such as the Internet Engineering Task Force Geopriv working group, to simplify the ability of companies to communicate privacy practices in simple standard formats and consumers through user agents and other automated

---

[2] Frederic Lardinois, "Mark Zuckerberg talks about new Facebook privacy controls (Live Blog)", May 26, 2010.
https://wave.google.com/wave/waveref/googlewave.com/w+w0tNX3NxA

tools to parse and act upon them. Meta-data about privacy practices is an important element of a competitive privacy environment. The U.S. privacy framework must consider not just the substance of privacy disclosures, but, similar to the ongoing work by the Administration to promote government transparency, it must concern itself with the form and format of such disclosures.

Through data portability, service interoperability, standardization and automation U.S. policy can advance privacy by reducing the transaction costs facing consumers seeking to understand and act upon privacy issues in the marketplace.

**Digital Due Process**

The Electronic Communications Privacy Act (ECPA), passed in 1986 and not significantly updated since, establishes standards for government access to email and other electronic communications in criminal investigations. It is very much a product of its time—reflecting both the technology and its specific use by businesses and consumers at the time of its enactment. While the law remains a critical and indispensable aspect of the U.S. privacy framework, it is mired in the technological past and therefore distorts the marketplace by drawing privacy-lines that pit innovation against privacy at nearly every turn. The law must be updated to provide consistent privacy protections in a technology-neutral manner that respects the growing dependency of individuals, companies, and the government on the internet for an increasing array of sensitive activities.

Specific aims of ECPA reform can be found in the comments of the Digital Due Process coalition, of which I am a member and comment signatory.

**Leveraging the existing benefits of the current U.S. legal framework**

I wish to draw the attention of the Department to a set of forthcoming articles by Kenneth Bamberger and me.[3] These articles present findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with Chief Privacy Officers identified by their peers as industry leaders and information from internal organizational charts, process documentation, and discussions with managers responsible for policy implementation.

In Privacy *on the Books and on the Ground*, we identify important regulatory elements neglected by the traditional story of privacy in the U.S.—the emergence of the Federal Trade Commission as a privacy regulator, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—and trace the ways in which these players and tools supplement a privacy debate largely focused on processes (such as notice and consent mechanisms) with a growing corporate emphasis on substance: preventing violations of consumers' expectations of privacy. This article reveals the importance of two alterations to the U.S. legal landscape that have been underappreciated in the literature and should be considered in the context of reforms to the U.S. and global privacy frameworks. First, the emergence of the FTC as a roving regulator with broad yet ambiguous power to evaluate privacy practices in the marketplace through its consumer protection lens. The FTC's mandate to protect consumers from "unfairness" and "deception" permits dynamic regulation that evolves with changing contexts, and forces corporate practices to develop accordingly. Second, state security breach notification laws raised the soft and hard costs of mismanaging personal information.

---

[3] Bamberger, Kenneth A. and Mulligan, Deirdre K., *Privacy on the Books and on the Ground*. Stanford Law Review, Vol. 63, 2010; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: http://ssrn.com/abstract=1568385; and Bamberger, Kenneth A. and Mulligan, Deirdre K., *Catalyzing Privacy*, (currently under submission with Law & Policy)

Together these changes have led companies to integrate substantive considerations of consumers' privacy expectations into their workflows, rather than leaving privacy to the lawyers and their process-based "click through if you 'consent' to the privacy policy" approach.

In *Catalyzing Privacy* we document specific shifts in corporate privacy management that have occurred during the period of regulatory shift described in *Privacy on the Ground*, including the increased power of corporate privacy leaders within the corporate and their external orientation, privacy reframed as a risk management function and integrated into mechanisms that relate to core firm values, and privacy's operationaliztion within the firm through distributed networks of dedicated privacy professionals and specially-trained employees within business units empowered with practices and tools that assist with identifying and addressing privacy during the design phase of business development.

These two articles provide several important insights for what we consider to be the "third wave" of privacy initiatives—tort laws being the first, data protection the second, and security breach notification and consumer protection analysis marking the beginning of the third—that should inform the process begun with this Inquiry.

Our account supports the argument that calls for federal regulation structured exclusively around fair information practice principles are ill-advised. Efforts to expand procedural mechanisms to empower individuals to control their personal information, must not eclipse robust substantive definitions of privacy and the protections they are beginning to produce, or constrain the regulatory flexibility that permits their evolution, for both have proved important tools in efforts to limit and police corporate over-reaching, curb consumer manipulation, and define and protect a shared expectation about the personal sphere in the marketplace. Within the corporation our interviewees indicated that Fair Information Practice Principles were insufficient to guide corporate behavior—particularly in times of profound technical or market change—and could unintentionally pigeonhole privacy as a purely legal matter. In contrast, it appears that the relationship between consumer protection and trust has allowed the CPOs against a dynamic external backdrop of engaed regulators, activists, academics and press, to transform internal perceptions about privacy from a compliance oriented, rule dominated, legal hurdle to be addressed at the end stage of product design, to a consultation and dialogue about how technical designs, business strategies, and policies can respect consumers' expectations and support trust in their companies. Relatedly, our interviewees echo the growing regulatory concern that absent a substantive touchstone, a data-protection regime can focus resources on developing a host of often meaningless consent processes, which must be designed and redesigned in an effort to do better—where the meaning of "better" is unclear and only partially tethered to individuals' expectations of privacy. Thus, any reform should foster the FTC's enforcement activities aimed at protecting consumers' reliance on conventional information flows because they have brought greater substance and meaning to an area routinely critiqued for its formalism. Viewing privacy as a context-dependent set of practices and expectations protects against corporate and bureaucratic desires to reduce it to a set of a priori process-oriented rules, and the legalization and regularization that critics and proponents alike claim plague data protection. And protecting existing social norms about information use, rather than leaving each individual to the mercy of the marketplace, is key to addressing both collective and individual interests.

Second, procedurally, our research identifies the important role of the forums provided by the FTC as sites for structuring and advancing a collective understanding of privacy among advocates, industry, academics and regulators. The collective engagement facilitated through these broad, inclusive stake-holder activities has yielded both substantively groundbreaking outcomes—a divergence from caveat emptor with respect to privacy disclosures—as well as unique changes in corporate privacy management. The FTC's combination of enforcement threats with its centrality in fostering a social network of entrepreneurial privacy advocates offers a model for avoiding both the shortcomings of static

top-down command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests. This model should guide the choice and design of whatever regulatory institutions take the lead on information privacy in the corporate sector moving forward. They must both possess and use regulatory tools that exploit market, corporate and advocacy capacity to develop collective understanding of risks and solutions to future privacy problems.

Finally, our articles begin to illuminate the ways in which corporate privacy professionals impart meaning and structure to societal privacy concerns within corporations. Debates about the establishment of a dedicated privacy agency in the United States emphasize the importance of governmental privacy expertise in shaping the rules governing corporate behavior. The U.S. may embrace a more formal institutional structure for privacy. And this would likely yield several important domestic and international benefits. However, whether the vision of a centralized privacy expertise within a free-standing or existing government agency is realized, it is important that regulators and civil society continue to leverage the broad, vibrant and entrepreneurial "cadre of specialists" on privacy that has developed in the private sector—within companies, advocacy organizations and academia. In the absence of a DPA staffed with data protection experts, and faced with increasing ambiguity as to what privacy requires, corporations depend on these new professionals to guide them through the challenges wrought by evolutions in technology and business practice. These professionals do not view themselves as compliance officers, but as norm entrepreneurs. Empowered by external threats that support their entrepreneurial efforts, they offer a unique capacity to embed privacy—as trust and consumer expectations—into the corporate psyche as well as business operations. Choices about regulatory form should be attentive to the important bridging role these insides play particularly as society becomes more pervasively networked, and privacy protection requires ongoing and on-the-ground attention to dynamic privacy interests that manifest in very different ways within different firms.

In conclusion, as the DOC continues this Inquiry and the broader domestic and international privacy community reflects upon the key global instruments of privacy and data protection, our research underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy can be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today's frameworks operate on the ground.

I look forward to engaging with DOC and other stakeholders on this important topic.

Sincerely,

Deirdre K. Mulligan

**UNITED STATES DEPARTMENT OF COMMERCE**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**

**In the Matter of**

***Information Privacy and Innovation in the Internet Economy*** **Docket No. 100402174-0175-01**

# COMMENTS OF DIGITAL DUE PROCESS

**June 14, 2010**

In response to the Notice of Inquiry in the above captioned matter, Digital Due Process is pleased to submit the following comments.

Digital Due Process (DDP) is a broad coalition of technology and communications companies, trade associations, advocacy groups, and think tanks, as well as academics and individual lawyers. A full, current list of DDP members appears at the end of this document. On March 30 of this year, DDP issued principles for updating the key federal law that defines the rules for government access to email and private files stored in the Internet "cloud." The coalition effort was prompted by the need to preserve traditional privacy rights in the face of technological change while also ensuring that law enforcement agents can carry out investigations and that industry has the clarity needed to innovate.

To set a consistent standard in line with the traditional rules for law enforcement access in the offline world, the group's recommendations focus on the Electronic Communications Privacy Act (ECPA). Passed in 1986 and not significantly updated since, it establishes standards for government access to email and other electronic communications in criminal investigations.

Technology has changed dramatically in the last 20 years, but the law has not. The traditional standard for the government to search one's home or office and read one's mail or seize one's personal papers is a judicial warrant. The law needs to be clear that the same standard applies to email and documents stored with a service provider, while at the same time be flexible enough to meet law enforcement needs.

The group is reaching out to government officials and anticipates extended dialogue with law enforcement agencies to develop consensus on updates to the law. We urge the Department to join in this process.

## ECPA Reform: Why Now?

The Electronic Communications Privacy Act (ECPA) was a forward-looking statute when enacted in 1986. It specified standards for law enforcement access to electronic communications and associated data, affording important privacy protections to

subscribers of emerging wireless and Internet technologies. Technology has advanced dramatically since 1986, and ECPA has been outpaced. The statute has not undergone a significant revision since it was enacted in 1986 – light years ago in Internet time.

As a result, ECPA is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies. ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected. Concern about the privacy afforded personal and business information can hold back adoption of emerging technologies, discouraging innovation. ECPA's complexity also imposes substantial costs on service providers seeking to review and comply with data requests from law enforcement. At the same time, ECPA must be flexible enough to allow law enforcement agencies and service providers to work together effectively to combat increasingly sophisticated cyber-criminals or sexual predators.

The time for an update to ECPA is now. For more than a year, privacy advocates, legal scholars, and major Internet and communications service providers have been engaged in a dialogue to explore how ECPA applies to new services and technologies. We have developed consensus around the notion of a core set of principles intended to simplify, clarify, and unify the ECPA standards; provide clearer privacy protections for subscribers taking into account changes in technology and usage patterns; and preserve the legal tools necessary for government agencies to enforce the laws and protect the public.

## The Economic Context for ECPA Reform

Since ECPA was adopted in 1986, the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity. According to the most recent Pew survey, an estimated 74% of Americans use the Internet.[1/] Information technology has driven the U.S. economy in the past two decades,[2/] and could, given the proper policy framework, support re-invigoration of the economy for years to come.[3/] The Internet and information technology could be especially important in job creation.[4]

---

1/ Pew Research Center, "Internet, broadband and cell phone statistics," (January 5, 2010) http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx. However, the fact that Internet usage has remained essentially static since 2006, *id.*, suggests that continued attention is needed to the policy framework supporting Internet expansion.

2/ *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

3/ *See id*. at 53 ("Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job

Cloud computing[5/] is a key element of technological innovation today. Businesses and individuals are now increasingly storing data "in the cloud," with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[6/] More than two-thirds of Internet users use some form of cloud computing service.[7] Cloud computing, "by altering the basic economics of access to computing and storage … has the potential to reshape how U.S. and global businesses are organized and operate."[8/] Most importantly, American tech companies are global leaders in the cloud computing industry today.

---

of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

[4] According to the Bureau of Labor Statistics, "Two of the fastest growing detailed occupations are in the computer specialist occupational group. Network systems and data communications analysts are projected to be the second-fastest-growing occupation in the economy. Demand for these workers will increase as organizations continue to upgrade their information technology capacity and incorporate the newest technologies. The growing reliance on wireless networks will result in a need for more network systems and data communications analysts as well. Computer applications software engineers also are expected to grow rapidly from 2008 to 2018. Expanding Internet technologies have spurred demand for these workers, who can develop Internet, intranet, and Web applications." *Occupational Outlook Handbook: 2010-2011 Edition, available at* http://www.bls.gov/oco/oco2003.htm.

[5/] At its most basic level, cloud computing involves the use of network servers. "Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams." Cloud Computing Definition, *available at* http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html.

[6/] As an example of the potential savings from cloud computing, the Obama Administration's Chief Information Officer, Vivek Kundra, "pointed to a revamping of the General Services Administration's USA.gov site. Using a traditional approach to add scalability and flexibility, he said, it would have taken six months and cost the government $2.5 million a year. But by turning to a cloud computing approach, the upgrade took just a day and cost $800,000 a year." Daniel Terdiman *White House Unveils Cloud Computing Initiative*, cnet News, Sept. 15, 2009, *available at* http://news.cnet.com/8301-13772_3-10353479-52.html

[7] *Use of Cloud Computing Applications and Services*, Pew Internet & American Life Project, Sep. 12, 2008, Pg. 4, available at http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

[8/] Jeffrey Rayport & Andrew Heyward, Andrew: *Envisioning the Cloud: the Next Computing Paradigm* (Mar. 20, 2009). According to the authors, cloud computing will lower capital requirements for technology start-ups, permit businesses to manage IT resources without tying up capital in IT capacity, while managing energy resources more efficiently; facilitate consumer access to an endless array of powerful applications at low cost; support innovation by reducing the human investment needed to build and maintain IT infrastructure; and foster cooperation and collaboration, without the coordination costs typically associated with bringing

The issue of privacy is important to the users of cloud computing. A 2008 study found that 64 percent of American Internet users are concerned about cloud computing companies turning over their files to law enforcement.[9] A survey completed just last week found that a large majority of Americans (88%) believe consumers should enjoy legal privacy protections online similar to those they have offline, while only 4% disagree.[10] Moreover, cloud computing experts warn that potential clients are seeking data storage centers outside the U.S. due to concerns that our laws give the government access to huge quantities of information with little judicial oversight.[11] If this trend continues, American workers may miss out on the jobs that would accompany the growth of this industry.

The use of location information is another trend creating major market opportunities for U.S. companies. There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[12/] More applications such as these are emerging every day. A 2010 study forecast that revenues from mobile location-based services could grow to more than $12.7 billion by 2014.[13] However, uncertainty about the privacy afforded location information can hold back consumer use of this technology.[14]

---

people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

[9] Id., at p. 7.

[10] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010) http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. According to the survey, the large majority (79%) believes law enforcement should have to get a warrant, like the one they have to get to wiretap phone conversations, to track where a user goes on the Internet, while 12% do not.

[11] Jeffery Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, Marketspace, Mar. 20, 2009, p. 38, available at http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

[12/] *See* Educause Learning Initiative, *7 Things You Should Know About … Location Aware Applications*, *available at* http://net.educause.edu/ir/library/pdf/ELI7047.pdf.

[13] Robin Wauters, *Mobile Location-Based Services Could Rake in $12.7 Billion by 2014: Report*, TechCrunch, Feb. 23, 2010, http://techcrunch.com/2010/02/23/location-based-services-revenue.

[14] Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (Feb. 2010), p. 18, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

## Changes in Technology Have Outpaced the Law

Justice Brandeis famously called privacy "the most comprehensive of rights, and the right most valued by a free people." Of course, privacy must be balanced against other societal interests. Electronic communications and associated data can provide key evidence in the investigation of many crimes, and the assistance of service providers is often necessary to access such evidence. With respect to communications privacy and law enforcement investigations, the courts and Congress have sought to develop rules for government surveillance that balance three interests: the individual's constitutional right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust.

A primary reason that Congress adopted ECPA in 1986 was to provide sound footing for investment and innovation. In 1986, the fledgling wireless and Internet industries wanted to be able to assure potential customers that their communications were private. Congress recognized that consumers would not trust new technologies if the privacy of those using them was not protected. In the quarter century since the enactment of ECPA, there have been fundamental changes in communications technology and the way people use it, including –

- **Email**: Most Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Because of the importance of email and unlimited storage capabilities available today, most people save their email indefinitely, just as they previously saved letters and other correspondence. The difference, of course, is that it is easier to save, search and retrieve digital communications. Many of us now have many years worth of stored email. Moreover, for many people, much of that email is stored on the computers of service providers.
- **Mobile location:** Cell phones and mobile Internet devices constantly generate location data that supports both the underlying service and a growing range of location-based services of great convenience and value. This location data can be intercepted in real-time, and is often stored in easily accessible logs files. Location data can reveal a person's movements, from which inferences can be drawn about activities and associations. Location data is augmented by very precise GPS data being installed in a growing number of devices.
- **Cloud computing**: Increasingly, businesses and individuals are storing data "in the cloud," with potentially huge benefits in terms of cost, security, flexibility and the ability to share and collaborate.
- **Social networking:** One of the most striking developments of the past few years has been the remarkable growth of social networking. Hundreds of millions of people now use these social media services to share information with friends and as an alternative platform for private communications.

In the face of these developments, ECPA does not provide protection suited to the way technology is used today:

- **Conflicting standards and illogical distinctions:** ECPA sets rules for

governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.

- **Unclear standards:** ECPA does not clearly state the standard for governmental access to location information.
- **Judicial criticism:** The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law." In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.
- **Constitutional uncertainty:** The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.

This murky legal landscape does not serve the government, customers or service providers well. Customers are, at best, confused about the security of their data in response to an access request from law enforcement. Companies are uncertain of their responsibilities and unable to assure their customers that subscriber data will be uniformly protected. The current state of the law does not well serve law enforcement interests either as resources are wasted on litigation over applicable standards, and prosecutions are in jeopardy should the courts ultimately rule on the Constitutional questions.

The solution is a clear set of rules for law enforcement access that will safeguard end-user privacy, provide clarity for service providers, and enable law enforcement officials to conduct effective and efficient investigations.

## Guiding Principles for ECPA Reform

The overarching goal of our review of the ECPA was to balance the law enforcement interests of the government, the privacy interests of users, and the interests of communications service providers in certainty, efficiency and public confidence.

We were guided by the following concepts:

- **Technology and Platform Neutrality**: A particular kind of information (for example, the content of private communications) should receive the same level of protection regardless of the technology, platform or business model used to

create, communicate or store it.

- **Assurance of Law Enforcement Access**: The reform principles would preserve all of the building blocks of criminal investigations – subpoenas, court orders, pen register orders, trap and trace orders, and warrants – as well as the sliding scale that allows the government to escalate its investigative efforts.
- **Equality Between Transit and Storage**: Generally, a particular category of information should be afforded the same level of protection whether it is in transit or in storage.
- **Consistency**: The content of communications should be protected by a court order based on probable cause, regardless of how old the communication is and whether it has been "opened" or not.
- **Simplicity and Clarity**: All stakeholders – service providers, users and government investigators – deserve clear and simple rules.
- **Recognition of All Existing Exceptions**: Over the years, a variety of exceptions have been written into the ECPA, such as provisions allowing disclosures to the government without court orders in emergency cases. These principles should leave all those exceptions in place.

Rather than attempt a full rewrite of ECPA, which might have unintended consequences, we focused on just a handful of the most important issues – those that are arising daily under the current law: access to email and other private communications stored in the cloud, access to location information, and the use of subpoenas to obtain transactional data.

Our principles do not seek to answer all questions or concerns about ECPA. Though members of the coalition may differ on the specifics, and some individual members would support additional changes, we all agree that these principles provide a framework for opening a public dialogue on the issue.

## Specific Background on ECPA Reform Principles

### 1. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.

- This principle applies the safeguards that the law has traditionally provided for the privacy of our phone calls or the physical files we store in our homes to private communications, documents and other private user content stored in or transmitted through the Internet "cloud"-- private emails, instant messages, text messages, word processing documents and spreadsheets, photos, Internet search queries and private posts made over social networks.

- This change was first proposed in bi-partisan legislation introduced in 1998 by Senators John Ashcroft and Patrick Leahy. It is consistent with recent appeals court decisions holding that emails and SMS text messages stored by

communications providers are protected by the Fourth Amendment, and is also consistent with the latest legal scholarship on the issue.

**2. The government should obtain a search warrant based on probable cause before it can track, prospectively or retrospectively, the location of a cell phone or other mobile communications device.**

- This principle addresses the treatment of the growing quantity and quality of data based on the location of cell phones, laptops and other mobile devices, which is currently the subject of conflicting court decisions; it proposes the conclusion reached by a majority of the courts that a search warrant is required for real-time cell phone tracking, and would apply the same standard to access to stored location data.

- A warrant for mobile location information was first proposed in 1998 as part of the bipartisan Ashcroft-Leahy bill. It was approved 20 to 1 by the House Judiciary Committee in 2000.

**3. Before obtaining transactional data in real-time about when and with whom an individual communicates using email, instant messaging, text messaging, the telephone or any other communications technology, the government should demonstrate to a court that such data is relevant to an authorized criminal investigation.**

- In 2001, the law governing "pen registers and trap & trace devices"—technologies used to obtain transactional data in real-time about when and with whom individuals communicate over the phone—was expanded to also allow monitoring of communications made over the Internet. In particular, the data at issue includes information on who individuals email with, who individuals IM with, who individuals send text messages to, and the Internet Protocol addresses of the Internet sites individuals visit.

- This principle would update the law to reflect modern technology by establishing judicial review of surveillance requests for this data based on a factual showing of reasonable grounds to believe that the information sought is relevant to a crime being investigated.

**4. Before obtaining transactional data about multiple unidentified users of communications or other online services when trying to track down a suspect, the government should first demonstrate to a court that the data is needed for its criminal investigation.**

- This principle addresses the circumstance when the government uses subpoenas to get information in bulk about broad categories of telephone or Internet users, rather than seeking the records of specific individuals that are relevant to an investigation. For example, there have been reported cases of bulk requests for information about everyone that visited a particular web site on a particular day, or everyone that used the Internet to sell products in a particular jurisdiction.

- Because such bulk requests for information on classes of unidentified individuals implicate unique privacy interests, this principle applies a standard requiring a showing to the court that the bulk data is relevant to an investigation.

Members of Digital Due Process:

AOL
AT&T
Data Foundry
eBay
Google
Integra Telecom
Intel
Loopt
Microsoft
Qwest
Salesforce.com
TRUSTe

American Booksellers Foundation for Free Expression
American Civil Liberties Union
American Library Association
Association of Research Libraries
Americans for Tax Reform
Bill of Rights Defense Committee
Center for Democracy & Technology
Center for Financial Privacy and Human Rights
Citizens Against Government Waste
Competitive Enterprise Institute
Computer & Communications Industry Association
The Constitution Project
Consumer Action
Distributed Computing Industry Association
Electronic Frontier Foundation
FreedomWorks
Information Technology and Innovation Foundation
NetCoalition
The Progress & Freedom Foundation

Individuals:

Patricia Bellia, Notre Dame Law School
David Berger, Wilson, Sonsini Goodrich & Rosati
Michael Carroll, American University, Washington School of Law
Fred Cate, Indiana University Law School
Danielle Keats Citron, University of Maryland School of Law
Ralph D. Clifford, University of Massachusetts School of Law
Susan Crawford, University of Michigan Law School
Susan Freiwald, University of San Francisco Law School

James Grimmelmann, New York Law School
Eric Goldman, Santa Clara University School of Law
Robert A. Heverly, Michigan State University College of Law
Dan Hunter, New York Law School and The Wharton School, University of Pennsylvania
Charles H. Kennedy, Wilkinson Barker Knauer, LLP
Liza Barry-Kessler, Privacy Counsel LLC
Mark A. Lemley, Stanford Law School
Jennifer Lynch, UC Berkeley Law School
Rebecca MacKinnon, Center for Information Technology Policy, Princeton University
Anthony Martin, Husch Blackwell Sanders LLP
Deirdre Mulligan, UC Berkeley iSchool
Paul Ohm, Professor of Law, University of Colorado
Scott Parsons, Portland State University
Frank A. Pasquale, Seton Hall Law School
David G. Post, Beasley School of Law, Temple University
Ira Rubinstein, New York University School of Law
Pam Samuelson, UC Berkeley Law School and iSchool
Katherine J. Strandburg, New York University School of Law
Jennifer Urban, UC Berkeley Law School
Michael Zimmer, School of Information Studies, University of Wisconsin-Milwaukee
Marc Zwillinger, Zwillinger Genetski LLP

For further information, contact:

James X. Dempsey
jdempsey@cdt.org
202-365-8026


**Before the**
**DEPARTMENT OF COMMERCE**
**Washington, DC 20230**

# COMMENTS
# of the
# DIRECT MARKETING ASSOCIATION, INC.

**Responding to the Notice of Inquiry**
**on "Information Privacy and Innovation in the Internet Economy"**

**Docket No. 100402174-0175-01**

**June 14, 2010**

Linda Woolley
Executive Vice President, Government Affairs
Gerald Cerasale
Senior Vice President, Government Affairs
Direct Marketing Association, Inc.
1615 L Street, NW Suite 1100
Washington, DC 20036
(202) 861-2444

Counsel:
Stuart Ingis
Emilio Cividanes
Julia Kernochan Tama
Venable LLP
575 Seventh Street, NW
Washington, DC 20004
(202) 344-4613

**Direct Marketing Association, Inc.**

**Comments on "Information Privacy and Innovation in the Internet Economy"**

**Docket No. 100402174-0175-01**

The Direct Marketing Association ("DMA") commends the Department of Commerce for launching its Privacy and Innovation Initiative and applauds the Department's commitment to ensuring that the Internet remains "open for innovation."[1] The DMA appreciates the opportunity to submit these Comments in response to the Department of Commerce's Notice of Inquiry on "Information Privacy and Innovation in the Internet Economy" (the "NOI").[2]

The DMA (www.the-dma.org) is the leading global trade association of businesses and nonprofit organizations using and supporting multichannel direct marketing tools and techniques. The DMA advocates industry standards for responsible marketing; promotes relevance as the key to reaching consumers with desirable offers; and provides cutting-edge research, education, and networking opportunities to improve results throughout the end-to-end direct marketing process. Founded in 1917, the DMA today represents thousands of companies from dozens of vertical industries in the United States and 50 other nations, including a majority of the Fortune 100 companies, as well as nonprofit organizations. Included are cataloguers, financial services, book and magazine publishers, retail stores, industrial manufacturers, Internet-based businesses, and a host of other segments, as well as the service industries that support them.

In the first two sections of these Comments, the DMA presents its general view that the current U.S. approach to privacy regulation has effectively fostered innovation and preserved consumer choice and explains why the DMA believes that industry self-regulation is the best approach to refining and enforcing privacy protections, especially in the marketing arena. The third and final section of the Comments responds to selected questions posed in the NOI.

## I. The U.S. Approach to Privacy Regulation Has Effectively Fostered Innovation and Preserved Consumer Choice

As the NOI recognizes, the Internet is no longer a distinct industry, but penetrates every area of Americans' business and private lives. The DMA's member companies grapple each day with the business and ethical consequences of this expansion and the attendant technological innovation. The DMA does not believe that this rapid pace of change heralds a need for new regulation. On the contrary, today's vibrant Internet ecosystem results from, and demonstrates the need to retain, the existing U.S. approach to

[1] 75 Fed. Reg. 21226 (April 23, 2010).
[2] *Id.*

privacy regulation, which has allowed innovation to flourish while preserving consumer choice.

The United States was the birthplace of the Internet and remains the global leader in online technological innovation. As the Internet became available to consumers in the late 1990s, the Department of Commerce, Federal Trade Commission, other regulatory bodies, and Congress assessed the need to regulate the new medium. This consideration weighed the harms and benefits of information use. The result was a broad consensus in favor of avoiding heavy-handed regulation in order to foster technological innovation and economic growth.

With this balance in mind, U.S. privacy regulation is founded on several core principles known as "fair information practices," which are designed to ensure that consumers can exercise meaningful control over their private information while allowing beneficial information use to continue. As summarized by the Federal Trade Commission in a report to Congress, these principles are:

1. Notice/awareness,
2. Choice/consent,
3. Access/participation,
4. Integrity/security, and
5. Enforcement/redress.[3]

Over the decades, the fair information practices have been proven to be a flexible and adaptable framework that preserves consumer choice while promoting innovation and economic growth and allowing beneficial uses of information to continue.

In keeping with this balanced approach, Congress has largely followed a "sectoral" framework in U.S. privacy legislation. Federal privacy statutes that apply to businesses typically address particular areas of concern, such as children's online privacy, or specific sectors perceived as handling sensitive information, such as the financial industry or health care entities. The Department of Commerce notes this pattern in the NOI and requests input on how it affects businesses.[4] The DMA believes that compelling policy reasons support this reluctance to regulate business privacy practices more broadly. It would not be feasible or prudent to impose a "one size fits all" set of standards across the economy, given the wide variation in different industries' information collection and uses. Data practices are complex, and the sectoral framework allows Congress to devise tailored responses to specific areas of concern. In addition, sweeping legislation is not necessary given that self-regulation and other existing tools continue to be effective in preserving the fair information principles.

---

[3] Federal Trade Commission, "Fair Information Practice Principles," in *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 9, 2010).

[4] 75 Fed. Reg. at 21230.

Further, the online advertising business is a highly dynamic market characterized by rapid technological change. In this environment, regulation that is specific to a technology or business model could deter entry, thwart innovation, and limit competition in the sale of online advertising. Fewer choices for online ad sales could exacerbate the already significant financial pressure on advertiser-supported media. No company can succeed in today's highly competitive marketplace unless it wins and retains the trust of its customers. Rather than impose disparate regulation, the government should promote industry self-regulatory approaches that protect privacy while promoting competition among technologies and business models.

Against this regulatory backdrop, the rise of the Internet has led to an explosion of innovation that has transformed every aspect of our lives, generating advances ranging from more efficient business communications to unprecedented forms of digital entertainment. Advertising has provided critical support for this development across business models and technologies. As noted in the NOI, online commerce is thriving and increasing, even during the current economic downturn. This e-commerce is spurred by online advertising and marketing. In addition to turning to the Internet for its e-commerce resources, consumers have come to expect rich online content and services at little or no cost to the consumer.

The wide availability of these benefits is subsidized by online advertising revenues. Market innovators also rely on advertising revenues to create and implement new products and services. Online advertising can be targeted based on context (the content of a website or webpage) or on the browsing history associated with a particular computer. Conducted responsibly, this type of collaboration does not jeopardize consumer privacy. It relies largely on anonymous data that is not linked back to a named individual, much of which may be discarded after a single online session. Although not all online advertising is targeted, the ability to make advertising more relevant to consumers' likely needs and interests is a benefit to consumers, and also allows advertising efficiently to subsidize other activities.

The DMA believes that the benefits of data collection, sharing and use for advertising and marketing purposes far outweigh any risks to consumers. In general, marketing causes no identifiable harm to consumers. Marketing allows consumers to receive information about commercial opportunities that they may value, and consumers are free to respond (or not) as they see fit. If a consumer does not value a particular message, the consumer will simply ignore it. Moreover, marketing carries societal benefits as a facilitator of economic growth, and is a form of constitutionally protected speech. While the DMA recognizes that certain data practices do raise specialized policy concerns, the DMA strongly believes that these concerns should be addressed on a case-by-case basis and in dialogue with industry, while allowing most advertising and marketing uses of data to continue unhindered. The DMA believes that marketing data should only be used for marketing purposes. The DMA further believes that regulation should not be specific to a technology or business model, which would impede both competition and innovation.

While there are those who may claim that privacy concerns affect online usage, this argument is discredited by American consumers' evident enthusiasm for Internet technologies and the resultant growth in online economic activity. American consumers are avid users of the Internet, and are quickly embracing emerging technologies like cloud computing, mobile computing, and social networking. Consumers' embrace of e-commerce shows that they widely value the convenience, customization, and features that companies can offer online. It is evident that the prevailing U.S. approach to privacy regulation strikes an appropriate balance that benefits consumers and industry alike.

The DMA cautions against new legislation, regulation, or policies that could disrupt this beneficial cycle. Unnecessary restrictions on online advertising could reduce the relevance of commercial messages to consumers. If online advertising becomes less effective, it will impede companies' ability to provide ad-supported content and services to the public. This could hinder innovation or e-commerce, or drive businesses to shift from offering free content and services to demanding direct payments from consumers. Similarly, any restrictions on data used to power commercial messages could cause consumer confusion and undermine the very consumer trust that has enabled Internet commerce to thrive. Given the penetration of the Internet into all areas of business, it is important to note that regulation of the online ecosystem amounts to regulation across industries. Shifts in U.S. policies toward the Internet would likely have economic "ripple effects" that are difficult to predict. This type of instability is to be avoided at any time, but especially when the economy is fragile.

The DMA also believes that the Federal Trade Commission ("FTC"), as the primary federal enforcement agency in this arena, has long made an appropriate choice to focus its enforcement resources on practices that cause demonstrable harms to consumers, such as physical harms, economic injuries, or unwarranted intrusions such as spam and spyware.[5] This approach allows the Commission to identify and target discrete practices that warrant enhanced privacy measures, as it has done with online behavioral advertising, while generally allowing innovation to thrive. This "harm-based" focus is consistent with the approach that the United States, often represented by the FTC, has taken in the development of the Information Privacy Principles of the Asia-Pacific Economic Cooperation ("APEC") economies.[6] The DMA also believes that the harm-based philosophy respects the individualized nature of privacy preferences and correctly recognizes that tangible harm to consumers is the most meaningful and objective yardstick to determine whether regulation or enforcement is needed. In addition, the harm-based approach tends not to favor or disadvantage a particular business model, since it zeros in on a specific, objectionable practice, which is most appropriate.

[5] David Vladeck, Remarks on "The Role of the FTC in Consumer Privacy Protection" before the International Association of Privacy Professionals, Washington, DC (December 8, 2009).
[6] The "Preventing Harm Principle" is the first principle of the APEC Privacy Framework. APEC Secretariat, *APEC Privacy Framework* 11 (2005).

## II. Self-Regulation Is the Best Approach to Refining and Enforcing Privacy Protection in the Marketing Arena

### *A. Benefits of Self-Regulation*

The NOI requests comments about the state of efforts to develop self-regulation in the privacy arena.[7] The DMA strongly believes that industry self-regulation based on the fair information practices is the best approach to online privacy protection, especially in the realm of marketing and advertising. Self-regulation is flexible enough to respond quickly to changes in the market and in business operations, ensuring that rules do not become outdated or stymie innovation.

Self-regulatory programs such as the DMA's provide meaningful controls and accountability. DMA member companies have a major stake in the success of e-commerce and Internet marketing. They understand that their businesses depend on consumers' continued confidence in the online medium, and they support efforts that enrich a user's experience while fostering consumer trust in online channels. Compliance with the DMA's comprehensive *Guidelines for Ethical Business Practice* (the "Guidelines") is required for all DMA members.[8] The DMA can and does take action to enforce compliance, including by referring matters to enforcement authorities. In addition, companies that represent to the public that they are DMA members but fail to comply with the Guidelines may be liable for deceptive advertising under federal or state laws.

Specifically, the self-regulatory approach is the most efficient and effective way to respond to privacy issues related to marketing and advertising. Advertising provides great benefits to consumers by making them aware of products, services, and offers that may interest them. Receiving such messages does not harm consumers in any conceivable way, because unwanted messages can easily be ignored. Data collection and uses in support of advertising have raised some privacy questions, but the DMA believes that these questions are being adequately addressed through self-regulation and submits that self-regulation generally remains the most appropriate method for industry to improve marketing practices with input from government authorities.

The DMA acknowledges that steps beyond self-regulation may be appropriate where a specific practice is found to cause identifiable and concrete harm to consumers. When warranted, such practices should be addressed on a case-by-case basis to avoid unnecessarily disrupting the entire online ecosystem.

---

[7] 75 Fed. Reg. at 21229.

[8] Direct Marketing Association Guidelines for Ethical Business Practice, *available at* http://www.dmaresponsibility.org/Guidelines/.

### *B. DMA Guidelines for Ethical Business Practice*

The effectiveness of self-regulation is demonstrated by the DMA's lengthy history of leadership in establishing effective and thorough industry self-regulatory standards. The DMA and its members have developed standards for online data practices and many other business activities as part of our Guidelines. We have repeatedly updated our Guidelines, most recently in January 2010, to take account of new technologies and concerns. Among other requirements under the current Guidelines, companies should:

- Not display, disclose, rent, sell or exchange data and selection criteria that may reasonably be considered sensitive or intimate, where there is a reasonable consumer expectation that the information will be kept confidential;[9]

- Not transfer personally identifiable health-related data gained in a medical treatment context for marketing purposes without the specific prior consent of the consumers;[10]

- Treat personally identifiable health-related information volunteered by or inferred about consumers outside a treatment context as sensitive and personal information, and provide clear notice and the opportunity to opt out and take the information's sensitivity into account in making any solicitations;[11]

- Not rent, sell, exchange, transfer, or use marketing lists in violation of the Guidelines;[12]

- Provide notice of online information practices, including marketing practices, in a way that is prominent and easy to find, read, and understand, and that allows visitors to comprehend the scope of the notice and how they can exercise their choices regarding use of information;[13]

- Identify and provide contact information for the entity responsible for a website;[14]

- Comply with the new self-regulatory principles for online behavioral advertising, discussed below;[15]

---

[9] Guidelines, Article 32.
[10] Guidelines, Article 33.
[11] *Id.*
[12] Guidelines, Article 35.
[13] Guidelines, Article 38.
[14] *Id.*
[15] *Id.*

- Assume certain responsibilities to provide secure transactions for consumers and to protect databases containing consumers' personally identifiable information against unauthorized access, alteration, or dissemination of data;[16]

- Restrict data collection and marketing for children online or via wireless devices, consistent with the Children's Online Privacy Protection Rule;[17] and

- Follow specific rules for data compilers, including suppressing a consumer's information from their databases upon request, explaining the nature and types of their sources to consumers upon request, reviewing customer companies' use of data and requiring customers to state the purpose of their data use, and reviewing promotional materials used in connection with sensitive marketing data.[18]

These examples are only a sample of the restrictions contained in the Guidelines, which provide DMA member companies with a comprehensive blueprint for ethical marketing practices.

Most recently, the DMA worked with a coalition of other leading trade associations and companies to develop Self-Regulatory Principles for Online Behavioral Advertising ("Self Regulatory Principles"), released in July 2009.[19] These principles require advertisers and websites to inform consumers about data collection practices and enable them to exercise control over that information. The Self-Regulatory Principles define "online behavioral advertising" as the "collection of data from a particular computer or device regarding Web viewing behaviors over time and across non-affiliate websites for the purpose of using such data to predict user preferences or interests to delivery of advertising to that computer or device based on the preferences or interests inferred from such web viewing behaviors."[20] The Principles call on companies to:

- Provide enhanced notice outside of the company's privacy policy on any web pages where data is collected or used for online behavioral advertising purpose;

- Provide choice mechanisms that will enable users of websites at which data is collected for online behavioral advertising purposes the ability to choose whether data is collected and used or transferred to a non-affiliate for such purposes;

- Provide reasonable security for, and limited retention of, data collected and used for online behavioral advertising purposes;

---

[16] Guidelines, Article 37.
[17] Guidelines, Article 16.
[18] Guidelines, Article 36.
[19] Self-Regulatory Principles for Online Behavioral Advertising, *available at* http://www.iab.net/media/file/ven-principles-07-01-09.pdf (last visited May 13, 2010).
[20] Self-Regulatory Principles, at 2.

- Obtain consent before applying any material change to their online behavioral advertising data collection and use prior to such material change; and

- Provide heightened protection for certain sensitive data.

The Principles have been incorporated into the DMA Guidelines and are now binding on all DMA member companies. The DMA encourages the Department of Commerce and other federal agencies to recognize and promote industry self-regulation, such as the DMA Guidelines, that benefits consumers by protecting privacy without hindering competition.

## III. Responses to Selected Questions Posed in the NOI

### *A. Notice and Choice Should Remain the Foundation of U.S. Privacy Regulation*

#### *1. The Notice and Choice Model, Including the Development of Specialized Notice Mechanisms When Appropriate, Remains the Best Way to Balance Innovation and Privacy*

The NOI states that the Department of Commerce has heard from certain stakeholders that "the customary notice an choice approach to consumer protection may be outdated[.]"[21] The DMA disagrees with this view. Furthermore, the DMA does not believe that it would be appropriate or productive for data managers to adopt "use-based" rules across all data flows that would regulate all types of uses and purposes for which personal information may be employed. Defining appropriate uses may make sense in some instances such as health or financial data but not in others. Overly broad use restrictions could limit innovation and the development of new business models.

As discussed above, notice and choice, implemented in conjunction with the other fair information principles, have been effective for decades in allowing innovation to flourish while preserving consumer control over their information. Switching to a different regime would abandon this proven model and could constrain important business practices. The notice and choice model is already designed to provide consumers with the information and tools to enforce their individual privacy preferences. A privacy commitment in the form of a privacy notice can also be used by self-regulatory enforcement, law enforcement, consumers, and consumer advocates to ensure businesses are living up to their commitments.

While there may be certain situations where additional use restrictions are appropriate, rather than abandoning the notice and choice model in favor of an untested alternative, the DMA believes that the focus should be on improving how information is presented to consumers and developing new tools to assist consumers in making more

[21] 75 Fed. Reg. 21226, 21229 (April 23, 2010).

informed choices. The DMA suggests that further guidance from regulators on how privacy policies can be made more friendly to consumers would be welcome. To date, federal regulators have provided little concrete guidance on how website policies could be improved. In order to encourage adoption of such guidance, it would also be helpful to provide a safe harbor mechanism so that companies that follow such guidance are shielded from liability. The recent efforts of a group of agencies in issuing a new model privacy notice for financial information, based on consumer testing, provide a useful model for such an undertaking.

However, efforts to improve notice mechanisms should recognize that the percentage of consumers that read or take action on privacy policies is not a valid measure of whether policies are adequate or the notice and choice model is working. Consumers are generally busy, have many priorities, and likely see no need to consult a policy – no matter how accessible or readable – unless they have specific concerns. The fair information practices invite the consumer to play a role in his own protection, but the consumer is free to decline this invitation. Declining to read a privacy policy is not evidence of a policy failure, but a preference which should be respected to the same extent as a choice to be actively concerned about privacy.

The DMA recognizes that there are certain practices for which a traditional privacy policy does not provide sufficient transparency. One example of an innovative notice and choice mechanism is the DMA's online tool, www.dmachoice.org, for consumers to set individualized preferences about what marketing communications they wish to receive. This centralized tool is an effective way for consumers to make meaningful choices about marketing uses of their personal information.

The DMA has also found that self-regulation in dialogue with federal regulators can provide an effective forum to develop specialized policies to address practices for which a traditional privacy policy may not be sufficient. As online operations become increasingly complex, such case-by-case policy responses can ensure that consumers are receiving adequate notice to make a meaningful choice about whether to use a website or service. For example, the Federal Trade Commission recently drew industry's attention to the unique considerations raised by online behavioral advertising. When third parties contribute to advertising operations, their data practices may not be included in the website privacy policy where a consumer would most likely seek such information. Thus, the Commission recognized a need for a specialized policy response.

In response to the Commission's call for action, "enhanced notice" to consumers is a key part of the Self-Regulatory Principles for Online Behavioral Advertising. Participating advertisers will present a consistent and recognizable logo in close proximity to every behaviorally-targeted online advertisement. Consumers may click this logo for more information about why they received the advertisement and directions on how to opt out of targeted messages. This innovative solution will ensure that consumers can easily receive notice of the data practices of third parties. As technology evolves, regulators may identify additional situations where the unique transparency and choice

solutions are appropriate. In such situations, the DMA expects that dialogue between regulators and industry will be effective to devise an appropriate and tailored response.

*2. Opt-In Consent Is Not the Solution*

The DMA notes that consumer "choice" has been construed in most contexts to require allowing consumers an opportunity to opt out of unwanted practices. This approach allows beneficial data flows to proceed unless an individual expresses a contrary preference. However, there has been some recent public debate about whether opt-in consent for data collection, use, and/or disclosures should be required in various settings. The DMA is concerned that opt-in consent, even on a limited scale, would drastically alter the online experience as we know it. Given the collaborative architecture of the Internet, data-sharing interactions between website owners and other companies are commonly required for the orderly functioning of a website. These interactions are currently seamless, and facilitate website features and efficiencies that consumers value. A requirement for opt-in consent creates a presumption against the free flow of data and will disrupt this existing online architecture. Ultimately, such new restrictions would undermine consumer enjoyment of the Internet, which is the foundation of online commerce.

There is no indication that legitimate data flows harm consumers or should be discouraged. In particular, the DMA is not aware of any evidence of concrete harm to consumers from the legitimate data practices that support online advertising. The DMA also is not aware that a societal consensus against data transfers has been identified, or that researchers have shown that consumers would be willing to accept a changed Internet experience in exchange for reducing such transfers. In the absence of such convincing evidence, the DMA believes that it would be detrimental to innovation and consumer welfare to introduce new requirements related to opt-in consumer consent. Indeed, it is likely that constant appearances of notice boxes will annoy and frustrate consumers, and will dilute the impact of such mechanisms. To the extent that the debate regarding opt-in consent is related to concerns about the sufficiency of disclosures about data practices to enable consumers to make more informed decisions, the DMA submits that such a concern would be better addressed by focusing on methods to improve the provision of notice.

***B. Privacy-Enhancing Technologies***

The NOI seeks "input on the development, use and acceptance of privacy-related technologies and business processes and their potential to enhance consumer trust in Internet commerce."[22] DMA believes that privacy-enhancing technologies and the "privacy by design" philosophy should be core tools in the effort to promote innovation while preserving consumer control. Privacy-enhancing technologies promote consumer control by harnessing innovation and competition rather than stifling them. DMA

[22] 75 Fed. Reg. at 21230-21231.

strongly encourages the Department of Commerce to explore how the government can support businesses in developing new products and technologies that can address policy challenges without the need for regulation. Companies have a natural incentive to develop privacy-enhancing technologies that address issues that concern consumers, and consumers will provide a market for tools that are effective and meet their needs. Where these incentives are not quite strong enough, government can spur the development or adoption of such tools through steps like establishing safe harbors, extending official recognition to effective tools, or purchasing effective technologies for use by government employees or agencies.

The DMA believes that privacy-enhancing technologies will also be effective in addressing concerns about online data collection and use. Leading Internet browsers have already developed and deployed privacy controls that allow consumers to make detailed choices about whether and what information is tracked or saved as those consumers navigate the Internet. It is probable that increasing numbers of consumers will use browser controls as awareness and functionality increase. Browser controls allow consumers with privacy concerns to exercise control over their information in a way that does not disrupt the underlying Internet architecture. The DMA expects that browser controls and similar market-driven tools can effectively safeguard consumers' online privacy, and recommends that these promising tools should be given more opportunity to flourish before government agencies embark on any new regulation in the area of online behavioral advertising. DMA self-regulation in this area and the "PCI" standards that govern sensitive information have proven useful towards protecting data.

The NOI specifically requests comment on the concept of developing "trusted identity providers" to assist consumers in managing their data.[23] The DMA suggests that the best way to encourage the development of such providers is through the operation of the marketplace. Any new government mandate would be likely to disrupt the natural pace and direction of technological innovation by business.

### *C. Consumer Expectations and Education*

The NOI asks whether the focus of privacy laws and regulations should be on satisfying subjective consumer expectations or on enacting objective principles.[24] As a general matter, the DMA does not believe that U.S. privacy policy should be based on subjective consumer expectations. Consumers' privacy expectations and preferences are nuanced, highly individualized, and constantly changing in response to new technologies. Given the intricacy of today's technology, consumers also may not be in the best position to understand or assess the benefits and risks of a particular data practice. It is therefore practically impossible to measure such expectations with any level of reliability or to translate them into useful policy judgments. Any attempt to set broad standards by identifying an "average" consumer view will likely hinder technological development

[23] 75 Fed. Reg. at 21231.
[24] 75 Fed. Reg. at 21229.

that other consumers may find valuable. Further, it would cause great economic harm and thwart innovation to set standards based on the "eggshell" consumer, which is the essence of many proposals put forward by advocates. This inability to measure or generalize consumer expectations supports the DMA's view that consumer notice and choice remain the most simple, elegant, and effective solution for managing privacy concerns, especially in the rapidly evolving online world.

However, the DMA believes that consumer education is an essential and effective means to encourage consumers to exercise their privacy choices. In particular, consumer education can be valuable in advancing both the development and the adoption of privacy enhancing technologies. As consumers learn more about existing technologies and adopt them in greater numbers, this market incentive will naturally spur additional technological development, establishing a virtuous cycle that expands the range and usefulness of consumer offerings. Consumer education is an important facet of the DMA's efforts to implement the Self-Regulatory Principles for Online Behavioral Advertising. The DMA also encourages government bodies to engage in consumer education efforts to promote privacy awareness and the use of privacy enhancing technologies of all kinds. For example, browser controls and plug-ins are widely available through leading browsers, and consumers who are concerned about privacy should be encouraged to enable these controls.

### *D. Minimizing Inconsistent and Unnecessary Restrictions on Business*

The NOI poses several questions regarding the potential for inconsistent regulation across countries, jurisdictions, and U.S. states.[25] As a general matter, the DMA believes that it is appropriate to strive for consistency in the regulations that apply to business data practices. However, consistency should not be achieved by spreading restrictive regulations from one jurisdiction to the next. The DMA encourages the Department of Commerce and the Administration to work to ensure that U.S. companies are not hindered in their growth and operation by foreign countries' efforts to impose restrictions that harm American businesses and do not comport with the U.S. approach to privacy regulation. Likewise, the Administration should refrain from supporting state efforts to limit businesses' data practices in ways that are stricter than or out of step with the approaches of other states.

* * *

The DMA appreciates the opportunity to provide these Comments to the Department of Commerce. Please contact Linda Woolley at 202-861-2444 or lwoolley@the-dma.org with any questions.

[25] *Id.* at 21229-21230.

**Before the**
**DEPARTMENT OF COMMERCE**
**Internet Policy Task Force**

| | | |
|---|---|---|
| In the Matter of | ) | |
| Information Privacy and | ) | Docket No. 100402174-0175-01 |
| Innovation in the Internet Economy | ) | |

---

**COMMENTS OF eBay Inc.**

---

Scott Shipman, CIIP
Senior Counsel, Global Privacy Leader
eBay Inc.
2065 HAMILTON AVE
SAN JOSÉ, CALIFORNIA 95125
408-376-7512

June 14, 2010

eBay Inc ("eBay") hereby submits these comments to the Department of Commerce's ("Department") "Information Privacy and Innovation in the Internet Economy" Notice of Inquiry ("NOI"). eBay appreciates the opportunity to provide our thoughts and feedback on issues as important as information privacy protections and promoting innovation on the Internet.

Founded in 1995 in San Jose, Calif., eBay (NASDAQ:EBAY) connects millions of buyers and sellers globally on a daily basis through eBay, the world's largest online marketplace, and PayPal, which enables individuals and businesses to securely, easily and quickly send and receive online payments. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites, which together have a presence in more than 1,000 cities around the world.

eBay takes the quality of the privacy protections we provide to our users very seriously. The success of our community is based on trust, which is strengthened by our ability to provide our users with a level of transparency and control concerning the collection and use of information about them and their activities. Because of our strong privacy protections, Privacy International rated eBay one of the best companies for privacy on the Internet[1] and eBay is the most trusted company in 2009 for privacy as rated by U.S consumers[2].

eBay strongly believes that innovation in the Internet economy depends on consumer trust and that maintaining consumer privacy is essential to the continued growth of the Internet. Thus, eBay supports initiatives that seek to provide a rational and constructive framework to protect consumers while recognizing legitimate uses of personal information. Therefore, we applaud the Department's efforts to conduct a comprehensive review of the nexus between privacy policy and innovation in the Internet economy.

Although eBay believes that a number of the questions posed in the NOI are important to the overall discussion of developing a strong and effective U.S. privacy policy framework, we have focused our comments to the particular questions raised in Question 1 of the NOI: "The U.S.

1 Privacy International Consultation Report, 2007. Available at:

http://www.privacyinternational.org/issues/internet/interimrankings.pdf

2 Survey conducted by Ponemon Institute and TRUSTe in September 2009. See www.truste.com, Press room, Archives, September 16, 2009 **:** 2009 Most Trusted Companies In Privacy Announced

Privacy Framework Going Forward", specifically those relating to the continued relevance of the notice and choice approach and whether other models, such as use-based models, would be a more useful approach:

> *Is the notice and consent approach to consumer data privacy still a useful model? Are there alternative approaches or frameworks that might be used instead of notice and choice? Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use.*

## I. Is the notice and consent approach to consumer data privacy still a useful model?

eBay has consistently been an Internet industry leader in advocating stronger privacy protections over the past several years. After seeing the need to rally industry support for greater federal action and involvement on this issue, eBay co-founded the Consumer Privacy Legislation Forum, now known as the Business Forum for Consumer Privacy ("BFCP"), which has been the primary developer of the use and obligations model, which we will discuss in greater detail below.

We believe it is important to note that responsible data collection has become almost a de facto necessity for most, if not all, Internet companies today and allows these entities the opportunity to customize and personalize their services and products to better meet the needs and expectations of consumers. Or more simply put, data collection is an important tool used by entities to innovate and compete globally.

However, we strongly believe that the current notice and consent policy framework has not only been ineffective at promoting innovation in this area, but it has not adequately protected consumer data from unexpected or inappropriate collection and use. Innovation is really about moving into "unchartered territory", but the notice and consent model has proved to be an extremely brittle and restrictive binary framework that has hindered organizations from moving forward in a responsible manner.

While we fully support the need to ensure transparency, notice, choice, accountability, and user preferences, we believe that the current notice and consent model has created a never ending series of requests for consent that has resulted in counterproductive "reflexive" or "blind" consumer consent. In other words, after years of being inundated by consent requests from a multitude of entities, oftentimes consumers

consent to user agreements or privacy polices without thorough review and examination.

In our opinion, the notice and consent model needs to evolve and adapt to the information economy in order to provide the protections needed to encourage consumer trust while still seamlessly delivering to consumers the services they desire.

## II. Are there alternative approaches or frameworks that might be used instead of notice and choice?

We believe that the use and obligations model is an alternative approach that would not only improve the consumers experience of the Internet while substantially removing privacy risks associated with undesired collections of user data for commercial purposes, but it would also permit the responsible Internet company to fully utilize this important business tool.

For years, it has been widely accepted and endorsed that any privacy policy must first be built upon the foundation of traditional principles of fair information practices. These principles include transparency of data collection and use, consumer engagement, data security, and data accuracy. Although these traditional principles may still apply today and are still a sound starting point for any privacy framework, the traditional way of applying these principles, for instance through the notice and consent model, no longer effectively provides consumers with adequate protection, as we stated above.

We believe that the use and obligations model provides an alternative framework that applies these traditional principles of fair information practices in a manner that takes into consideration the way data is used and managed today. In short, instead of the collection of data and consumer consent triggering an entity's obligation to protect data (notice and consent), we propose that the way an entity uses data determines the actions the entity must take to: (1) provide transparency and choice to the consumer; (2) offer access and correction when appropriate; and (3) to determine the appropriateness of the data with respect to its quality, accuracy and integrity.

## III. Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use.

The fundamental principles of the use and obligations model is explained in great detail in the BFCP's Privacy's white paper released in late 2009, "A Use and Obligations Approach to Protecting Privacy: A Discussion Document." [3] The white paper clearly outlines and defines the categories of data use, the potential harm associated with each use and the data protection obligations associated with each use.

According to the BFCP white paper, there are five primary categories of data use and two categories of obligations. The categories of data use are as follows: (1) fulfillment; (2) internal business operations; (3) marketing; (4) fraud prevention and authentication; and (5) external, national security and legal.

The categories of obligations include: (1) those that facilitate consumer participation and engagement (i.e. transparency, notice, choice, and access and correction); and (2) those that involve an organization's internal activities to assess and mitigate data security risks (i.e. collection limitation, data use minimization, data quality and integrity, data retention, etc.)

As explained above, the obligation(s) will depend on the use of the data and ultimately the organization's desire to prevent harm to the consumer. For example, data used for marketing purposes would trigger the following obligations: (1) notice; (2) an opportunity to opt-out; (3) generalized access to the data collected; and (3) a requirement for the organization to assess the risks to the individual when determining collection and use minimization and data retention policies.[4] It is important to note that responsibility for meeting these obligations is not solely on the organization, but on all holders of the collected data, such as third party vendors and service providers, which would hold the third parties to the same standards as the organization itself and provide an added layer of protection for the consumer's data.

---

[3] "A Use and Obligations Approach to Protecting Privacy: A Discussion Document", The Business Forum for Consumer Privacy: December 7, 2010. To access the full document please follow this link: http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf

[4] For additional examples, please reference Table A located on page 6 of the BFCP's white paper.

## IV. Conclusion

eBay thanks the Department for its commitment to encouraging privacy and innovation in the Internet economy and for the opportunity to provide comments on the current policy framework and potential alternative frameworks, such as the use and obligations model, which we believe might assist in moving the dial in regard to promoting innovation and restoring consumer trust. eBay looks forward to working with the Department in the months and years ahead on these important issues.

EDUCAUSE

Docket No. 100402174
Notice of Inquiry

June 7, 2010

Attention: Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce

Dear Members of the Internet Policy Task Force:

Thank you for the opportunity to submit comments in response to the Department's review on Information Privacy and Innovation in the Internet Economy. We respectfully submit these comments on behalf of EDUCAUSE – a non-profit organization whose mission is to advance higher education by promoting the intelligent use of information technology.

We are writing to express the views of the higher education information technology and privacy community regarding the strategic and operational impact of information privacy and the Internet economy upon our nation's colleges and universities. We recognize that the Department has consulted many academic experts – faculty who come from our community of institutions whose academic discipline, research, and experience lend incredible expertise; however, we represent the voice of campus administrators and higher education leaders who can speak on the importance of innovation, privacy practices, and the Internet economy to the future of higher education.

Higher education, working with the federal government, established high speed data networks for research and education. The deployment of information technologies has transformed higher education through learning technologies that support curriculum and distance education, online libraries and digital repositories, and software applications for administration and research or grid computing. The increased leverage of commercial applications for enterprise systems and ongoing experiments with a variety of platforms for cloud computing requires standards for privacy and security that reflect higher education's interest in protecting its constituents and preserving the foundation of our teaching, research, and service missions to American society.

Privacy protections directly impact the higher education community, its students, employees, and guests. Current privacy law and regulation is overly complex and confusing, where higher education institutions are governed by numerous and varied laws, institutional policies, and local institutional cultures. We strongly feel that there is a need for standardization and clarity to today's privacy framework in order to preserve and facilitate further innovation in the higher education sector.

1150 18th St. NW, Suite 1010
Washington, DC 20036
Main 202.872.4200
Fax 202.872.4318

4772 Walnut St., Suite 206
Boulder, CO 80301
Main 303.449.4430
Fax 303.440.0461

educause.edu

We would like to briefly address some of the issues raised in the Request for Comment.

1. The U.S. Privacy Framework Going Forward

The application of privacy practices in colleges and universities draws upon a combination of approaches: voluntary adoption and promotion of fair information privacy practices; compliance with a diverse array of state, federal, and foreign laws and regulations; and other legal or contractual requirements. Additionally, core academic values in our institutions (e.g., academic and intellectual freedom, ethics, research on human subjects, social responsibility, etc.) typically adhere to heightened standards of privacy protections that extend beyond minimal legal requirements. However, the "consumers" of the programs and services offered at a college or university bring privacy expectations that are shaped by their experiences in commerce, government, and other sectors of the economy. Thus, colleges and universities are increasingly impacted by a fragmented compliance regime that regulates our sector according to the type of information we collect and maintain (e.g., health, financial, education records, etc.).

There is also concern among administrators that these obligations are imposing "unfunded mandates" during a time where demands on funding exceed resources available. We support a comprehensive privacy framework that transcends sectors of the economy that will simplify compliance, minimize costs for not-for-profit institutions, and maximize appropriate privacy protections for individuals.

2. U.S. State Privacy Laws

Public or state-assisted higher education institutions may be subject to state laws and local requirements depending upon their independence or status as a state agency. All institutions may be subject to data privacy or security laws depending on the scope of the legislation. The application of state privacy and information security laws to colleges and universities is complicated by the fact that while the locus of operations for an institution is typically limited to a single state, the students who attend these institutions come from states across the nation. Therefore, security breach notification laws (enacted in at least 46 different states) create a confusing and complicated legal and regulatory landscape. The advent of the Internet for use in interstate commerce, including educational applications such as distance education and collaborative research programs, will require more uniform, federal approaches to mitigate the challenges of implementing a fragmented set of diverse state laws.

3. International Privacy Laws and Regulations

As colleges and universities expand their academic, research, and service missions overseas, we are particularly mindful of the complexity of foreign and multinational privacy regimes. Some colleges and universities are establishing formal campuses abroad, bringing into play privacy compliance in the countries where those campuses are located. More commonly, faculty and students travel to other countries for study or

research for very short durations, often moving from country to country during the course of their visit. Addressing privacy compliance in coordinated international research efforts and academic ventures carried out this way can be especially difficult. Harmonization of data privacy principles and laws would have significant benefit to the higher education community and facilitate global collaboration and innovation for the benefit of society around the world.

4. Jurisdictional Conflicts and Competing Legal Obligations

The complexity of data breach legislation throughout the various states and questions regarding enforcement across state lines is symptomatic of the challenges faced by colleges and universities. Additionally, the lure of "cloud computing" to improve services and reduce costs in higher education is tempered by uncertainties regarding legal jurisdiction that even the providers of cloud computing services are not able to resolve. A significant barrier to the adoption of these innovative and cost effective services by higher education as a whole has been the providers' inability to limit data storage or flow within the boundaries of the U.S.; thus, making the use of these services too risky for higher education.

5. Sectoral Privacy Laws and Federal Guidelines

In addition to the federal laws cited in the Notice of Inquiry (e.g., HIPAA, FCRA, GLBA, COPPA, etc.) that have nuanced applications to institutions of higher education, the Family Education Rights and Privacy Act (FERPA) addresses the privacy of student education records. The Department of Education's Family Policy Compliance Office is responsible for issuing regulations and enforcement. From an institutional perspective, the diverse array of federal regulatory and enforcement agencies (i.e., Department of Health and Human Services, Federal Trade Commission, Department of Education, etc.), combined with the unique approach taken by each data privacy law adds additional levels of complexity that make creating a uniform approach to compliance difficult at the enterprise level.

Although a consumer may be oblivious to how their various types of information are governed by federal law and regulation, they are typically subject to a variety of institutional policies or practices as well, each uniquely designed to protect their privacy in accordance with the compliance obligations imposed on educational institutions. For example, a website privacy policy may exist at the institution's choice or because it is required by state law; a notice of privacy practices may be issued to students who visit the student health center; a policy on student education records may be referenced in course syllabi; a consent form may be required before a student participates in a research project where they are deemed a human subject. While these individual approaches may heighten sensitivity and awareness of the need for privacy protections, they also confuse if not obscure expectations of the consumer for whom they are designed to protect.

6. New Privacy-Enhancing Technologies and Information Management Processes

Colleges and universities have been leaders in the development and use of privacy-enhancing identity management technologies and practices. The National Science Foundation funded the National Middleware Initiative, led by EDUCAUSE and Internet2, in an effort to advance the use of middleware technologies in higher education for purposes of identification, authentication, and authorization. Institutional efforts to centralize data collection and use for identity and access management help to eliminate the unnecessary redundancy of multiple user IDs and passwords for access to individual systems and in the process improve privacy protections for the individual. Increasingly, the move towards more federated systems of identity management, including the use of the InCommon Federation (www.InCommon.org) for research and education networks, creates a trust framework that minimizes the information exchanged between identity providers and relying parties. The community of trust inherent among higher education institutions makes us a good testing ground for the application of inter-institutional federations.

7. Small and Medium-Sized Entities and Startup Companies

While the most well known higher education institutions tend to be large organizations as measured by number of students, employees, scope of activity, and resources, the vast majority of institutions are small to mid-size that include two-year (community) colleges and four-year colleges and universities. These institutions are often resource-constrained and rarely have a chief privacy officer or another individual expert on privacy matters. Fortunately, the size and scope of their operations limit the impact of certain laws that might only apply to larger, research universities. However, they share many of the same challenges with respect to compliance with state, federal, and foreign laws, having to do so with fewer resources.

8. The Role for Government/Commerce Department

We believe that the U.S. Department of Commerce is well-positioned to assess the impediments to commerce and innovation that our current privacy regulatory regime imposes. Where commerce and innovation are overly impeded without compelling privacy gain, the Department should aim to develop solutions. One critical solution that the Department could help lead is to bring together regulatory bodies and other experts domestically and internationally with the goal of harmonizing requirements and facilitating important services, research, innovation that are dependent on the flow of data. In such an effort, we offer the following recommendations for how the work should proceed:

1. Establish principles – not overly prescriptive rules – that protect privacy and advance innovation. Examples include meaningful consent, reasonable access, and security controls that are effective for varying types and sizes of organizations.

2. Differentiate among choice requirements depending upon the type of information and forms of use. In other words, there should be fewer privacy concerns and less need for robust opt-in procedures when an organization is not using data for advertising or marketing purposes or making decisions that significantly impact the individual (such as employment-related uses.) The converse is true as well.

3. Encourage legislation to standardize breach notification standards and procedures.

4. Establish a focus on research activities and how privacy laws should be applied in a way that allows important research to proceed while adequately protecting privacy.

5. Facilitate innovation by developing and supporting methods whereby entities can participate in new, Internet-based systems of collaboration, including the utilization of cloud computing providers who should be incented to abide by regulations and best practices in privacy protection.

6. Promote the simplification and standardization of privacy statements that are understandable to users.

In conclusion, we thank the Internet Policy Task Force for examining these critical issues, especially the impact of the Internet economy on privacy and innovation, both deeply important to our nation's colleges and universities. We look forward to continued work with the Department and the Internet Policy Task Force to formulate policies that will address the privacy challenges we face in higher education.

Sincerely,

Greg Jackson
Vice President, Policy and Analysis

# Edward Robert McNicholas, Esq.

1131 Bayliss Drive • Alexandria, Virginia 22302
(202) 302-1772 • EdwardMcNicholas@gmail.com

June 14, 2010

**Comments on Information Privacy and Innovation in the Internet Economy**

The following comments are submitted for consideration as part of the Department's comprehensive review of privacy policy and innovation in the Internet economy, pursuant to the Department of Commerce's April 23, 2010, Notice of Inquiry.[1]

The Department's thoughtful consideration in this key area of economic growth is essential to ensuring the continuation of the United States' leadership in global electronic commerce. The Notice of Inquiry addresses precisely those areas in which the Department should focus its attention, and, in particular, the need for international negotiations to resolve the persistent legal conflicts that hamper innovation and global competition.

In summarizing the current U.S. privacy framework, the Department, however, overlooks much of the distinctly U.S. contribution to the development of rights of privacy. For instance, although the Department correctly notes the importance of the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, it neglects to note that these principles were based on the 1973 report by the U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens*, which first called for a code of fair information practices.

More fundamentally, the Department's scope of inquiry should extend beyond statutory pronouncements and various regulatory codes and proposals to appreciate and express the organic fullness of U.S. privacy protections. U.S. privacy law is as least as much a creation of constitutional law and the courts, as it is of the legislature, and the Department will miss much of the distinctly American contributions to international privacy law if it focuses too much on the various codes of privacy practice being developed by regulatory agencies. This omission is

[1] For the sake of clarity, I note that these comments reflect my personal views and do not reflect the views of any law firm, its clients, any government, or any other organizations with which I am affiliated or represent.

particularly significant because U.S. companies base much on their risk assessment on these common law restrictions. Few would doubt that the potential for a consumer class action based on a privacy tort is as significant as the potential for a notice of a regulatory inquiry in shaping corporate behavior. U.S. enforcement of privacy rights by the threat of potentially enormous punitive damages and the vigorous and inventive class action plaintiff's bar is a very significant driver of actual compliance in the U.S., and it is an aspect of privacy law in which many EU countries can offer relatively few comparable examples. Failing to give a vigorous explanation of the full basis of U.S. privacy law neglects much of its long-standing constitutional origins and can give foreign governments the distinctly incorrect impression that U.S. privacy law is a recent innovation in response to the European Union's Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJL 281, 23 Nov. 1995 p.31. Moreover, it can leave U.S. interests subject both to EU-style complex regulation as well as the common law enforcement largely absent in the EU.

Particularly in light of the need to ensure sufficient flexibility in privacy norms to match the development of the Internet economy, we should emphasize, not diminish, the common law's special genius in adapting to innovations. Surely the Department should cite Warren & Brandeis's 1890 *The Right to Privacy*, 4 Harvard Law Review 193, as a seminal formulation of U.S. privacy law, as much as it does the thoughtful publications of the White House during the 1990s. It bears emphasis, particularly in the context of the European Union negotiations, that the U.S. Constitution has since its inception respected rights of privacy and autonomy by guaranteeing our First and Fourth Amendment freedoms. At the heart of the Fourth Amendment lies "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." *Winston* v. *Lee*, 470 U.S. 753 (1985) (quoting *Olmstead* v. *United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)); *see also California Bankers Ass'n* v. *Shultz*, 416 U.S. 21, 65 (1974) (recognizing right to be let alone as embedded within Constitutional limits upon searches and seizures). Our Supreme Court has consistently recognized that, "[t]o protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting); *see also Katz* v.

*United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) (recognizing a reasonable expectation of privacy in the substantive content of telephone discussions).

Some foreign commentators on U.S. law have been particularly fond of noting that, under the Fourth Amendment, the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" *Smith* v. *Maryland*, 442 U.S. 735, 743-44 (1979) (citing cases); *see United States* v. *Miller*, 425 U.S. 435, 443 (1976). Particularly in light of this trend and the European Union's nascent consideration of these issues of governmental privacy under the Lisbon Treaty, it is important for the Department to express that our Fourth Amendment continues to provide robust privacy protection for the Internet economy by protecting the contents of communications. *See Katz* v. *United States*, 389 U.S. 347, 362 (1967) (Harlan, J., concurring) (recognizing a reasonable expectation of privacy in the substantive content of telephone discussions). Indeed, the Fourth Amendment concerns that information loses privacy interests when it is conveyed to third parties are not relevant to the First Amendment in many contexts, because the First Amendment is fundamentally concerned with protection of communication, and communication inherently involves conveying information to third parties. As the Supreme Court has made clear, First Amendment rights to anonymity and privacy continue to exist even though information is communicated to a third party. *See, e.g., NAACP* v. *Alabama ex rel. Patterson*, 357 U.S. 449 (1960). These rights are as vital to the Internet economy as ever because "[a]nonymity is a shield from the tyranny of the majority." *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (citing J.S. Mill, *On Liberty and Considerations on Representative Government* (R. McCallum ed. 1947)); *see also, e.g., Watchtower Bible & Tract Soc'y* v. *Village of Stratton*, 536 U.S. 150 (2002); *Buckley* v. *American Constitutional Law Found., Inc.*, 525 U.S. 182, 200, 204 (1999).

These comments are intended to encourage the Department to emphasize that the U.S. leadership in the protection of personal privacy on the Internet stems not only from its statutes but also from seminal cases such as the Supreme Court's recognition that the right to anonymous speech applies equally to anonymous association via the Internet. *Reno* v. *ACLU*, 521 U.S. 844, 870 (1997) (there is "no basis for qualifying the level of First Amendment scrutiny

that should be applied to [the Internet]).[2] Indeed, these First Amendment principles support key aspects of evolving notions of privacy as an aspect of broader conceptions of human autonomy, such as the rights of free association, as is *Reno* v. *ACLU*, religious liberties, and related, so-called hybrid rights such as the ability of parents to direct the education of their children, as acknowledged in *Pierce* v. *Society of Sisters*, 268 U.S. 510 (1925) and *Wisconsin* v. *Yoder*, 406 U.S. 205 (1972).

In reflecting the state of U.S. privacy law, it bears emphasis that our constitutional norms continue to find fruitful elaboration in Prosser's privacy torts, as re-stated in the *Restatement (Second) of Torts* formulation of four privacy torts: Intrusion upon Seclusion, Section 652B; Appropriation of Name or Likeness, Section 652C; Publicity Given to Private Life, Section 652D; and False Light Publicity, Section 652E.

European code-based approaches to privacy can erode these fundamental liberties and aspects of the U.S. constitutional framework by potentially imposing requirements for prior regulatory approvals for use of personal information. Such concepts of prior restraint are rightly anathema to the U.S. fundamental freedom of speech, and the Department should vigorously contest efforts to undermine such freedoms.

Agreements such as the EU Safe Harbor framework well exemplify a balanced approach to privacy that respects both the fundamental rights of privacy and freedom of speech, but the Department should continually emphasize to our European allies that the fundamental human right to the freedom of speech is at least as significant as is the fundamental human right to personal privacy.

Likewise, as the various EU Member States continually remind U.S. entities of the need to comply with local laws in each jurisdiction, the Department should acknowledge and emphasize the products of our various laboratories of democracy such as the California Supreme Court decision, *Burrows* v. *Superior Court*, 529 P.2d. 590 (Cal. 1974) (reaching the opposite result from *Miller* on similar facts). Indeed, many state constitutions expressly recognize a right to privacy. Although some state courts have recognized an implicit right to privacy, explicit privacy provisions are more common and are found in Alaska, Arizona, California, Florida,

[2] The evolution of these rights into the Internet era should also inform the Department's consideration of issues, such as the protection of Internet copyright. *See, e.g.*, *Harper & Row Publishers, Inc.* v. *Nation Enterprises*, 471 U.S. 539, 568 (1985) (recognizing that the First Amendment does not protect copyright infringement).

Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington.[3] The constitution of California, in particular, is noteworthy because its constitutional right to privacy exists even without state action. *See Hill* v. *NCAA*, 865 P.2d 633, 644 (Cal. 1994) (en banc); *see also* Cal. Civ. Code § 1798.1 ("The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California . . . and that all individuals have a right of privacy in information pertaining to them."); *Jeffrey H.* v. *Imai, Tadlock & Keeney*, 85 Cal. App. 4th 345, 353 (Cal. Ct. App. 2000).

Global innovation is well served by the Department's thoughtful consideration of the ways in which privacy laws support and inhibit global information flows, and I entirely support this effort. In formulating its restatements of U.S. privacy law, it is vital to the accuracy of those summaries – and the living truth of our constitutional culture – that the Department reflect and embrace the various common law and state contributions to the exceptional privacy protections enjoyed by the citizens of the United States.

Please contact me directly if I may be of further assistance to the Department.

Sincerely,

/s/ Edward Robert McNicholas

[3] Alaska Const. art. I, § 22; Arizona Const. art. II § 8; California Const. art. I § 1; Florida Const. art. I § 12; Hawaii Const. art. I §§ 6-7; Illinois Const. art. I §§ 6 & 12 Louisiana Const. art. I § 5; Montana Const. art. II § 10; South Carolina Const. art. I § 10; and Washington Const. art. I § 7.

GIBSON DUNN

Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

June 14, 2010

DELIVERED VIA E-MAIL

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Re: Comments of Facebook, Inc. on Information Privacy and Innovation in the Internet Economy

Dear Mr. Strickling:

Facebook, Inc. respectfully submits the attached comments in response to the U.S. Department of Commerce, National Telecommunications and Information Administration's Notice of Inquiry on Information Privacy and Innovation in the Internet. 75 Fed. Reg. 21,226 (Apr. 23, 2010); 75 Fed. Reg. 32,372 (June 8, 2010).

Sincerely,

John F. Bash
Gibson, Dunn & Crutcher LLP
1050 Connecticut Ave. NW
Washington, DC 20036
(202)-955-8298

Attachment(s)

**Comments of Facebook, Inc.**

**In Response to the "Notice of Inquiry"**

**by the**

**U.S. Department of Commerce,**

**National Telecommunications and Information Administration:**

**Information Privacy and Innovation in the Internet Economy**

**Submitted June 14, 2010**

Colin S. Stretch
Deputy General Counsel
Timothy D. Sparapani
Director, Public Policy
Facebook, Inc.
1601 S. California Avenue
Palo Alto, CA 94304
(650)-485-6271

## TABLE OF CONTENTS

**Comments of Facebook, Inc.**

**In Response to the "Notice of Inquiry"**
**by the**
**U.S. Department of Commerce,**
**National Telecommunications and Information Administration:**

**Information Privacy and Innovation in the Internet Economy**

**Submitted June 14, 2010**

Facebook, Inc. submits these comments in response to the Department of Commerce's notice of inquiry regarding "the nexus between privacy policy and innovation in the Internet economy."[1] Facebook commends the Department for establishing its new Internet Policy Task Force and for making it a "top priority to ensure that the Internet remains open for innovation."[2] The Department properly recognizes that "the Internet is crucial to U.S. innovation, prosperity, education and political and cultural life."[3] And as the Department notes, in the coming years U.S. policymakers will face a host of questions about whether and to what extent legal constraints should be placed on the Internet's openness as a means of expression and information exchange.

Facebook is the largest social-networking service in the world. It allows users to connect and share information over the Internet—thoughts, photographs, news articles, videos—with their relatives, friends, colleagues, and others, all free of charge. In the span of only six years, Facebook has grown to serve over 450 million active users—one-fourteenth of the world's population.

---

[1] 75 Fed. Reg. 21,226 (Apr. 23, 2010).

[2] *Id.*

[3] *Id.*

Facebook was created and launched from a Harvard dorm room by CEO Mark Zuckerberg in 2004. Its network initially reached only four universities, but by the end of 2004, as Facebook expanded to other colleges, nearly one million active users had signed up. In 2005, Facebook expanded its networks to reach high schools and foreign institutions, and in 2006 Facebook was opened up to anyone with an e-mail address.

At the same time as Facebook has expanded its user community, it has developed innovative information-sharing functionalities responding to the immense public demand for greater openness and connectivity—a photo-sharing feature that, with some 48 billion pictures online, constitutes the largest photo archive in the world; a "Wall" feature through which users can post messages on their friends' individual pages; and the immensely popular "News Feed," which informs a user's network of friends about changes in the user's status and displays user-created content. Facebook has also established Facebook Platform, which enables third-party developers to create innovative "social" applications that enhance the Facebook experience and allow users to experience and benefit from the Facebook community on numerous devices and locations around the Internet.

The development of Facebook's service has mirrored the rapid evolution of the Internet and Internet norms. Users join Facebook precisely because they *want* to share their information with others, as a way of expressing themselves, communicating ideas, forming communities and maintaining relationships across the country and the globe. At the same time, a core aspect of Facebook is the set of extensive controls that Facebook gives users to customize who sees their information and how it is used. One of Facebook's driving principles is to continue to press forward in enhancing the openness and connectivity of the Internet, and of social-networking sites in particular, while improving the tools that allow users to control how their information is shared.

Facebook submits these comments to give the Department its perspective on how all stakeholders—users, industry, government—can work together to develop policies that will encourage innovation to the maximum extent possible and that will reflect the public's growing preference for increasingly open and personalized paths of communication. In Facebook's view, a self-regulatory approach that allows for individual user choice offers the best path

forward—the clearest way to balance user demand for openness and sharing with legitimate concerns about personal information. Government agencies like the Department of Commerce can play a valuable role in encouraging the development of better mechanisms for user control over information and championing efforts that prove successful.

## I.

## The Internet and Innovation

### A. The Internet Today

It goes without saying that the Internet has brought profound changes to American life. Its rapid growth and expansion have yielded incalculable benefits to the American and global economies. At a social level, the Internet has enabled new forms of communication and expression, from e-mail to blogs to wikis. At the same time, the Internet has invited new threats, such as Internet fraud, phishing, spam, computer viruses, and cyber terrorism. The challenge for policymakers is determining how to combat such threats without stifling the innovation that makes the Internet such a powerful medium.

Since the late 1960s when the Internet was developed as a research project for the Department of Defense (called "ARPANET"),[4] the few links that originally connected a handful of universities and laboratories now connect nearly 2 billion people around the world.[5] Today 74 percent of Americans use the Internet.[6] That number will approach 100 percent soon, given that 93 percent of Americans between the ages of 18 and 29 use the Internet,[7] and the first generation of children who grew up with the Internet is rapidly reaching maturity. Seventy-one

---

4 *See generally The Internet*, *in* THE NEW YORK TIMES GUIDE TO ESSENTIAL KNOWLEDGE 454-59 (2007).

5 *Internet Usage Statistics, The Internet Big Picture*, World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm.

6 PEW INTERNET & AMERICAN LIFE PROJECT, DEMOGRAPHICS OF INTERNET USERS (2010) http://www.pewinternet.org/Static-Pages/Trend-Data/Whos-Online.aspx.

7 *Id.*

percent of Americans use the Internet every day.[8] This rapid growth had led to rapid innovation, with users demanding new services and facilitating those services through their participation.

The Internet has provided numerous functionalities that have fundamentally changed the way people interact with the world. The two dominant innovations of the 1990s were the World Wide Web and e-mail. But the past decade has seen an explosion in innovative functionalities that could not have been imagined during the Internet's infancy. Many of these technologies—commonly termed "Web 2.0"—promise to transform American life in much the same way that web-browsing and e-mail did in the late 1990s.[9] What distinguishes them from the first wave of functionalities is their level of interactivity and user-driven characteristics. Whereas traditional web-browsing restricts the user experience largely to viewing content, with the limited ability to engage in structured and bilateral transactions such as sending e-mail or making online purchases, Web 2.0 applications enlist users as both the viewers *and* creators of online content, frequently in a framework that is social and involves open forums or communities defined by the users.

The offerings of Web 2.0 span a wide range of functionalities and offer varying degrees of user controls. Blogs (originally short for "web logs") allow individuals to publish their thoughts and to spark debate on anything from politics to sports to their personal lives. Wikis (such as Wikipedia) function by allowing any user to post information and then allowing other users to modify and adjust the content, thereby leveraging the knowledge of the entire user community to keep entries thorough and up to date. Various consumer review sites, such as Yelp and Citysearch, allow patrons to provide ratings and reviews of restaurants, bars, and other local services. The website Pandora uses advanced algorithms to tailor music playlists to a user's tastes—ensuring that listeners receive a stream of music they like, while also allowing lesser-known musicians to gain exposure to listeners who are likely to appreciate their sound. And YouTube, an instant hit when it went live in 2005, allows even the least sophisticated

---

8 PEW INTERNET & AMERICAN LIFE PROJECT, TREND DATA (DAILY) (2010) http://www.pewinternet.org/Trend-Data/Online-Activities-Daily.aspx.

9 *See* Katie Hafner, *The Young Turks of Cyberspace*, N.Y. TIMES, July 27, 2008, at BR; Ben Zimmer, *Social*, N.Y. TIMES MAG., Apr. 4, 2010.

Internet users to upload video to the Web of anything from political demonstrations to home movies.

Web 2.0 also includes a host of social media focused on expression and personal connections. Social-networking services like Facebook, LinkedIn, MySpace, and Google Buzz enable users to connect with friends and others and to post content such as messages, business developments, and photographs on personalized pages. For a quarter of American Internet users, signing on to one of these social-networking sites is a daily activity.[10] A related service is provided by Twitter, which permits users to write short messages called "tweets" (140 words or fewer) that can be read by anyone who elects to follow those users. User demand for social media has also driven more specialized social-networking services. Blippy functions like Twitter, but focuses on what people are purchasing, allowing individuals to quickly share information about good buys and interesting products. Buzzd spreads real-time reviews of bars, restaurants, and clubs, allowing users to know what spot is "buzzing" on a given night. Gowalla, Foursquare, and other services have taken the power of the social network and linked it back to specific geographic locations in the brick-and-mortar world by allowing users to explore cities with their friends even when they are not in the same location. Classmates.com taps into existing alumni networks and allows users to reconnect with their peers from primary school, high school, and college.

Even in the realm of dating services, social networking has given users choices and experiences previously unavailable. Match.com, the most popular dating service, allows users to explore social and geographical networks to find potential partners. An innovative new service, Meezoog, has further leveraged the social network to pair people based on "trusted paths" and "social proximity."

Collectively, these and other innovative Web 2.0 applications have profoundly affected Americans' social interactions, sense of community, acquisition of information, and expression of viewpoints. In 2010 there exists a plethora of entirely new ways of connecting and

---

10 PEW INTERNET & AMERICAN LIFE PROJECT, TREND DATA (DAILY) (2010) http://www.pewinternet.org/Trend-Data/Online-Activities-Daily.aspx.

communicating, and these innovations promise to reshape the way Americans relate to each other and the world. But critically, each of these new forums for communication requires some level of user input and some sharing of user information, whether it is simply sharing knowledge on Wikipedia or actually posting personal information on a social-networking site. As the social experience of the Internet has become more interactive, it has also encouraged users to share their opinions and aspects of their lives with more people, providers, and the public at large. It is no surprise, then, that a recent groundbreaking study, the Pew Internet & American Life Project, a project of the Pew Research Center, found that users have become more comfortable with the amount of information about them available online.[11]

The impact of the Internet on the economy can be felt in more concrete, quantifiable ways as well. In 2009, online retail spending in the United States was nearly $130 billion, only slightly lower than in 2008 despite the enormous impact of the recession on the U.S. economy.[12] One estimate suggests that the commercial Internet adds $1.5 *trillion* in value to businesses and consumers worldwide.[13] And in a time of economic hardship, Web 2.0—and social networking services in particular—are providing a much needed engine of jobs, growth, investment, and innovation.

A critical component of that continued growth is online advertising. Like Web 2.0 applications generally, online advertising has grown to reflect user input, in contrast to the more static, one-size-fits-all advertising of traditional print and television media. In particular, online advertisers have employed "tailored" or "behavioral" advertising, which is directed at consumers based on their preferences, as demonstrated through their web-browsing activity or information they provide online. The Chairman of the Federal Trade Commission ("FTC"), Jon Leibowitz, recently praised these forms of advertising:

---

11 MARY MADDEN & AARON SMITH, PEW INTERNET & AMERICAN LIFE PROJECT, PEW RESEARCH CENTER, REPUTATION MANAGEMENT AND SOCIAL MEDIA 21 (May 26, 2010).

12 Jeff Clabaugh, *Online spending in 2009 falls*, MILWAUKEE BUS. J., Feb. 9, 2010.

13 ROBERT D. ATKINSON ET AL., THE INFO. TECH. & INNOVATION FOUND., THE INTERNET ECONOMY 25 YEARS AFTER .COM 1, 4 (2010).

> They are usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects.[14]

The efficiencies and benefits of behavioral advertising described by Chairman Leibowitz are particularly pronounced in the context of Web 2.0. As users express who they are and what they like through social media, service providers can better target advertisements to consumer preferences. And, in turn, more efficient advertising models will continue to provide the economic backbone and incentives for the "free" online services and applications that users have embraced and integrated into the fabric of their professional and personal lives.

### B. The Role of Government Regulation

To the great benefit of the public, the federal government has largely allowed the Internet to develop free of government regulation, while remaining vigilant to protect against serious threats to the physical and financial security of Internet users. That reserved posture is not the product of inattention but rather a conscious, bipartisan choice of policymakers and legislators.

In Section 230 of the Communications Decency Act, enacted by overwhelming majorities in the House and Senate in 1996,[15] Congress recognized that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, *with a minimum of government regulation*."[16] Congress declared that it was "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and interactive computer services, unfettered by Federal or State regulation."[17] In an age of dial-up

---

14 Jon Leibowitz, Chairman, Fed. Trade Comm'n, *Where's the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising*, Address at the National Cable & Telecommunications Association's The Cable Show 2010 (May 12, 2010).

15 The Communications Decency Act passed with the support of 81 U.S. Senators, both Republicans and Democrats. In the House, the Act passed unanimously. *See S.652 Telecommunications Act of 1996*, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=s104-652 (the Communications Decency Act is also known as the Telecommunications Act).

16 47 U.S.C. § 230(a)(4) (emphasis added).

17 *Id.* § 230(b)(2).

modems, Congress's prescience was remarkable. Few could have predicted in 1996 the tremendous role the Internet would come to play in commercial and social interactions.

Since the Communications Decency Act, Congress has continued to come together to ensure that the Internet will thrive in a robust zone of innovation and free thinking, unencumbered by stifling regulatory mandates or regulators operating with overly broad or ill-defined powers. The Internet Tax Freedom Act of 1998, also passed with broad bipartisan support,[18] imposed a moratorium on state taxes on Internet access.[19] That same year, Congress approved a "Declaration That the Internet Should Be Free of Foreign Tariffs, Trade Barriers, and Other Restrictions," with nearly unanimous support from both sides of the aisle.[20] In that declaration Congress made clear that electronic commerce must be free from "burdensome and discriminatory regulation."[21] Congress' ability to enact bipartisan legislation designed to facilitate innovation and growth on the Internet, even in a polarized political climate, highlights the national importance of such legislation.

Like Congress, the federal courts have recognized the need to proceed cautiously when it comes to regulating the Internet. For example, in *Zeran v. AOL*, a plaintiff attempted to impose liability on American Online for the defamatory messages posted by an anonymous third party on an online bulletin board. The Fourth Circuit Court of Appeals refused to extend tort liability to AOL based primarily on the congressional policy of non-regulation.[22] The court relied on § 230 of the Communications Decency Act, recognizing a congressional objective to "maintain the robust nature of Internet communication and, accordingly, to keep government interference

---

18 The Internet Tax Freedom Act of 1998 was approved by a vote of 96-2-2 in the Senate and passed by a voice vote in the House. *See U.S. Internet Tax Legislation*, OPENCONGRESS.COM, http://www.opencongress.org/wiki/U.S._internet_tax_legislation#Internet_Tax_Freedom_Act_of_1998.

19 *See* 47 U.S.C. § 151 (the moratorium has been extended by amendment until 2014).

20 Omnibus Consolidated and Emergency Supplemental Appropriations Act, Pub. L. No. 105-277, 112 Stat. 2681 (codified at 19 U.S.C. § 2241); *see also H.R. 4328 Omnibus Consolidated and Emergency Supplemental Appropriations Act 1999*, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=h105-4328 (detailing the Act's passage with unanimous Senate consent and a vote of 391-25-18 in the House).

21 112 Stat. at 727.

22 129 F.3d 327 (4th Cir. 1997).

in the medium to a minimum."[23] The court also cited Congress's findings that the Internet offers "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[24]

The hands-off approach to Internet regulation adopted by both Congress and the courts is critical for at least two reasons. First, in an area of such rapid technological change, regulations are likely to provoke unforeseen and undesirable consequences. Attempts to impose rigid legal requirements on websites or other Internet-based platforms will make it far more difficult for a college sophomore experimenting somewhere to devise the "next big thing." Would-be start-ups, faced with onerous and complex legal requirements or fearful that their activities could provoke the ire of a regulator armed with a broad and ambiguous legal standard, will find it more challenging to attract venture capital and talent—particularly foreign innovators, who may find their services put to better use in a jurisdiction without such legal uncertainty. The very fluidity of the Internet, which is fast-moving and not amenable to rigid line-drawing, will make it incredibly hard to calibrate legal standards that remain meaningful without stunting the Internet's capacity for technological innovation. Given that reality, the presumption should be that regulation will be limited.

The Chairman of the Federal Communications Commission ("FCC"), Julius Genachowski, recently recognized how the openness of the Internet fosters the creation of pathbreaking Internet-based applications like Facebook:

> Mark Zuckerberg was a college student in 2004 when he started Facebook, which just announced that it added its 300 millionth member . . . . This is the power of the Internet: *distributed innovation and ubiquitous entrepreneurship*, the *potential for jobs and opportunity everywhere* there is broadband. . . . [I]n the 21st century, the garage, the basement, and the dorm room remain places where innovators can not only dream but bring their dreams to life.[25]

---

23 *Id.* at 330.

24 *Id.*

25 Julius Genachowski, Chairman, Fed. Comms. Comm'n, Prepared Remarks at the Brookings Institute (Sept. 21, 2009), *available at* http://www.openInternet.gov/read-speech.html (emphasis added).

Were that openness to be constricted by ill-advised, ambiguous legal constraints, we might never know what future American innovators would have created in their garages or dorm rooms.

In the words of the current head of the FTC's Bureau of Consumer Protection, David Vladeck, it would be "foolhardy" to "set strict or binding regulations or inflexible norms" with respect to Internet privacy issues.[26] Because the "technologies . . . are evolving so quickly," he explained, the government should not "try to set rules in place knowing that two or three years later they would be rendered obsolete."

Second, it is important that policy-makers avoid legal regimes that limit consumer choice by restricting the ability of a provider of content or functionality to change its design or options over time. Many of today's most popular and functional Internet-based applications—from Gmail to iTunes to Facebook—started out with a far different suite of options than they currently offer, and then evolved to their current formats. Their ability to satisfy customer demand depended critically on their ability to make what were often substantial changes to their user interface and services. For Internet companies—just as for a movie producer, a musician, or a manufacturer—enhancing users' lives can involve developing and offering experiences that users themselves have not yet thought of. The original offering that falls flat is an unavoidable byproduct of innovation and cultural and economic progress (for example, Apple's early-1990s Newton device achieved nowhere near the success of its later iPod or iPad). For these reasons, legal constraints that "freeze" Internet applications by hampering their ability to alter initial offerings—on the ground of preserving amorphous "user expectations"—would be nothing short of disastrous for Internet innovation and consumer choice. They would also unreasonably favor new entrants over companies with an established record of success and would incentivize those new entrants to provide consumers with as few options as possible for fear of having those options frozen in place by regulators.

---

26 *See* Interview by John Villafranco (for the TheAntitrustSource.com) with David Vladeck, Director, Fed. Trade Comm'n Bureau of Consumer Prot. (Mar. 19, 2010), *available at* http://www.abanet.org/antitrust/at-source/at-source.html.

For these and other reasons, Internet features that enhance users' control of the information they share, discussed at greater length below, are far preferable to attempts by U.S. or foreign regulators to impose rigid constraints on information-sharing on the Internet.

None of this is to say that there is no role in the Internet for regulation. Far from it. The government must be constantly watchful for serious threats to the physical well-being of Americans and for criminals and miscreants who leverage the Internet's openness and capacity for anonymity to engage in financial scams, identity theft, and other fraudulent activity that causes tangible harm to members of the public. That is why Congress has enacted targeted statutes that address those problems without cabining the creative freedom that is the lifeforce of the Internet. In laws like the Computer Fraud and Abuse Act,[27] the Child Online Privacy Protection Act,[28] and the CAN-Spam Act,[29] Congress has addressed specific problems—such as the collection of personal information from those too young to consent and the incessant annoyance of spam—through regulatory schemes that go no further than necessary to remedy the problems they address. Facebook has invoked these laws vigorously to defend its users against malicious online attacks and to help make the Internet safer for all by taking spammers out of commission: the Company, for instance, has obtained the two largest-ever civil judgments under the CAN-Spam Act. [30] Such laws, which eschew open-ended grants of regulatory authority or vastly over-inclusive prohibitions, should serve as the model for any future legislative initiatives. Moreover, as with those pieces of legislation, Congress should build an evidentiary record of real harm before intervening.

In addition, government agencies and private standard-setting bodies can be of assistance by formulating general principles of Internet conduct. For example, the FTC has established principles of self-regulation for both Internet privacy generally and for behavioral advertising.[31]

---

27 Pub. L. No. 99-474, 100 Stat. 1213 (Oct. 16, 1986).

28 Pub. L. No. 105-277, 112 Stat. 2581 (Oct. 21, 1998).

29 Pub. L. No. 108-187, 117 Stat. 2699 (Dec. 16, 2003).

30 A 2008 judgment against Adam Guerbez and Atlantis Blue Capital ($873 million) and a 2009 judgment against the "Spam King" Sanford Wallace ($740 million).

31 *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; FED.

[Footnote continued on next page]

Similarly, the private nonprofit organization TRUSTe certifies that websites, including Facebook, comply with its privacy guidelines. This sort of partnership between the public and private sectors will be integral to Internet regulation in the coming decades.

### C. Extraterritorial Aspects of Internet Regulation

Any policy approach to Internet-based applications should take into account the inherently international character of the Internet. A user "tweeting" in Los Angeles can instantly reach an audience in Mumbai, and the Wikipedia entry on George Washington can be edited by a high school student in Tokyo just as easily as by a professor in Milwaukee. Because of the fundamentally global dimension of the Internet, however, one nation's lawmakers can have an outsized impact on Internet policy. It is extremely difficult for Internet-based applications to adopt one set of features for one country and a different set for another country.

While the United States government has for the most part maintained a narrowly tailored approach to the regulation of the Internet, some other nations' regulators have taken a more interventionist approach. For example, many EU members have adopted significant restrictions on the sorts of consensual data collection and processing practices that are routinely undertaken by Internet-based services. Those restrictions, if applied to United States companies, could reduce the openness, connectivity, and efficiency that users (including American users) have come to expect from the Internet. For now, the European Union has agreed to the U.S. - European Union Safe Harbor Framework, developed by the Department of Commerce in consultation with the European Commission.[32] Ordinarily under the laws of the European Union, a company cannot export data from a European country into another country with

---

[Footnote continued from previous page]
TRADE COMM'N, SELF REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

32 U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (July 21, 2000), http://www.export.gov/safeharbor/eu/eg_main_018475asp.

allegedly "less adequate" data protections.[33] But the Safe Harbor agreement provides a set of guidelines that U.S. companies can follow when operating in Europe.

The Safe Harbor approach is far preferable to a system that permits one country to dictate Internet policy throughout the world. For a company like Facebook, for example, which boasts an active presence in over 180 countries and which counts 70% of its users from outside of the United States, it is essential to have a concise, consistent international regulatory policy. It would simply not be feasible for a service like Facebook to adjust its settings, controls, and technologies to comply with different regulations in all of the nations where it enjoys a user base. The Department of Commerce should actively consider and implement additional mechanisms to ensure that Web 2.0—and the jobs and innovation that American companies in this space are creating—are not hamstrung by international legal regimes that seek to curtail the consensual sharing of information and innovation on the Internet.

## II.

## Facebook and Internet Self-Regulation

It is no secret that certain voices in the online community have called for greater government regulation of Internet services, including websites like Google and social-networking services like Facebook. In some instances, these critics have articulated legitimate concerns about the security of user data against the threat of hackers and others. But efforts to ensure data security should not open the door to intrusive government regulation of other aspects of the Internet. Internet services are, by and large, self-regulating and self-correcting. Social networking services in particular have successfully adopted and nurtured robust self-correction mechanisms and will continue to do so in the future. In addition, there are a range of independent resources freely available on the Internet that inform users of how to further control their information and supplement the natural self-corrective tendencies of social-networking sites.

---

[33] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC).

### A. Self-Regulatory Features of the Internet and Social Networking Services

At core, the Internet is an open environment where people share information through a vast network of connections. The Internet's essential nature is about *sharing* and *connectivity*. There is no central decision-maker who decides what is or is not posted on the Internet—its very users drive and create the content. That user-driven structure has only been enhanced by Web 2.0 applications, which encourage a proliferation of user-generated content unconstrained by government or corporate decision-makers.

Because of the fundamental user-based orientation of the Internet, users collectively retain an incredible ability to force service providers to self-regulate—to adapt their policies and interfaces in ways that reflect user demand. And for many of these applications, self-regulation is inherent in their very structure.

One powerful example is the internal mechanisms of commercial service providers such as eBay, Inc. ("eBay") and Amazon, Inc. ("Amazon"). Users of eBay drive what is available for sale and what is purchased, and an internal rating and reporting mechanism ensures that fraudulent or misrepresented transactions are controlled and properly filtered out. As eBay's former CEO Meg Whitman put it, eBay is "a self-regulating marketplace that functions like a free economy."[34] And eBay itself has supplemented that natural self-regulation with cutting-edge technologies that control for potential risks.[35] Amazon's feedback system likewise provides effective self-regulation. Sellers are regularly rated by the community of users, which in turn provides a signal to new potential buyers regarding a seller's reliability.[36] If a buyer discovers that a seller is unreliable, the buyer can bring his or her business elsewhere.

Social-networking sites such as Facebook provide even more effective mechanisms for self-regulation and self-correction. By definition, social-networking sites are open

---

34 Robert D. Hof, *Meg Whitman on eBay's Self-Regulation*, BUSINESSWEEK, Aug. 18, 2003.

35 JEANNE PIA MIFSUD BONNICI, SELF-REGULATION IN CYBERSPACE 159-63 (2008).

36 *See Amazon Feedback FAQ*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html/ref=help_search_1-1?ie=UTF8&nodeId=1161284&qid=1275337333&sr=1-1.

environments, the entire point of which is to enable users to share information and comment on their experiences. These users engage the social-networking medium to connect and share information, but they also play a large role in policing the medium itself. Users who find that Facebook's policies are not conducive to their preferences can simply deactivate or delete their account and choose another social-networking site (or communications medium) with policies more in line with their preferences. Or, indeed, they can use Facebook itself to organize protests against new features they do not like—when Facebook launched its "News Feed" product, 10 percent of Facebook users joined a Facebook group to protest the Feed (some modifications were made and the News Feed is now immensely popular and integral to the Facebook experience). Simply, if a service that exists to enable users to share and communicate causes users to share in a manner they dislike, the service will experience user backlash in the same manner as a movie studio that produces bad movies or a consumer-products manufacturer that begins marketing low-quality goods.

The culture of user empowerment that defines Web 2.0 has itself spawned innovation in the very manner in which sites govern themselves. For example, in February 2009, Facebook established a Notice and Comment procedure that it uses when considering changes to its Statement of Rights and Responsibilities ("SRR") and its Privacy Policy.[37] Now, proposed changes to the SRR and Privacy Policy are posted on Facebook, typically for seven days. Users are encouraged to comment on the proposed changes, and Facebook devotes substantial internal resources to reviewing the comments received. Facebook has, on a number of occasions, modified proposed changes to its SRR and Privacy Policy to address this user feedback; in certain instances, Facebook's terms even call for a user vote before implementing a change. These industry-leading procedures promote transparency, help users better understand the terms of service, and represent an innovative model for user input and self-governance.

User choice is further enhanced by a large community of sophisticated Internet users who devote considerable time to critiquing and improving the social-networking experience. These users leverage their knowledge to organize concerted responses to disfavored policies, create

---

[37] Posting of Mark Zuckerberg to the Facebook Blog, *Governing the Facebook Service in an Open and Transparent Way*, http://blog.facebook.com/blog.php?post=56566967130 (Feb. 26, 2009 2:20 PST).

extensive blogs, user guides, and how-to manuals, and generally drive self-regulation and self-correction. Even a brief perusal of technology blogs and newspapers shows that there has been no shortage of input in recent months on Facebook's policies. That robust debate helps users decide whether they want to continue to be members of the Facebook community or would prefer to join (and in some instances, create) other social-networking communities with different suites of services and options. Social networking services, and the Internet in general, function effectively because users are highly engaged and information flows rapidly and efficiently. Discipline and self-regulation are critical, because if a service does not respond appropriately, users can and will go elsewhere.

And there are plenty of other places to go. For example, users can choose from a menu of social networking choices beyond Facebook. Twitter – which defaults users to open settings that permit anyone on the Internet to view content – is among the fastest growing web-based companies on the planet. Another popular option is LinkedIn, which targets users who are focused on professional networking. MySpace, a predecessor to Facebook, still boasts a large online community and recently made changes to its information-sharing policies in an attempt to distinguish itself from Facebook.[38] A new startup plans to launch a site called Diaspora as an alternative to Facebook. Google Buzz launched earlier this year and, nearly instantaneously, boasted over 100 million users. Users who want to maintain a Facebook account but who wish to take advantage of other social media have the option of maintaining—at no charge—a Facebook account as well as an account with another service. In short, there is no shortage of options for those who want something different than what Facebook offers, and that competitive diversity demands that Facebook continually respond to user preferences.

While the user community and market forces serve to control and police the outer limits of social-networking innovation, there are many independent resources that provide additional protection to users. These resources are another pillar of self-correction. Hundreds, if not thousands, of articles, commentaries, and guides have been produced and disseminated throughout the Internet regarding how to manage one's "online reputation." As to Facebook

---

[38] *MySpace Simplifies Settings as Facebook Criticised*, AFP, May 17, 2010.

specifically, entities ranging from the mainstream media to individual bloggers have produced comprehensive "how to" guides for sharing (and not sharing) information on Facebook.[39] Other services have emerged that will manage a user's online presence, not only on Facebook but throughout the Internet.[40]

All of these tools help make the users of social-networking sites savvy in protecting their information in accordance with their personal preferences. The Pew study found that 57% of adult Internet users monitor their online presence.[41] Among users age 18 to 29, 71% have adjusted their settings and controls to regulate how much they are sharing with others, and 65% of all social-networking site users have done so.[42] If these users feel that a service is overstepping its bounds, they will actively take steps to control their own personal information.

### B. Facebook's Continuing Evolution in Response to User Preferences

As Facebook has blossomed from a small start-up to a service with nearly half a billion users, it has, in response to the self-regulatory pressures described above, continually sought to improve its user interface, its data-sharing policies, and its overall user experience. In 2004, Facebook enabled users to do little more than post basic personal information and share it with their schoolmates. Today, Facebook, together with developers building applications on Facebook Platform, allows users to share political information, to engage in charity fundraising, to develop support networks, to build customized communities of interest, to play games with people from across the globe, and to engage in a host of other social interactions. Facebook's user-driven innovations have transformed it from a primarily college-based network of "friends" into a thriving, open community of individuals who share, group, exchange, and develop information. Its story is one of innovation in action, and it vividly illustrates why it is so

---

39 *See, e.g.*, ANTHONY MAYFIELD, ME AND MY WEB SHADOW: HOW TO MANAGE YOUR REPUTATION ONLINE (2010); MICHAEL FERTIK & DAVID THOMPSON, WILD WEST 2.0: HOW TO PROTECT AND RESTORE YOUR REPUTATION ON THE UNTAMED SOCIAL FRONTIER (2010).

40 For example, SaveFace, Reclaim Privacy, Reputation Defender, DoYouBuzz, Brand-Yourself.com, and many others.

41 MARY MADDEN & AARON SMITH, PEW INTERNET & AMERICAN LIFE PROJECT, PEW RESEARCH CENTER, REPUTATION MANAGEMENT AND SOCIAL MEDIA 8, 21 (May 26, 2010).

42 *Id.*

important for providers of Internet-based applications to remain free to experiment with new approaches.

Because the uses of social-networking sites are largely user-driven, it can be difficult to predict the ways in which new networks and connections on Facebook will develop. For example, recently some communities have begun to apply Facebook to assist with law enforcement. Others have deployed Facebook to advance searches for missing persons. Still others have used the service to alert their friends and neighbors to traffic patterns, discount sales, and neighborhood activities. No one could have predicted these benefits when Facebook began.

The growing multitude of Facebook features reflects a diverse set of needs and preferences among its user base. One study shows that Facebook has drastically increased the ability of users to develop and maintain essential social capital.[43] Another study makes clear that social networking allows for "friendship-driven" and "interest-driven" engagement by youth, allowing for new forms of self-directed and peer-based learning.[44]

Some of Facebook's most popular innovations were initially met with skepticism from privacy advocates and others. For example, Facebook's News Feed faced significant controversy when it was first released in 2006. That feature instantly presents users who log-in to Facebook with a real-time, ambient accounting of all of their connections, prioritized to feature information about the people and subjects the user is most closely connected to. News Feed updates users about events such as the birth of a friend's child, a colleague receiving a prestigious award, a concert by the user's favorite new band, or a news article that a relative has linked as particularly interesting. In response to input from users who feared that sensitive details would be instantly conveyed to all of their friends, Facebook quickly established more

---

43 Nicole B. Ellison, Charles Steinfield & Cliff Lampe, *The Benefits of Facebook "Friends": Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMPUTER-MEDIATED COMM. (2007), *available at* http://jcmc.indiana.edu/vol12/issue4/ellison.html.

44 *See* MIZUKO ITO ET AL., LIVING AND LEARNING WITH NEW MEDIA: SUMMARY OF FINDINGS FROM THE DIGITAL YOUTH PROJECT, THE JOHN D. AND CATHERINE T. MACARTHUR FOUNDATION REPORTS ON DIGITAL MEDIA AND LEARNING (2008).

granular controls over what information would be displayed on News Feed, and News Feed is now viewed as an essential component of Facebook, as any user can attest.

The self-correcting mechanism of user choice has compelled Facebook to constantly re-evaluate and refine its user preferences. As part of that process, Facebook has established some bedrock policies focused on user-protection. Facebook does not sell or share user's personal information with advertisers. And Facebook does not charge users for any of its services or applications. These policies ensure basic user protections, as Facebook does not have a direct monetary incentive to share or sell data to outside parties. Facebook sees these policies as core to Facebook's ability to build and maintain user trust, which Facebook views as indispensable to its ability to compete. Critically, however, other companies with other focuses may choose different strategies. One may require user-generated content to be distributed broadly if at all. Another may in all cases prevent distribution to anyone other than the user's confirmed connections. A third may sell user-generated content to third-party search providers, in the hopes that users will appreciate the broader distribution of their content that comes from search indexing. A fourth may sell information to ad networks, in the hopes that users will appreciate the improved advertising targeting they experience elsewhere on the Internet. The central point is that the proliferation of Web 2.0-based services competing in the marketplace provides users with a broad range of innovative choices today, and—absent a government mandate that supplants the wisdom of the marketplace with regulatory fiat—they will provide users with even more innovative choices tomorrow.

Facebook's recent changes to its controls and privacy policy provide a prime example of how social networking services and Internet-based services more generally have a dynamic ability to respond to users and self-correct. Over the years, Facebook has taken unprecedented steps toward ensuring that users understand what they are sharing and how its various controls interact with their information. In December 2009, Facebook rolled out a new and unprecedented Privacy Wizard, which all users were required to interact with to evaluate and select their privacy settings, before they could continue to use the Facebook service. Also last year, Facebook deployed a "per-object" publisher, which enables users to choose how widely to share on an item-by-item basis. With both innovations, Facebook sought to maximize both

simplicity and control, a delicate balance, while finding the right level of openness for each user and for the Facebook community as a whole.

In response to user reaction to several new products it recently announced, Facebook recently implemented further changes and additions to its controls, again working quickly—in the face of enormous technical complexity—to respond to views expressed in the user community. Facebook's recent changes achieve three primary goals: providing a single control for content (while maintaining its more granular controls for users who want to use them); narrowing the categories of user information that are necessarily public to those essential to provide its core functionality; and offering an easy way for users to "opt out" of Platform and thereby prevent the sharing of user information with applications.

As Facebook moves forward, it will face additional challenges relating to the balance between, on the one hand, user demand for sharing and connectivity and, on the other hand, the ability for users to control who has access to the content they share on Facebook. It also will aim to balance simplicity and ease of use with the learning process that inevitably accompanies technology as it becomes more sophisticated, be it a telephone, a TV remote control, or a computer. The current frontier of Facebook innovation involves its Platform functionality, which allows third-party developers to offer a nearly infinite variety of tools to enhance users' experience both on and off Facebook. With the consent of users, these third-party developers can access the information about users that allows developers to innovate to provide additional features not developed solely by Facebook itself. Hundreds of thousands of games, mobile applications, utilities, and other applications have been created through Facebook Platform.

A recent Facebook change illustrates how the gradual opening up of Facebook to third-party developers can greatly benefit users. When Facebook Platform was first launched in 2007, Facebook imposed a 24-hour data caching rule on developers (meaning they had to submit new requests for user data every 24 hours). Over time, based on feedback from users and developers, it became clear that the 24-hour caching rule was cumbersome, inhibited some applications, and generally deteriorated the user experience. Again seeking to respond to users and remain innovative, Facebook recently announced that it was eliminating the 24-hour caching rule—a

resource-intensive technical restriction—and instead rolling out more strict and nuanced principles and policies governing how developers acquire information from users.

These changes are intended to force developers to adopt and adhere to their own privacy policies, and to request only information that is necessary. Among other things, Facebook imposed granular data permission rules on its developers, requiring applications to request specific permissions from users if and to the extent they require access beyond the users' public information. In other words, just because a user approves a certain application does not mean that the application can access *all* of the user's information. This change took Facebook beyond the industry norm, which is to permit third-party applications to access *all* user information for those users who sign up to use applications. These new requirements give users increased control and awareness and will encourage developers to implement (and adhere to) their own privacy policies, thereby meeting user expectations and avoiding adverse marketplace consequences.

Facebook thus serves as prime example of the tremendous self-corrective tendency of Internet-based applications, particularly with respect to the balance between openness and privacy. Its rapid and continual responses to user feedback about privacy settings has helped it to become a better service while continuing to enhance the user experience and pioneer new ways to share information. And, Facebook's pioneering development of user controls for the information they share is an example for regulators in the U.S. and abroad of how approaches that vest decisionmaking in individual users, rather than in government regulators, is the most promising means of furthering user satisfaction and Internet innovation.

## III.
## Special Considerations Regarding Regulation of Social-Networking Sites

As the Commerce Department and other agencies evaluate regulatory policy toward the Internet, it will be valuable to bear in mind certain unique considerations that apply in the context of social-networking sites.

*First*, by definition, social-networking sites require users to share some information with others, and indeed exist to enable such sharing. Whether it be simply users' names, their images,

their professions, or a broader array of information regarding interests and activities, a social networking service simply cannot function without information sharing. If users were to join Facebook or a similar service, but none had any information visible to anyone except existing friends, it would be impossible for users to find others users or for the network to grow. Two users could not find each other, because there would be no publicly available information. Engaging a social-networking site is, by definition, a public endeavor. To be sure, services like Facebook give users control and limit the information that is necessarily public, but the nature of social networking requires some information to be shared publicly.

*Second*, users have different personal preferences for what information they want to share. That diversity of user demand renders a single legal standard for information-sharing infeasible. Some Facebook users, for example, choose an open policy as their default for the content they share; others restrict it to friends. Many others frequently vary distribution depending on the particular content they are sharing at a given time. Facebook and other social-networking sites have endeavored to give users a host of options—*i.e.*, granularity—to decide precisely what information is shared with whom. For the blunt tool of government regulation to replace that tailored approach with a one-size-fits-all policy would diminish consumer choice and be profoundly anticompetitive. As respected technology columnist L. Gordon Crovitz recently wrote, "[t]echnology now allows people to set their own balance between privacy and the benefits of disclosing information. Social media sites should make it as easy as possible to adjust this dial, but regulations can't possibly replace the individual privacy preferences of hundreds of millions of people being social online."[45] As the Department and other government authorities evaluate Internet policy, they should recognize social networking in particular as an area where user control should predominate over government control.

*Third*, as technologies continue to evolve, the type of information that users desire to share will continue to evolve as well, which weighs against any attempt to establish fixed legal restraints. For example, the capability to post video is a relatively new technological advancement. It is difficult to predict what innovations will come in the future. At the same

---

[45] L. Gordon Crovitz, *Privacy Isn't Everything on the Web*, WALL ST. J., May 24, 2010.

time, Facebook and other social-networking sites are ensuring that information-sharing controls are evolving and adapting with the technology. Facebook's per-object sharing controls are a prime example—a user can now designate a unique set of sharing preferences for a particular type of content (such as photos and videos posted by that user), and can vary that preference for a particular photo or video that the user users wishes to share more or less broadly.

*Fourth*, the *degree* to which users share information has continued to evolve and may change in unexpected ways in the future. Throughout the mid-1990s, the Internet remained mostly a forum for receiving content. At the time, users were very reluctant to engage in financial transactions online. Beginning in the late 1990s, however, users increasingly used the Internet as a means to engage in e-commerce, to the point where, today, online banking is ubiquitous, and where many consumers do the bulk of their buying—from food to furniture, from socks to stocks—online. Likewise, norms regarding behavioral advertising have evolved from deep skepticism and concern to widespread recognition of its benefits.[46] The proliferation of Web 2.0 services represents the next frontier. Increasingly, users value sharing and personal expression, not anonymity, and that trend is extending beyond the borders of social networking sites themselves. The Internet itself is becoming personalized, reflecting an individual's uses, preferences, interests, and social connections. Individuals already can receive a live feed aggregating their friends' activities in various networks, a personalized stream of tailored music based on their friends' musical tastes, and live "tweets" featuring their preferred political groups, candidates, causes, or celebrities. During the 2009 inauguration, Facebook partnered with CNN.com to provide those following the inauguration online an enormously popular live stream of updates featuring users' reactions to that historic event. In that example and many others, users embraced a "social" web—one in which any given user's experience of a popular website featured the social connections of that particular user, and was therefore different from, and more tailored than, the experience of any other user.

Government regulators cannot possibly predict what direction user preferences will go next, or the degree to which users will embrace and enable information-sharing to permit service

---

[46] *See* Leibowitz, *supra* note 15.

providers to meet their needs; any attempt to do so would be flawed at the outset. Attempts to regulate and establish unilateral standards not only would threaten the viability of social-networking sites, but would severely inhibit the innovation and subsequent self-correction that has marked the advance of the Internet over the last two decades—an advance that has been defined by technological developments, entrepreneurship, job creation, and newer, better ways for individuals to interact with the Internet.

*Fifth*, excessive regulation could threaten one of the next great advances in social networking: functionalities like Facebook Platform that allow developers to enhance and expand the functionality surrounding users' social networks. Internet innovation depends on a proliferation of independent developers having the ability to expand upon existing services. Facebook Platform has enabled the development of an entire Platform economy, featuring more than 700,000 applications. To pick just a handful of examples, the *Birthday Calendar* application allows users to track birthdays, anniversaries, and other important dates. The *Circle of Moms* application serves as a local support group for mothers, drawing on the collective knowledge of the community to provide support to a user. And on the charitable front, the *Causes* application provides an online platform for individuals and organizations to raise funds for charitable causes. Other applications allow users to receive their Facebook content on different devices (such as cell phones) or platforms (such as their desktop). Regulation that sought to limit or prohibit the ability of developers to access user information would stifle innovation and drastically reduce the benefits a user can gain from Facebook, and from the Internet as a whole.

*Sixth*, the potential harms from social-networking sites' failing to adequately respond to user preferences are different in kind from the types of harms—like the exploitation of children and financial fraud—that Congress has found justify regulation of the Internet. The FTC's David Vladeck has described interests such as public-health imperatives as "far more weighty,"[47] from a regulatory standpoint, than pure privacy concerns. We understand Director Vladeck to mean not that privacy is unimportant, but rather that the burden of justifying

---

[47] David Vladeck, *The Difficult Case of Direct-To-Consumer Drug Advertising*, 41 LOY. L.A. L. REV. 259, 289 (2007).

significant regulatory action should be comparatively higher. Courts, similarly, have recognized that the unexpected receipt of information by third parties often will not be a subject for legal redress, either because the information was voluntarily shared with others or because no identifiable harm resulted.[48] A legal approach that neglected these familiar principles of the common law and constitutional interpretation would open the door to opportunistic lawsuits by claimants who experienced no actual harm, and might subject promising start-up companies to crushing penalties—or deter entrepreneurial innovation in the first place.

*Seventh*, unlike the regulation of pure financial transactions on the Internet, the regulation of consensual data-sharing by social-networking sites could trigger substantial First Amendment concerns. Social networks are at core an expressive medium. Facebook users share everything from political opinions to photographs to random musings. The First Amendment protects such expression, allowing it to be regulated only when the government has a truly compelling interest.

First Amendment concerns with regulating social-networking sites are not merely academic; the freedom of expression that Facebook's breadth of dissemination encourages has profound real-world consequences. Facebook and other social-networking sites have fulfilled a key democratic function. Because such sites allow users to quickly share information and build communities, democracy advocates in repressive regimes around the globe have found them instrumental to spreading their message and engaging in political action. Facebook and Twitter provided a voice and an expressive medium to the advocates of democracy following the contested Iranian election,[49] and Facebook was famously used by Oscar Morales in Colombia in 2008 to organize massive street demonstrations against the FARC terrorist group.[50] Social-networking sites have played an important role in advancing grassroots democratic movements across the globe.

---

48 *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *United States v. Stults*, 575 F.3d 834 (8th Cir. 2009); *see also Ruiz v. Gap, Inc.*, No. 09-15971, 2010 WL 2170993 (9th Cir. May 28, 2010) (no actual harm to users whose information was exposed by theft of company laptops); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

49 Lev Grossman, *Iran Protests: Twitter, the Medium of the Movement*, NEWSWEEK, June 17, 2009.

50 Sibylla Brodzinsky, *Facebook Used to Target Colombia's FARC with Global Rally*, CHRISTIAN SCI. MONITOR, Feb. 4, 2008.

Here at home, Facebook has had a marked impact on domestic politics. In the 2008 presidential election, YouTube and Facebook cosponsored presidential debates with traditional media outlets such as CNN and ABC News.[51] Some have called the 2008 election the "Facebook Election," noting the service as a key source of grassroots support for President Obama.[52] At the same time, Facebook has become a key platform for candidates for state and local office to get their message out, especially those who otherwise could not afford expensive television and radio airtime. Beyond candidates for office, estimates suggest that over 300 *current* Members of Congress use Facebook in their official capacity.[53]

These political uses of Facebook underscore the serious First Amendment issues that would arise if the government actively regulated the way in which users share information on social networking cites. And of course, the robust First Amendment protections given to non-commercial speech apply to a range of other communications on social-networking sites that are of a non-political nature.

---

51 Brian Stelter, *ABC News and Facebook in Joint Effort to Bring Viewers Closer to Political Coverage*, N.Y. TIMES, Nov. 26, 2007; Virginia Heffernan, *Clicking and Choosing: The Election According to YouTube*, N.Y. TIMES, Nov. 14, 2008.

52 Matthew Fraser & Soumitra Dutta, *Barack Obama and the Facebook Election*, U.S. NEWS AND WORLD REP., Nov. 19, 2008.

53 Posting of Tony Romm to The Hill, *'Congress on Facebook' Goes Live*, http://thehill.com/blogs/hillicon-valley/technology/97683-congress-on-facebook-goes-live (May 13, 2010 7:58 EDT).

## IV.
## Conclusion

The Internet is among the most important innovations of our time. Nowhere has it been as vibrant as in the United States, where its growth and the at-times dazzling creativity it has spawned are due in part to a consistent, bipartisan congressional preference for limiting government regulation of the Internet to only specific, tailored circumstances.

The government nonetheless has an important role in supervising certain activities on the Internet, including fraudulent and abusive practices, especially when directed at children. The success of the Internet to date, however, counsels great caution before pursuing a more interventionist government role in the future. Internet services—and users' attitudes toward the Internet—are evolving more rapidly and in different directions than the government could ever predict or appropriately capture in a regulation. That is particularly true for social-networking sites. These services do not involve economic activities of a type the government has an established track record of regulating. Likewise, norms for "protecting" data and shielding it from disclosure cannot supply the predicate for regulating networks where individuals post messages, images, and ideas on the Internet with the very purpose of sharing. Ultimately, constitutional values suggest restraint before instituting government-imposed presumptions about how and when Internet users may share information with one another.

As the Commerce Department and other agencies take stock of the growth and uses of the Internet, and the innovation and American jobs that Web 2.0 and other technology companies are creating, they should make note of the robust mechanisms on the Internet itself for monitoring, self-correction, and disciplining unwelcome practices. If social-networking sites take steps that users oppose, they will lose users and suffer in the highly vocal Internet court of public opinion. A range of outside services and critics exist to observe the practices of social-networking sites, to suggest improvements, and to help users make the most of sites that—as they become more sophisticated—inevitably will take more time to master than when they were first introduced. Technology also can enhance companies' ability to increase user control over the information they share, as reflected in recent changes on Facebook. And, while user control is preferable to government fiat, the government and consensual standard-setting organizations

can play a valuable role in promoting "best practices" that enhance users' experience and control while preserving the innovation and freedom that are the Internet's lifeblood.

Respectfully submitted,

_____

Eugene Scalia
John F. Bash
Gibson, Dunn & Crutcher LLP
1050 Connecticut Ave. NW
Washington, DC 20036

*Counsel for Facebook, Inc.*


June 9, 2010

***By Electronic Delivery***

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Re: Information Privacy and Innovation in the Internet Economy

Ladies and Gentlemen:

This comment letter is submitted on behalf of the Financial Services Forum (the "Forum") in response to the Department of Commerce ("Commerce") Internet Policy Task Force's Notice of Inquiry ("Notice") relating to privacy and the Internet economy, published in the Federal Register on May 10, 2010. The Forum is a non-partisan financial and economic policy organization comprising the CEOs of 19 of the largest and most diversified financial services institutions doing business in the United States. In this letter, the Forum has addressed those issues that are of particular importance to financial institutions. We appreciate the opportunity to comment on this important matter.

**The U.S. Government Should be Sensitive to Overly Broad Regulation**

As the U.S. government considers privacy and the Internet, it is critical that the government is sensitive to ensuring the delicate balance between innovation and regulation. An overly prescriptive regulatory regime would likely stifle innovation without truly protecting consumer privacy interests. Moreover, such a result could place U.S. companies at a competitive disadvantage with respect to their global competitors.

An example of this disadvantage can be seen in restrictions on cross-border data transfers of personal information that have provided little, if any, meaningful benefit to consumers, while imposing substantial costs on businesses and governments. As the world has grown more globally connected, restrictions on cross-border data transfers have become outmoded.

Complex, global data flows are necessary in order for businesses to provide the services that their customers expect, as well as to manage their operations in an efficient and cost effective manner, such as to obtain the benefits derived from centralized data servers or company-wide portals. In fact, global data flows are now a common and essential component of our daily lives. For example, when travelling abroad, information must flow across borders in order for individuals to use ATM cards, including to authorize transactions, and banks must maintain the necessary information technology to allow customers to do so. Similarly, when a fraudster located in another country tries to use a credit card for an unauthorized purchase, information must be able to flow across borders in order to prevent such fraud. The benefits of these data flows are passed on to consumers in many forms, including, for example, enhanced customer services (*e.g.*, 24-hour customer hotlines) and a greater choice of products and services at lower prices. Countries, in turn, benefit from increased global business investments and activity. All in all, consumers, businesses and governments receive enormous benefits from global flows. Countries that limit cross-border data flows or impose highly regimented privacy regimes impose significant costs on their economies, including the substantial costs associated with compliance for those businesses that continue to operate within those countries and the costs of business opportunities lost to other countries in the increasingly competitive global technology-driven information-based economy. Those costs disproportionately outweigh the limited benefits that the laws actually provide.

Businesses seek to offer consumers a wide array of goods and services at competitive prices and to promptly meet and respond to their customers' needs. To do so, businesses need to manage their global operations effectively. This may include, for example, centralizing certain functions for the organization (*e.g.*, a central database for processing the organization's human resources data). Also, today's technology allows businesses to allocate resources more effectively, including, for example, dividing work among employees and contractors located around the world so that work can be accomplished around the clock following the sun. In order to do so, a business must be able to transfer both non-personal information, such as analytical data, as well as personal information, such as customer and employee data, to their operations around the world.

While such transfers are necessary to manage the business in an efficient manner, they also permit the organization to offer services to its customers. For example, by relying on service representatives from different time zones throughout the world to "come online" at different times, a business can provide customer service to assist customers who may be located halfway around the world. To be effective and convenient for the customer, these service representatives must have access to the organization's databases containing customer information, such as a customer's credit, purchase or other transaction records. They also need access to the organization's employee data so they can, direct any required follow-up service to the correct office.

It is also important to note that large multi-national businesses rely on global data flows in order to comply with legal and regulatory obligations and for risk control and fraud prevention activities. For global financial institutions, in particular, moving and centralizing data around the world is critical in order to effectively identify, assess, monitor and manage credit, operational and other risks. Moreover, global data flows are essential for financial institutions to prevent fraud, money laundering and terrorist financing. Financial institutions must also frequently rely

on global data flows to share information as required or permitted by law (*e.g.*, in connection with litigation, for regulatory examination purposes, and to conduct internal investigations). In fact, existing U.S. privacy laws include exceptions to limitations on sharing that recognize the critical need to ensure these types of data flows. *See*, *e.g.*, 15 U.S.C. §§ 6802(e)(3), (4), (8) (GLBA); 15 U.S.C. §§ 1681b(a)(1), (4)-(6), 1681u, 1681v (FCRA).

Limitations on the free flow of information or rules that require over-notification and impose unnecessary burdens will have an adverse effect on innovation, will limit the choices provided to consumers, impede the ability to comply with law and control criminal activity and make it more difficult for U.S. companies to compete against their global counterparts.

**A Sectoral Approach to Privacy is Appropriate**

The U.S. model for regulating business practices is rooted in a recognition that overly broad regulation adversely impacts businesses and, in turn, the economy. This has led to a reluctance to regulate business practices absent a demonstrated need. As a result, Congress tends to adopt legislation to address specific instances of abuse, all while protecting important national interests, whether those be related to maintaining or bolstering a vibrant economy or maintaining accurate and meaningful information about consumers that is critical to commerce (*e.g.*, ensuring the availability of credit report information for legitimate and appropriate purposes, as discussed below).

As a result, the U.S. has concluded that an omnibus or "one-size-fits-all" legislative approach to privacy lacks the necessary precision to avoid interfering with the benefits that follow from the free flow of information, as well as the benefits to the national economy that are derived from entities that are regulated at the national level, such as financial institutions.

Instead, the U.S. approach to privacy (comprised in a number of statutes) focuses on particularly significant privacy interests. These privacy interests may relate to particularly sensitive types of information, such as information about children, or about inappropriate uses of information, such as abusive e-mailing. Thus, the landscape of U.S. privacy law is quite broad and varied. The following are examples of U.S. privacy laws that protect important consumer privacy interests:

- children's personal information (Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.*);
- consumer telephone information (Telephone Consumer Protection Act, 47 U.S.C. § 227);
- consumer e-mail information (CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*);
- personal information collected by cable companies (Cable Communications Policy Act, 47 U.S.C. § 551);
- personal information collected by telephone companies (Customer Proprietary Network Information, 47 U.S.C. § 222);

- computer information (Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq*.);

- credit report information and information shared among affiliated companies (Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*.);

- information relating to customers of financial institutions (Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq*.);

- health information (Title II of the Health Insurance Portability and Accountability Act, Pub. L. No. 104-191);

- driver's license information (Driver's Privacy Protection Act, 18 U.S.C. § 2721 *et seq*.); and

- information about sex, race, color, religion and marital status (Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq*., Equal Employment Opportunity Act, 42 U.S.C. § 2000e *et seq*. and Fair Housing Act, 42 U.S.C. §§ 3604-3605);

- student information (Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g);

- employee polygraph information (Employee Polygraph Protection Act, 29 U.S.C. § 2001 *et seq*.);

- employee retirement information (Employee Retirement Income Security Act, 29 U.S.C. § 1025);

- mail (39 U.S.C. § 3623);

- communications by debt collectors (Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq*.); and

- video rental information (Video Privacy Protection Act, 18 U.S.C. § 2710).

This sectoral approach appropriately focuses on limiting inappropriate use of information, while ensuring privacy and enhancing deeply rooted traditions, including both free information flows and avoiding overly broad regulation. For example, the U.S. should continue to rely on business's public declarations concerning their privacy practices (*e.g.*, privacy notices), reinforced by government enforcement to ensure that businesses actually implement and follow their privacy promises. Where the government must intervene, it should only do so where it determines that particularly sensitive privacy interests of individuals are not otherwise being sufficiently protected and then only in a way that is narrowly tailored to protect those interests (the approach used in the various federal privacy statutes listed above, as well as those discussed in greater detail below).

**U.S. Law Provides Consumers with Substantial Protections for Financial Privacy Under a Sectoral Approach**

One area of U.S. privacy law that has historically received substantial federal oversight is financial privacy. Of the various types of personal information relating to consumers, consumer financial information has generally been deemed particularly sensitive and, as a result, deserving of greater protection. Consistent with the approach to federal privacy legislation described above, Congress has enacted numerous measures that are narrowly tailored to protect specific privacy interests, but that also take into account the business realities of how financial institutions operate. Existing federal protections for consumer financial information are robust, including, for example, privacy protections in the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), the Electronic Funds Transfer Act, the Equal Credit Opportunity Act, and the Fair Credit Billing Act.

As a result, financial institutions are subject to a detailed array of privacy obligations and limitations with respect to consumer financial information. The laws that comprise the rigorous privacy regime to which financial institutions are subject are designed to complement each other and work together. For example, these laws recognize the unique holding company structure within which many, if not most, financial institutions operate.

It is important to note that these financial privacy laws have been the subject of congressional and regulatory debate and refinement over the past 40 years (dating back to the enactment of the FCRA in 1970). Over time, where Congress or federal regulators have identified new issues requiring financial privacy protection, they have stepped in and provided that protection. For example, in 2003, Congress amended the FCRA to address the use of certain types of information shared among affiliated entities for marketing purposes.

The various financial privacy laws are working as intended, balancing the legitimate and appropriate needs of financial institutions for free flow of information and the actual business realities of how financial institutions operate against consumer privacy interests. There is no need to abandon or replace this comprehensive scheme of financial privacy laws that has been tailored by Congress and financial regulators over decades to protect consumers' financial privacy.

The federal government should continue to support a sectoral model that is customized to specific industry sectors or specific types of information. In fact, the method of regulating financial institutions may be a model for, and could be extended to, other sectors. The focus of financial regulation is not on limiting the collection of personal information or on providing notice to consumers regarding each use of information made by the financial institutions. Rather, the focus is on ensuring that personal information is used only for appropriate purposes and that the use of personal information in areas of particular consumer sensitivity, such as sharing of personal information with non-affiliated third parties, are limited where appropriate or subject to consumer choice. The GLBA and FCRA are two examples of laws regulating the financial sector that have struck the delicate balance between regulation and innovation.

*Gramm-Leach-Bliley Act*

The GLBA is one of the cornerstones of U.S. law that protects consumer financial privacy. The GLBA includes detailed and comprehensive limitations on the ability of financial institutions to share their customer information with nonaffiliated third parties. For example, the GLBA prohibits a financial institution from sharing personal information relating to a customer with a nonaffiliated third party, unless the institution has provided the customer with a copy of its privacy notice and an opportunity to opt out of sharing.[1] 15 U.S.C. § 6802(a). This opt-out right allows consumers, for example, to prevent financial institutions from sharing their information with nonaffiliated third parties that would use the information to market to the consumers. Nonetheless, the statute includes sensible exceptions to this limitation that take into account appropriate and necessary sharing of information, including, for example, to process transactions requested by consumers, for third parties to perform services, to prevent fraud, for risk control, to comply with legal obligations, to comply with subpoenas and summonses, and to respond to judicial process. *See* 15 U.S.C. § 6802(e).

Moreover, the requirement that a financial institution provide its customers with a privacy notice is not a one-time disclosure. Instead, a financial institution must provide its customers with a copy of its privacy notice initially at the time of establishing the customer relationship and then not less than annually thereafter during the course of that relationship. 15 U.S.C. § 6802(a). In another example of Congress and regulators updating the financial privacy laws over time, the federal agencies responsible for enforcing the GLBA, recently issued a model privacy notice that financial institutions may use. *See* 74 Fed. Reg. 62,890 (Dec. 1, 2009). The model was developed over the course of five years, in which the agencies conducted extensive qualitative and quantitative testing with consumers. The agencies' goal was "to identify barriers to consumer understanding of current privacy notices and to develop an alternative . . . that consumers could more easily use and understand." *Id*. at 62,893. As a result, the financial regulators have gone to great lengths to develop a model privacy notice that they believe is understandable. In so doing, the financial regulators appear to have reaffirmed their belief that a properly tailored notice that is given at the inception of the relationship and annually thereafter is appropriate and strikes the right balance.

The GLBA is not limited to the privacy of financial information; it also addresses the security of such information. In this regard, the GLBA requires that each financial institution implement a comprehensive, written and risk-based information security program that is designed to safeguard customer information. Specifically, a financial institution must develop, implement, and maintain a written, comprehensive information security program that includes administrative, technical, and physical safeguards that are designed to protect the financial institution's customer information. *See*, *e.g.*, 12 C.F.R. pt. 30, App. A (OCC). These safeguards extend to all handling of customer information by a financial institution. Moreover, the federal banking agencies require that banks also implement programs to respond to security incidents involving customer information, including notifying customers where appropriate. *Id.*

[1] It is important to note that the scope of the information to which this privacy protection extends is not limited, but is in fact quite broad. Specifically, the GLBA applies with respect to personally identifiable information that a consumer provides to a financial institution, that results from a transaction with, or a service performed for, a consumer or that is otherwise obtained by a financial institution. 15 U.S.C. § 6809(4).

*Fair Credit Reporting Act*

The FCRA was enacted in 1970 to address a specific concern—dissemination of incorrect consumer credit reports. In this regard, the FCRA regulates, among other things, the disclosure of credit report information by the consumer reporting agencies that aggregate this information and the use of this information by businesses, including, for example, financial institutions (*e.g.*, banks, insurance companies, and broker-dealers), utilities, landlords, and employers. Nonetheless, the FCRA begins with the express premise that the availability of fair and accurate credit report information is critical to the U.S. economy; stating specifically that the "banking system is dependent upon fair and accurate credit reporting." *See* 15 U.S.C. § 1681. For this reason, the FCRA permits the use of credit report information without consumer consent, but imposes strict limitations on who may obtain credit report information and the purposes for which the information may be used (*i.e.*, a narrow and statutorily defined set of uses, including, for example, determining a consumer's eligibility for credit, insurance, or employment). *See* 15 U.S.C. § 1681b(a). Moreover, the FCRA includes robust mechanisms to ensure that this information is accurate. These mechanisms include requirements that consumers be provided with access to information that is maintained and disseminated about them and the right to respond to information they believe to be inaccurate. *See, e.g.*, 15 U.S.C. §§ 1681g, 1681i, 1681m, 1681s-2. Among other things, the FCRA provides that, if a consumer suffers an adverse action based on credit report information (*e.g.*, a denial of credit, insurance or employment based on a credit report), the entity taking the action is required to notify the consumer of the action, identify the consumer reporting agency that provided the information and provide the consumer with a right to a free copy of that information. *See* 15 U.S.C. § 1681m(a). Consistent with its purpose, the FCRA provides consumers with the ability to limit the sharing and use of credit report information. *See* 15 U.S.C. § 1681a(d)(2)(A)(iii).

It is important to note that, in crafting the financial privacy laws, Congress and the regulators have struck a balance. In their judgment, every law need not provide the same rights and obligations. In some laws, such as the FCRA, access and correction rights are provided to ensure that information is accurate. In certain instances, the regulators have determined that other means of providing transparency and the opportunity for correction are appropriate (*e.g.* the issuance of periodic statements). Just as there is not one right answer for notice across every sector and every medium, so too lawmakers and regulators must have flexibility in determining which rights and obligations are appropriate for different situations.

*Federal Agencies Examine and Enforce Compliance with Financial Institutions' Privacy Obligations*

As indicated above, the GLBA and the FCRA comprise only two of the important financial privacy laws with which financial institutions must comply. In this regard, it is important to highlight that financial institutions are subject to a robust and mature regulatory model that is designed to ensure that financial institutions comply with their privacy obligations and with their publicly stated policies and procedures, including, for example, their GLBA privacy notices. Financial institutions have an existing and long-standing legal and regulatory oversight structure relating to privacy. In this regard, financial institutions are subject to detailed and rigorous examination and supervision by their functional regulators with respect to the various privacy requirements and limitations to which they are subject.

The following example of the examination and enforcement structure for national banks gives a sense of this regulatory oversight. Pursuant to the National Bank Act ("NBA"), the Office of the Comptroller of the Currency ("OCC") charters, regulates and supervises all national banks. The NBA directs the OCC to "examine every national bank." 12 U.S.C. § 481. The NBA further provides the OCC with the power "to make a thorough examination *of all the affairs* of [a national] bank." *Id*. (emphasis added). As a result, when an OCC examiner examines a national bank for compliance with, for example, the privacy obligations of the GLBA and the FCRA, the examiner will review the bank procedures designed to comply with its obligations. Moreover, the examiner will review the institution's privacy notice, its information security program, its incident response program and its FCRA affiliate sharing and affiliate marketing notices and related documentation.

If a particular harm is perceived with respect to the use of information collected over the Internet, it would be appropriate to craft specific oversight, regulation or legislation designed to address that harm, rather than create omnibus legislation that would supplant the sectoral system that has worked well. Financial institutions are required by federal law, including, for example, the FCRA and GLBA, to have robust and well-documented policies and procedures relating to the privacy and protection of personal information. These laws have been the subject of congressional and regulatory debate and refinement over the past 40 years. Because these existing financial privacy laws are effective and strike the right balance between transparency and efficiency, they should not be abandoned or replaced. If the decades worth of refinement that has gone into crafting these privacy protections is abandoned or replaced in favor of a new model, the significant costs that would be imposed on financial institutions to revise their privacy practices and disclosures would likely far outweigh any limited benefit.

**A Use-Based Approach Runs the Risk of Harmful Unintended Consequences**

Commerce's Notice suggests that a use-based approach may be considered as an alternative to the notice and choice model. A use-based approach is particularly difficult to implement by decentralized organizations that interact with consumers and customers through multiple and diverse platforms, channels, and venues and, therefore, needs careful consideration.

It is not clear that the use-based system that Commerce references in its Notice is a true alternative to a notice and choice system. For example, the proposed use-based approach appears to simply "move" the trigger for notice and choice from the time of collection to the time of use. As posited by Business Forum for Consumer Privacy, the use-based approach continues to rely on notice and choice, but rather than provide the notice and choice at the time of collection, notice and choice are provided for nearly each new use.

Moreover, to the extent that a use-based model is considered, it should take into account consumer expectations. In this regard, many uses of personal information should not result in notice. For example, if a bank or its service provider uses its customer's personal information in order to prepare and mail the customer her monthly statement, notice should not be required. This notice would not be meaningful to the customer. Rather, when a consumer opens a checking account, she not only expects but wants her bank to use her information to provide her with important information regarding her account. Similarly, notice should not be required for

other necessary and important uses, such as to prevent fraud, for risk control and to comply with legal requirements.

Notifying the customer of such use will likely result in over-notification which would cause the customer to overlook the notices that really matter. If a bank were required to provide notice for nearly every use of information, not only would it be extremely difficult to implement, but its customers might well receive more than a hundred notices a year (from the bank alone) to take into account all the various legitimate and appropriate bank uses of information, *e.g.*, to verify customers' identities, underwrite applications, process transactions, prepare and provide monthly statements, ensure funds are available, route customer service calls, prevent fraud, and perform credit risk analysis. Needless to say, consumers over time begin to ignore similar and frequent notices that they receive. If a consumer receives nine notices of a business use of her information that are consistent with the service she has requested (*e.g.*, to process her transactions), she is not likely to focus on the tenth notice. Moreover, to the extent that consumers actually try to make sense of this plethora of notices, it is unlikely that they would make any meaningful privacy decisions based on those notices. Under the use-model, consumers would be literally inundated and overwhelmed with notices from hundreds of businesses nearly every time there is a new use of the information. As a result, Commerce should be cognizant of over-notification and the diminution to the value of notification that such over-notification causes.

The sectoral approach is appropriate because it focuses on limiting inappropriate uses of information and protecting particularly sensitive types of information. If there is an unaddressed issue, the government should determine if particularly sensitive privacy interests of individuals are not otherwise being sufficiently protected and then should intervene only in a way that is narrowly tailored to protect those interests. There are legitimate concerns that a use-based model cannot be narrowly tailored and crafted in a similar way.

**Identifying and Fixing the Internet Problem**

No matter what type of approach is ultimately adopted with respect to the Internet, one must begin by identifying the privacy interests that are not being sufficiently protected in the online world. After identifying the "problem," consistent with the U.S. approach to regulating privacy described above, a solution that is narrowly tailored to protect those interests should be identified; it is not necessary to adopt an omnibus, one-size-fits-all privacy "solution" that would stifle innovation and increase compliance costs for business. In considering these issues, it may be found that there are varied solutions. In the past when Congress perceived a specific type of information required protection (*e.g.*, information about children or genetic information ) and when Congress viewed certain uses of information as inappropriate (*e.g.*, discrimination), Congress has a proven track record of enacting legislation to address the specific issue in a narrowly tailored fashion.

In the end, a one-size-fits-all approach that requires notice at the point of collection or for each use would likely prove counterproductive, because consumers would literally be overwhelmed with notices by hundreds of companies. Instead, as indicated above, the federal government should continue to support a sectoral model and should remain committed to ensuring personal privacy through a variety of means that also reflect its deeply rooted tradition of enhancing the

free flow of information and avoiding overly broad regulation and its unintended, but harmful, consequences.

Moreover, the government should be cognizant of the privacy laws that are currently in place, including the comprehensive protections that federal law provides for consumer financial information. The various financial privacy laws are working as intended, balancing consumer privacy interests with the legitimate and appropriate needs of financial institutions for access to information and the actual business realities of how financial institutions operate. There is no need to abandon or replace this comprehensive scheme of financial privacy laws that has been tailored by Congress and financial regulators over decades to protect consumers' financial privacy because of particular issues with respect to the Internet.

* * * *

We appreciate the opportunity to comment on this important matter. If you have any questions concerning these comments or if we can otherwise be of assistance in connection with this matter, please do not hesitate to contact me.

Sincerely,

Mark Schuermann
Senior Vice President for Government Relations
Financial Services Forum

**Before the**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**U.S. DEPARTMENT OF COMMERCE**
**Washington, D.C. 20230**

| | | |
|---|---|---|
| In the Matter of | ) | Docket No. |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | 100402174-0175-01 |
| | ) | |

**COMMENTS OF THE**
**FEDERAL TRADE COMMISSION**

## Introduction

The Federal Trade Commission ("FTC" or "Commission") appreciates this opportunity to comment on the Department of Commerce's ("Department") Notice of Inquiry on Information Privacy and Innovation in the Internet Economy ("Notice"). Currently, the FTC is exploring many of the same issues raised in the Notice as part of a recently concluded series of public roundtables on privacy and 21st century technology and business practices. These roundtables are part of an ongoing effort by the Commission to re-examine approaches to privacy, particularly in light of recent technological developments. The FTC plans to publish its initial privacy proposals later this year for public comment. The information gathered at these roundtables bears directly on the Department's inquiry.

The FTC is an independent administrative agency charged with promoting consumer protection, competition, and the efficient functioning of the marketplace. The keystone of the FTC's law enforcement mission is Section 5 of the FTC Act, which encompasses a wide range of business practices, including practices relating to both consumer privacy and business competition. Section 5 authorizes the FTC to challenge "unfair methods of competition," including violations of the antitrust laws, and "unfair or deceptive acts or practices in or affecting commerce."[1]

The Commission uses its Section 5 authority to address companies' privacy practices relating to the collection, use, and security of consumers' personal information. In addition, under the Gramm-Leach-Bliley Act,[2] the Commission has implemented rules requiring financial privacy notices and the administrative, technical, and physical

---

1 15 U.S.C. § 45(a).

2 15 U.S.C. §§ 6801-09, 6821-27, Pub. L. No. 106-102, 113 Stat. 1338 (1999). For more information on the FTC's role in enforcing the Gramm-Leach-Bliley Act, see FTC, The Gramm-Leach-Bliley Act, http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

safeguarding of personal information. The Commission also protects consumer privacy under a variety of other statutes, including the Fair Credit Reporting Act,[3] the Children's Online Privacy Protection Act,[4] and the CAN-SPAM Act.[5] The Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act") further enhances the Commission's ability to cooperate with foreign enforcement authorities in addressing cross-border privacy violations.[6]

## I. Promoting Innovation and Information Privacy through Competition and Consumer Protection Policies

As the Department's Notice observes, there is an important and mutually reinforcing relationship between competition policies and consumer protection policies in the context of privacy protection. Together, they benefit consumers by fostering new products and services, lower prices, and increased consumer confidence while conducting activities online.

Competition pressures producers to innovate by offering consumers the most attractive array of choices with respect to price, quality, and other options. Competitive firms constantly search for superior profit opportunities as they seek to win the favor of customers, who effectively vote with their dollars for preferred products and services. The U.S. Supreme Court has recognized that the benefits of competition go beyond lower prices and also extend to other dimensions, including the development of new products and services that will benefit consumers. "The assumption that competition is the best method of allocating resources in a free market recognizes that *all elements of a bargain - quality, service, safety, and durability* - and not just the immediate cost, are favorably affected by the free opportunity to select among alternative offers."[7]

At the same time, consumer protections promote informed consumer decision-making and require sellers to honor promises made about their offerings. In other words,

---

[3] 15 U.S.C. § 1681 et seq. For more information on the FTC's role in enforcing the Fair Credit Reporting Act, see FTC, Fair Credit Reporting Act, http://www.ftc.gov/os/statutes/fcrajump.shtm.

[4] 15 U.S.C. §§ 6501-6506, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998). For more information on the FTC's role in enforcing the Children's Online Privacy Protection Act, see FTC, The Children's Online Privacy Protection Act, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

[5] 15 U.S.C. §§ 7701-7713, Pub. L. No. 108-187, 117 Stat. 2699 (2003). For more information on the FTC's role in enforcing the CAN-SPAM Act, see FTC, Spam, Rules & Act, http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm.

[6] Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)). For more information on the FTC's role in enforcing the U.S. SAFE WEB Act, see FTC, THE U.S. SAFE WEB ACT: THE FIRST THREE YEARS, A REPORT TO CONGRESS (2009), *available at* http://www.ftc.gov/os/2009/12/P035303safewebact2009.pdf.

[7] *Nat'l Soc'y of Prof'l Eng'rs v. United States*, 435 U.S. 679, 695 (1978) (emphasis added); *accord, FTC v. Superior Court Trial Lawyers Ass'n*, 493 U.S. 411, 423 (1990).

strong consumer protection policies enable and clarify consumer choices by prohibiting firms from engaging in unfair or deceptive acts or practices and, thus, reinforce competition on the merits.

As the Department's Notice explains, the mutually beneficial relationship between innovation, which is driven by competition, and consumer protection policies applies forcefully to the dynamic Internet context. This relationship between competition and consumer protection policies is critical to facilitating the development and consumer use of the content and applications enabled by the Internet's infrastructure. Indeed, privacy practices may be an important factor that influences consumers' choices among competing products and services. In turn, competitive pressures can push companies to tailor their privacy practices more closely to what consumers desire in order to attract and retain them as customers. The Commission recognizes that inadequate protection of personal information and data security in the Internet context could hamper consumer confidence and undermine the Internet's benefits. For these reasons, the Commission often reviews acts and practices in the Internet area from both a competition and consumer protection perspective including, for example, how consumer protection considerations may affect the competitive analysis of various practices.

## II. FTC Activities Relating to Online Privacy and Security

The FTC has made online privacy one of its highest consumer protection priorities for more than a decade. As technology has evolved, the FTC's goals have remained constant: to protect consumers' personal information and to ensure that consumers have the confidence to take advantage of the many benefits offered by the ever-changing online environment.[8] The Commission has sought to achieve these goals through law enforcement, consumer and business education, and policy initiatives.

First, enforcement remains the bedrock of the Commission's privacy program. For example, since 2001 the FTC has brought almost 30 cases challenging business practices that allegedly failed to adequately protect consumers' personal information.[9] These cases emphasize the importance of protecting consumers' data against common security threats and the need for businesses to evaluate their security procedures on an ongoing basis. Most recently, for instance, the entertainment company Dave & Buster's agreed to settle FTC charges that it left consumers' payment card information vulnerable to hackers. The Commission alleged that the company, among other things, failed to use appropriate firewalls or to limit access to its computer networks through wireless access points, resulting in breaches that led to several hundred thousand dollars in fraudulent charges.[10] In another recent enforcement action, the FTC settled charges against Sears

---

[8] *See generally* FTC, Privacy Initiatives, http://www.ftc.gov/privacy/index.html.

[9] *See id.*

[10] *See generally* Press Release, FTC, Dave & Buster's Settles FTC Charges it Failed to Protect Consumers' Information (Mar. 25, 2010), *available at* http://www.ftc.gov/opa/2010/03/davebusters.shtm.

alleging that company failed to disclose adequately the scope of personal information it collected from consumers via a downloadable software application. The settlement calls for Sears to stop collecting data from the consumers who downloaded the software, to destroy all data it had previously collected, and not to engage in similar conduct in the future.[11]

Second, the Commission actively seeks to educate consumers and businesses about privacy and security issues.[12] For example, it sponsors the site OnGuardOnline.gov, which provides practical tips from the federal government and the technology industry to help consumers guard against Internet fraud and protect the security of their computers and personal information. As an example of business education, the Commission recently released a guide for businesses on how to address the security risks associated with peer-to-peer ("P2P") file-sharing software.[13]

Third, the Commission is actively engaged in policy initiatives to improve consumer privacy. For example, the FTC staff has promoted self-regulation in the context of behavioral advertising, the practice of tracking consumers' online activities for the purpose of serving them with targeted advertisements. Behavioral advertising offers potential benefits for consumers in the form of free or subsidized online content and more relevant advertising. However, it also raises important privacy concerns, including the invisibility of the practice to consumers, the potential for companies to develop and store detailed profiles about consumers, and the risk that the data collected for behavioral advertising – including sensitive data regarding health, finance, or children – could fall into the wrong hands or be used for unanticipated purposes.

In the fall of 2007, the Commission held a town hall meeting to explore the privacy implications of online behavioral advertising. Following this meeting, staff issued a set of proposed self-regulatory principles for public comment and, after receiving over 60 comments, issued a final report on the subject in February 2009. The FTC's behavioral advertising principles emphasize the importance of transparency and consumer choice. In response to the FTC's efforts, some industry organizations have developed new self-regulatory principles for online behavioral advertising. A number of companies also have instituted new policies and procedures to inform consumers about online tracking and provide consumers with additional protections and controls over these practices. Such developments include new tools to allow consumers to opt out of receiving targeted online advertisements. The Commission will continue to encourage self-regulation and monitor progress in this area.

---

[11] *Sears Holdings Mgmt. Corp.*, FTC File No. 082-3099 (final order Aug. 31, 2009).

[12] *See generally* FTC, ID Theft, Privacy, & Security, http://www.ftc.gov/bcp/menus/consumer/data.shtm.

[13] FTC, Peer-to-Peer File Sharing: A Guide for Business, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm.

Most recently, the FTC has hosted a series of day-long roundtables to review consumer privacy issues more broadly. The purpose of the roundtables was to explore how best to protect consumer privacy while supporting beneficial uses of consumer data and technological innovation.[14] The roundtable record is discussed in more detail below.

## III. The U.S. Privacy Framework Going Forward

The Department's Notice raises a series of questions regarding the current status of the U.S. privacy framework and whether there are modifications that would better support innovation, fundamental privacy principles, and evolving consumer expectations. The issues raised in the Department's Notice are very similar to the ones that Commission staff has been examining as part of its roundtables, in which the Department participated. In its Notice, the Department specifically cites these roundtables as an example of the reassessment of approaches to privacy that are currently taking place both domestically and globally, given the ongoing changes in the information economy.

The Commission began the roundtable discussions because of concerns that existing approaches to consumer privacy have practical limitations. For example, the current privacy framework in the United States is based on companies' issuance of long, complicated privacy notices that purport to explain the companies' privacy practices and consumers' choices regarding how their information is used. In reality, we have learned that many consumers do not read, let alone understand, such notices, limiting their ability to make informed choices. In addition, the emergence of new business models, such as social networking, raise new challenges in ensuring that privacy practices are transparent to consumers and consistent with their reasonable expectations. One of the key goals of the roundtables has been to explore how best to ensure consumer privacy in this changing environment.

The Commission gathered a wealth of information from academics, industry representatives, government officials, and consumer groups who attended the roundtables. Discussions focused in detail on the collection and use of data in several specific contexts, including behavioral advertising, information brokering, social networking, cloud computing, and the use of mobile devices.

Participants debated the parameters of what constitutes "sensitive" consumer information and whether such a concept, in fact, can be defined objectively or whether it is purely a subjective construct. They also explored possible ways to reconcile the privacy interests of individuals with other societal goals, such as improving public health through the aggregation of health-related information. Further, discussions at the roundtables focused on various models for managing the privacy and security of consumer information, including: fair information principles, sector-specific regulation,

---

[14] More information about the Privacy Roundtables can be found at FTC, Exploring Privacy, A Roundtable Series, http://www.ftc.gov/bcp/workshops/privacyroundtables/.

self-regulation, and approaches that would enable individuals to apply their privacy preferences themselves.

Several important themes emerged from these roundtable discussions. First, experts confirmed that consumers generally do not understand data collection practices and are largely unaware that there may be companies collecting and analyzing their data for use by other companies. Second, participants noted that consumers should have greater control over their privacy without undue burdens, such as having to spend considerable time reviewing dense privacy disclosures. Third, it may be reasonable and useful to distinguish between data practices that raise genuine privacy concerns and those that do not. Fourth, protecting consumers' privacy should not stifle marketplace innovations that consumers genuinely desire. Fifth, an improved privacy framework should be both flexible enough to accommodate diverse business models and also simple enough to provide clear norms and expectations. The Commission will take into account all of the comments it received through the roundtable process as it develops initial recommendations on privacy later this year.

In addition to these roundtable discussions, the Commission also is embarking on a review of the Children's Online Privacy Protection Rule. The current rule was enacted in 2000 and, among other things, requires web site operators to obtain parental consent before collecting, using, or disclosing personal information from children under the age of thirteen. In light of rapidly changing technologies, such as the increased use of smartphones and other mobile Internet access devices, the FTC hosted a public workshop on June 2, 2010 to explore whether to update the rule.[15]

## IV. International Privacy

As the Notice observes, Internet commerce and related technologies, such as cloud computing, are increasingly global in nature. Thus, the FTC's policy work is not limited to domestic activities. The FTC actively participates in international policy initiatives relating to privacy and cross-border data flows through various international networks and organizations, including the Organization for Economic Cooperation and Development ("OECD") and the Asia-Pacific Economic Cooperation ("APEC") forum.

The FTC supports continued dialogue with its foreign counterparts and with international organizations on how to protect privacy and security across borders without restricting beneficial information flows. For example, in 2009, the Commission staff hosted a two-day international conference in conjunction with the OECD and APEC to

[15] More information about this review can be found at FTC, FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule, http://www.ftc.gov/opa/2010/03/coppa.shtm.

address how companies can manage data security in a global environment where data can be stored and accessed from multiple jurisdictions.[16]

The Commission also understands that, in a global economy, companies find it increasingly challenging to comply with varying privacy requirements around the world, particularly those relating to the cross-border transfer of personal consumer information. Likewise, the cross-border enforcement of privacy laws and regulations continues to raise novel questions for consumer protection authorities. The Commission recognizes that, as the need for cross-border data flow increases, facilitating companies' compliance with applicable laws as well as protecting consumers' data in the event of a failure to do so will require international cooperation.

In December 2006, Congress recognized the increasing threats facing U.S. consumers in the global marketplace from the proliferation of spam, spyware, telemarketing, and other cross-border consumer law violations, and passed the U.S. SAFE WEB Act. The Act enhances the FTC's ability to protect consumers by giving the agency new or expanded powers in several key areas.[17] The FTC has used the Act's authority to quickly and effectively protect consumers in the global economy. The Act has helped the FTC to overcome obstacles to cross-border enforcement it faced in the past and is critical to the FTC's ability to address problems that consumers may face in the future.[18] The FTC, therefore, has recommended that Congress preserve this much-needed authority and repeal the 7-year sunset provision contained in the Act.[19]

In addition, the FTC is actively involved in cross-border privacy enforcement initiatives. In November 2009, APEC approved a privacy enforcement cooperation arrangement for privacy enforcement authorities in the APEC region.[20] The FTC is actively participating in implementing this arrangement. Most recently, the FTC, along with ten other privacy enforcement authorities around the world, started a privacy enforcement cooperation network called the Global Privacy Enforcement Network

---

16 More information about this workshop can be found at FTC, Securing Personal Data in the Global Economy, http://www.ftc.gov/bcp/workshops/personaldataglobal/index.shtm.

17 The Act authorizes the FTC, in appropriate consumer protection matters, to share compelled and confidential information and provide investigative assistance to foreign law enforcement agencies addressing conduct substantially similar to conduct that would violate U.S. law. 15 U.S.C. §§ 46(f), (j), 57b-2(b)(6). It also gives the FTC a variety of other tools to improve international enforcement cooperation, which the FTC has used in a substantial number of consumer protection cases.

18 *See generally* FTC, *supra* note 6.

19 *Id.* at 19-21.

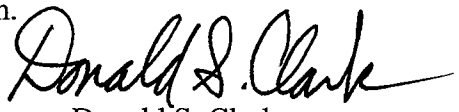
20 *See* APEC, APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, *available at* http://aimp.apec.org/Documents/2010/ECSG/DPS1/10_ecsg_dps1_013.pdf.

("GPEN"). The FTC also has brought several cases enforcing the U.S.-European Union "Safe Harbor" arrangement for data transfers.[21]

**Conclusion**

The Federal Trade Commission is pleased to provide these comments on information privacy and innovation in the Internet economy in light of our years of experience protecting consumer privacy both online and offline. The FTC will continue to devote substantial resources to protecting consumers using the Commission's law enforcement, consumer education, and policy development tools. The Commission would be pleased to assist the Department of Commerce in any way that would be useful toward the completion of its inquiry and report on information privacy and innovation in the Internet economy.

By Direction of the Commission.



Donald S. Clark
Secretary

[21] *See generally* Press Release, FTC, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework (Oct. 6, 2009), *available at* http://www.ftc.gov/opa/2009/10/safeharbor.shtm.

**BEFORE THE**
**DEPARTMENT OF COMMERCE**

**OFFICE OF THE SECRETARY**
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**INTERNATIONAL TRADE ADMINISTRATION**
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

Request for Comments

INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY

DOCKET# 100402174–0175–01

---

COMMENTS OF THE FUTURE OF PRIVACY FORUM

---

Jules Polonetsky
Co-Chair and Director, The Future of Privacy Forum
919 18th Street NW
Washington, DC 20036
202-713-9466
julespol@futureofprivacy.org

Christopher Wolf
Co-Chair, The Future of Privacy Forum
Bret Cohen
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
202-637-8834
202-637-5910 (fax)
christopher.wolf@hoganlovells.com
Counsel for THE FUTURE OF PRIVACY FORUM

June 14, 2010

## TABLE OF CONTENTS

**Page**

## I. INTRODUCTION

The Future of Privacy Forum ("FPF") submits these Comments in response to the Department of Commerce Notice of Inquiry dated April 23, 2010 ("*NOI*").[1] In the *NOI*, the Department announced a comprehensive review by its Internet Policy Task Force of the nexus between privacy policy and innovation in the Internet economy.[2] The Department is seeking comments regarding the impact of the current privacy framework on Internet commerce and innovation. The Department also is soliciting input on the necessity of adjusting today's privacy framework to promote innovation and privacy in the web-centric information environment.[3]

The Internet plays an important role in America's economic growth, and in the everyday lives of Americans. It is an unprecedented medium for communication, education, entertainment, and commerce. Increasingly, online technology enables businesses to collect, use, share, and store vast amounts of personal and anonymous information about people using the Internet. Such use of data promises to fuel additional economic growth online. But, increasingly, people are concerned about their privacy online.[4] Thus, for Internet commerce to flourish, privacy protection must improve.

---

[1] *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 Fed. Reg. 21,226 (Apr. 3, 2010).

[2] *Id.*

[3] *Id.* at 21,228.

[4] According to a recent study by the Pew Internet & American Life Project, young people especially are concerned about their online privacy. *See* Pew Internet & Am. Life Project, Reputation Management and Social Media: How people monitor their identity and search for others online (May 26, 2010), *available at* http://pewinternet.org/Press-Releases/2010/Reputation-Management.aspx.

At a time when many are calling for a new paradigm to protect personal data online as the way to improve privacy, the reality is that the well-known Fair Information Practices,[5] with their bedrock transparency principle, will continue to underlie the ways in which personal privacy is protected for some time to come. Thus, while FPF encourages and supports new thinking about structural ways in which privacy can be protected and enhanced online, we also encourage innovations within the current Fair Information Practices framework, as well as implementation of all of the principles contained within the framework whenever feasible.[6] Given the Department's role in supporting and facilitating U.S. business today and in the near term, we focus in this submission on ways in which online privacy can be enhanced within the existing framework.

We believe there is ample room for improvement and innovation. For example, the results of a research study released by FPF earlier this year indicate that simplified and user-friendly methods to communicate about data use can substantially improve transparency and consumers' understanding about how their information is used online. An example of a notice icon developed collaboratively by FPF is described below. We also highlight in the submission recent innovations and improvements in online privacy, and identify areas where improvements are needed.

Finally, we suggest ways in which the Department can exercise leadership in promoting online privacy (and thereby promote online commerce) through specific initiatives.

---

[5] *See, e.g.*, CTR. FOR DEMOCRACY & TECH., COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY ON THE STAFF DISCUSSION DRAFT OF CONSUMER PRIVACY LEGISLATION 1-2 (June 4, 2010), *available at* http://cdt.org/files/pdfs/20100604_boucher_bill.pdf.

[6] In addition to transparency, other widely accepted Fair Information Practices include Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Accountability and Auditing, and Security. *Id.*

## II. ABOUT THE FUTURE OF PRIVACY FORUM AND ITS ROLE IN THE DEVELOPMENT OF IMPROVED PRIVACY PRACTICES

FPF is a Washington, DC-based think tank whose purpose is to examine current and emerging challenges to personal privacy and to propose practical ideas to improve personal privacy now and in the future.[7] The efforts of such a non-governmental, non-profit entity is one way to advance privacy that should be encouraged by the Department, and we briefly highlight our recent efforts here.

As an example of FPF's role in the evolution of privacy practices, FPF recently led a project for the design of new forms of timely, informative, and eye-catching privacy notices concerning the collection of personal information for targeted advertising online. The genesis of the project was the realization that static and densely written privacy policies are limited in their ability to communicate clearly with consumers about what information is being collected and used by online businesses. Addressing this issue, the Federal Trade Commission ("FTC") expressed concern early last year that privacy policies were not being read or understood by consumers, and it urged the industry to develop new ways to notify consumers about online data collection and use.[8]

[7] FPF is supported by Adobe, AOL, AT&T, The Better Advertising Project, BlueKai, Deloitte, eBay, Intel, Lockheed Martin, Microsoft, The Nielsen Company, Proctor & Gamble, Qualcomm, Verizon, Visa, and Yahoo! and has an advisory board comprised of leading figures from industry, academia, law, and advocacy groups. The positions taken by FPF are entirely its own and do not necessarily reflect those of its supporters and advisory board members.

[8] *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf.

With this in mind, FPF partnered with the global marketing communications company WPP to launch a consumer-focused effort that relied on the skill of advertising and communications professionals to produce notices accessible through symbols or "icons."[9] The icons were tested with an Internet survey of a large group of users to determine their utility in providing effective notice, and to select the most effective symbols and language.[10] The icons and associated language that were selected already have been deployed for testing by Yahoo!, AT&T, and eBay and they have been adopted as part of the self-regulatory programs of a coalition of leading industry groups. Thus, FPF has taken a leadership role in the undertakings urged by the FTC.[11]

Another major FPF initiative concerns privacy and the Smart Grid. Modernization efforts are underway to make the current electrical grid "smarter" through the collection of data about consumer usage. FPF is taking the lead here as well, working with the GridWise Alliance, the Privacy Commissioner of Ontario, and others to address the potential privacy concerns

---

[9] *See* Future of Privacy Forum, Future of Privacy Forum Release Behavioral Notices Study (Jan. 27, 2010), http://futureofprivacy.org/2010/01/27/future-of-privacy-forim-release-behavioral-notices-study.

[10] *See* Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, *available at* http://nytimes.com/2010/01/27/business/media/27adco.html.

[11] FTC Chairman Jon Leibowitz recently reinforced his support for these efforts, stating that the FTC is not interested in regulating behavioral advertising so long as the industry is making "progress" toward self-regulation. Jon Eggerton, *Leibowitz: FTC Not Interested in Regulating Behavioral Ads If Industry Can Do Job*, Broadcasting & Cable (May 12, 2010), http://broadcastingcable.com/article/452590-Leibowitz_FTC_Not_Interested_in_Regulating_Behavioral_Ads_If_Industry_Can_Do_Job.php. He also said the commission has "great hopes" for proposed self-regulatory guidelines proposed by direct and online marketers in conjunction with the Better Business Bureau.

implicated by the Smart Grid and to propose that privacy protections be built into the Smart Grid network as it is developed, using the principles of "Privacy by Design."[12]

Finally, among the major ongoing FPF initiatives, FPF is beginning to focus attention on the data collection issues raised by the growing popularity of Internet-based applications, or "apps," especially those supported by social networking platforms and by mobile devices. FPF believes that users should be provided with sufficient and timely information by app developers so that users can understand how data about them may be used when they interact with apps.

As the name suggests, FPF is focused on privacy issues that loom large for the future, which is why we are pleased to make this submission in connection with the Department's focus on the future of online privacy in the United States.

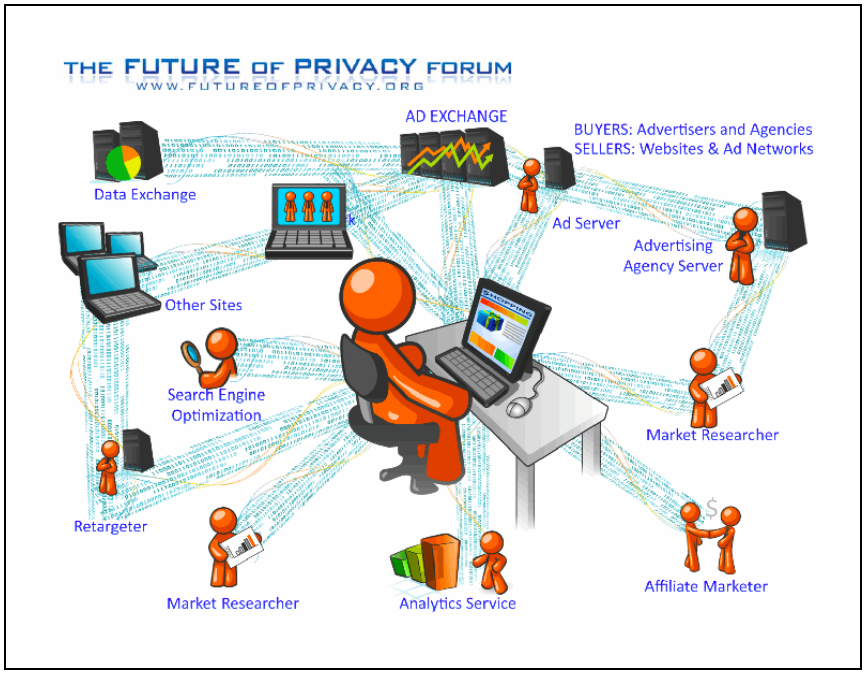
[12] FPF filed comments to the National Institute of Standards and Technology's Smart Grid Interoperability Standards Project to encourage responsible data management practices by all entities involved in the Smart Grid ecosystem and facilitate stakeholder discussions to develop best practices. Comments of the Future of Privacy Forum, Report to the National Institute of Standards and Technology on the Smart Grid Interoperability Standards Roadmap, Department of Commerce, Docket No. 0906181063-91064-01 (filed July 30, 2009); *see also* THE FUTURE OF PRIVACY FORUM & INFO. AND PRIVACY COMM'R OF ONT., SMARTPRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION (2009), *available at* http://ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf; Comments of the Future of Privacy Forum to the FCC on NBP Public Notice #2, GN Docket No. 09-47 (filed Oct. 2, 2009).

## III. EXAMPLES OF INNOVATION AND AREAS OF NEEDED IMPROVEMENT IN ONLINE PRIVACY

This proceeding provides the opportunity for FPF to highlight best practices and to identify areas for improvement in online privacy. We hope that the Department will continue to provide a forum for the exchange of this kind of information that will incentivize the development of privacy-enhancing technologies and practices by those in the online ecosystem.

We begin by examining new methods of information exchange and the ways in which organizations inform users about and provide choices regarding the online collection and use of personal data.

The Internet has led to the development of highly efficient online data use platforms through which companies collaborate and combine their individual expertise to promote online commerce and to improve consumers' experiences. Whether an online user knows it or not, by visiting one website he or she can share data with dozens of companies: a web publisher, an ad exchange, a search engine, an analytics company, advertisers, and more. An example of these information exchanges is illustrated in the following graphic:



The success and efficiency of these platforms generates value for publishers and contributes to the growth of an open Internet with free content. Despite the fact that consumers may believe the site they are visiting is responsible for all data activity resulting from their visit, the fact is that data collection and use is often far from transparent. It is by no means clear whose privacy policy controls the collection, use, and sharing of data collected from visits to web pages.

A number of companies in the online ecosystem have taken the initiative to provide innovative features that increase the transparency of their uses of consumer information and maximize the level of control that consumers have over these uses. In the following section, we highlight a few notable innovations in privacy-enhancing technologies.

## A. Noteworthy Innovations

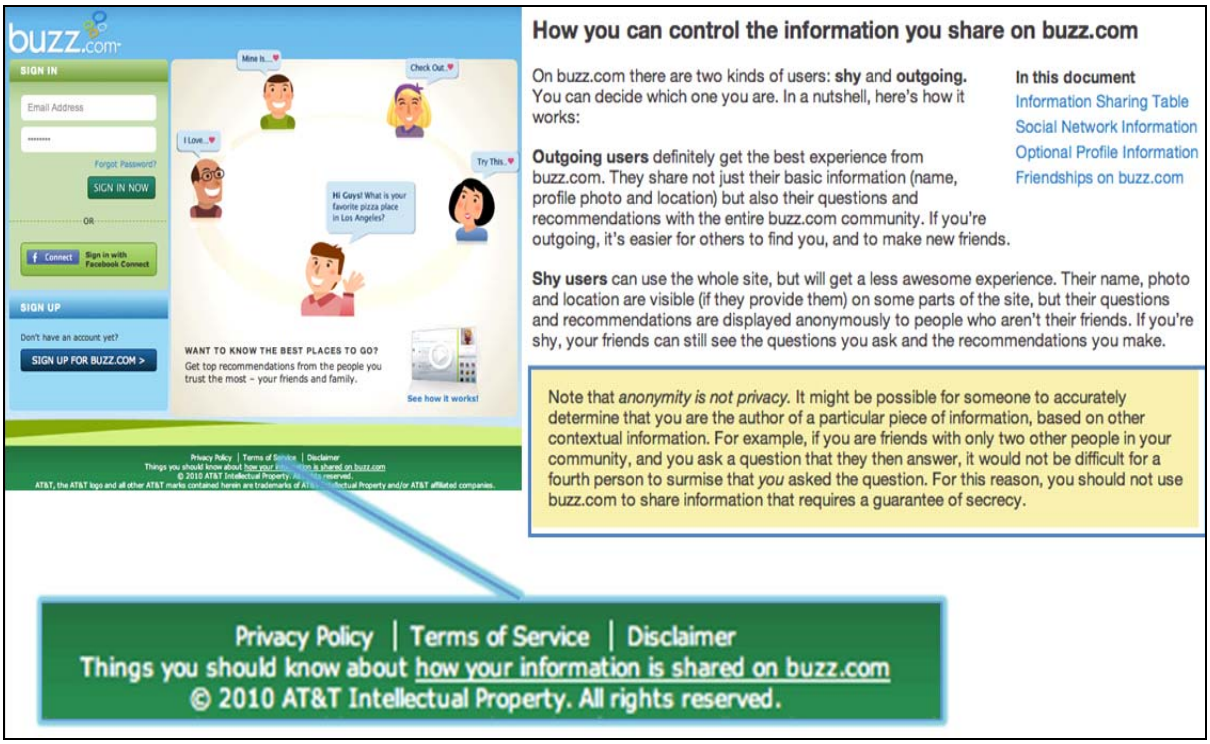
### 1. Labeling privacy policies in a common-sense fashion by directing users to see "how your information is being used"

Privacy policies remain the primary means of providing legally required notice to consumers about the collection and use of their information. California's Online Privacy Protection Act requires most companies that operate online in the United States to have privacy policies.[13] Given that privacy policies likely will remain the norm for the foreseeable future, some companies have undertaken commendable efforts to transform these policies into a format more easily understood by the average Internet user.

---

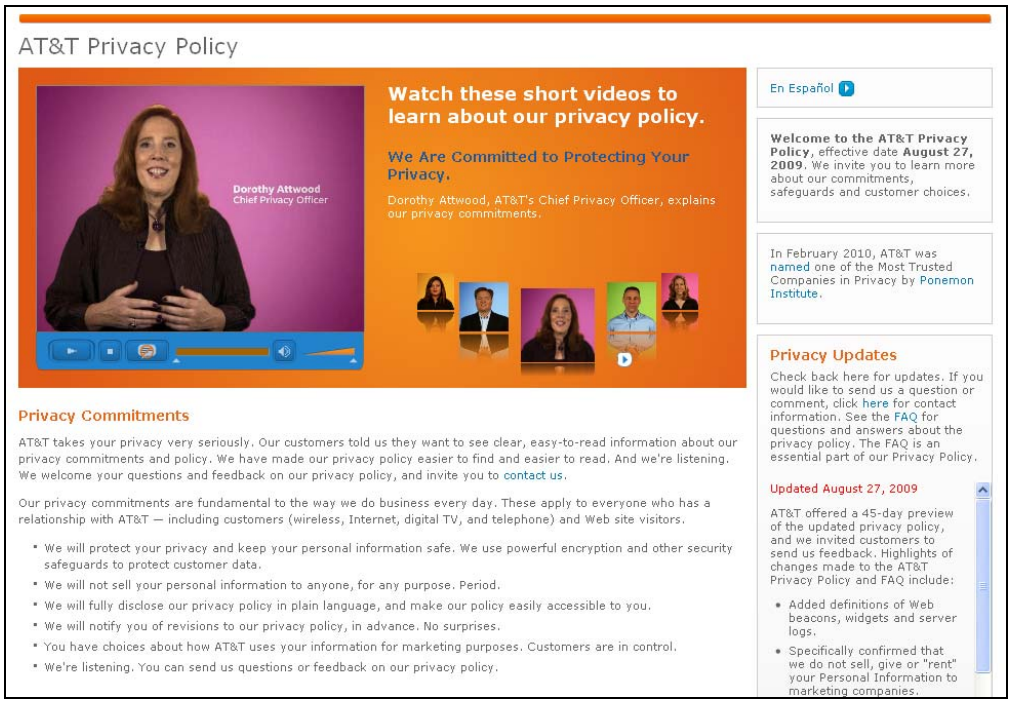
[13] *See* Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575-22579. Also, a recent discussion draft of a bill released by Representatives Rick Boucher (D–VA) and Cliff Stearns (R–CA) would require companies to post privacy policies when they collect and share user information online for advertising purposes. Draft bill § 3, http://boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf. The FTC, using its investigative and enforcement authority under Section 5 of the FTC Act, 15 U.S.C. § 45, ensures that promises made in online privacy policies are kept. *See* FTC, A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority (July 2008), http://ftc.gov/ogc/brfovrvw.shtm.

A good example of this innovation is buzz.com that, in addition to its listed privacy policy, maintains a link to "how your information is shared on buzz.com." This link provides concise, straightforward information about buzz.com's information sharing practices, even noting that anonymity does not guarantee secrecy, as shown here:

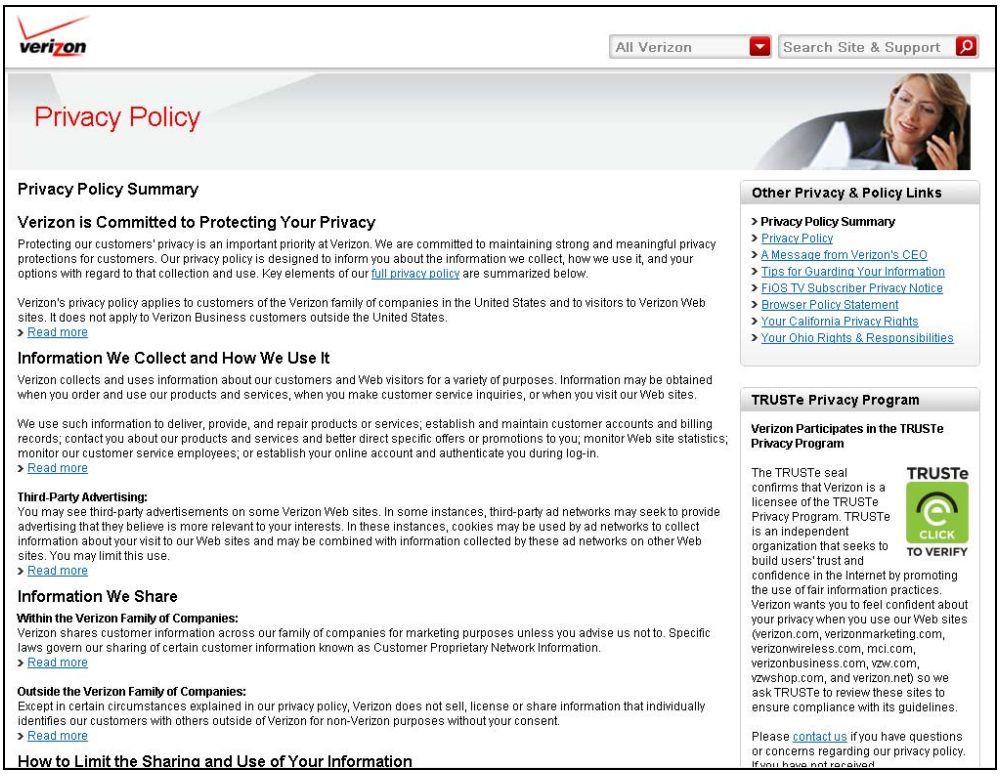



As another example, in June 2009, communications company AT&T unveiled a new, unified privacy policy that replaced seventeen separate privacy policies for various AT&T companies, products, or services.[14] In drafting this policy, AT&T incorporated feedback from focus groups. Before the policy went into effect, AT&T offered customers a forty-five-day preview, answered questions, and made clarifications to policy language. The result, illustrated below, included videos of AT&T employees describing aspects of its policy to make it more easily understood by consumers.

[14] AT&T, AT&T Named One of the Most Trusted Companies in Privacy: Ponemon Institute Survey Shows Consumers Rank AT&T Among Leaders in Protecting Personal Information (Feb. 25, 2010), http://att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=30569.




Likewise, Verizon employs a plain English, layered approach to its privacy policy, with simple statements on how it collects and uses personal information, and hyperlinks for users to obtain more detailed information about the privacy policy, as shown here:



The alternatives to dense, legalistic privacy policies offered by AT&T, Verizon, and others constitute an important move towards greater transparency and consumer understanding.

### 2. The use of an icon to attract consumer attention and link to information

The most common criticism of the privacy policy approach to notice and choice is that most website users do not read or understand lengthy legalistic policies accessible only by clicking on a tiny link at the bottom of a web page.[15] Earlier this year, FPF released the results of a research study that tested, as an alternative to the privacy policy approach, the effectiveness of using new icons and key phrases to provide web surfers with more transparency and choice about behavioral advertising practices.[16] The results indicated that the icons and phrases, plus an education campaign, can play an important role in educating consumers about behavioral advertising. The study also found that applying transparency and choice to behavioral ads increased the percentage of those who were comfortable with behavioral advertising by 37%. The study was praised by FTC Chairman Jon Leibowitz, who in the past has urged companies to provide succinct notice about ad targeting,[17] as well as FTC Consumer Protection Director David Vladeck, who called the icon a step "for the good" at the FTC Privacy Roundtable this year.[18]

---

[15] *See infra* Section III.B.2.

[16] FUTURE OF PRIVACY FORUM, ONLINE BEHAVIORAL ADVERTISING "ICON" STUDY: SUMMARY OF KEY RESULTS (Jan. 25, 2010), *available at* http://futureofprivacy.org/final_report.pdf.

[17] Chairman Leibowitz stated: "I'm very heartened with what the Future of Privacy Forum has announced. Most current online privacy policies are essentially incomprehensible from even the savviest online users." Wendy Davis, Can WPP Demystify Behavioral Targeting? (May 20, 2009), http://mediapost.com/publications/?fa=Articles.showArticle&art_aid=106519.

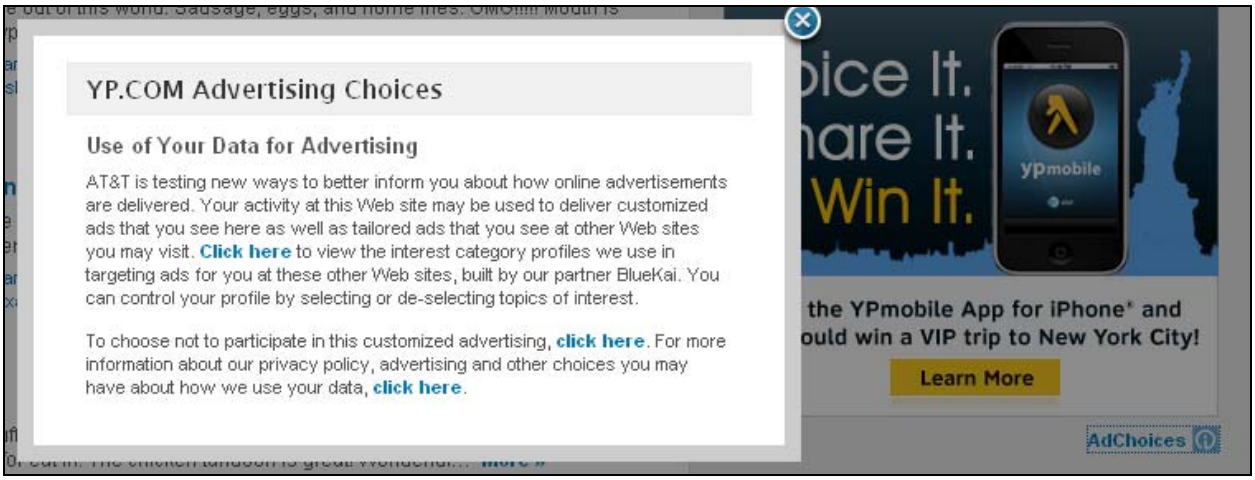
[18] *See* Jules Polonetsky, Behavioral Ads Good for Business, Sez the NAI (Mar. 24, 2010), http://futureofprivacy.org/2010/03/24/behavioral-ads-work-and-cost-more-sez-the-nai.

The "Power I," pictured at right, has been adopted following the release of the FPF Report.[19] It will serve as part of the self-regulatory programs of the Internet Advertising Bureau ("IAB"), the Network Advertising Initiative ("NAI"), the Association of National Advertisers, and the American Association of Advertising Agencies, and will be managed by the Better Business Bureau. Furthermore, in April, the NAI and IAB, both self-regulatory organizations for the online advertising industry, jointly released their CLEAR Ad Notice technical specification that enables the use of standard meta data in ad delivery coding to provide more detailed information about the type of ad targeting taking place. This enhanced notice will be accessible to users via the Power I symbol,[20] as shown here:

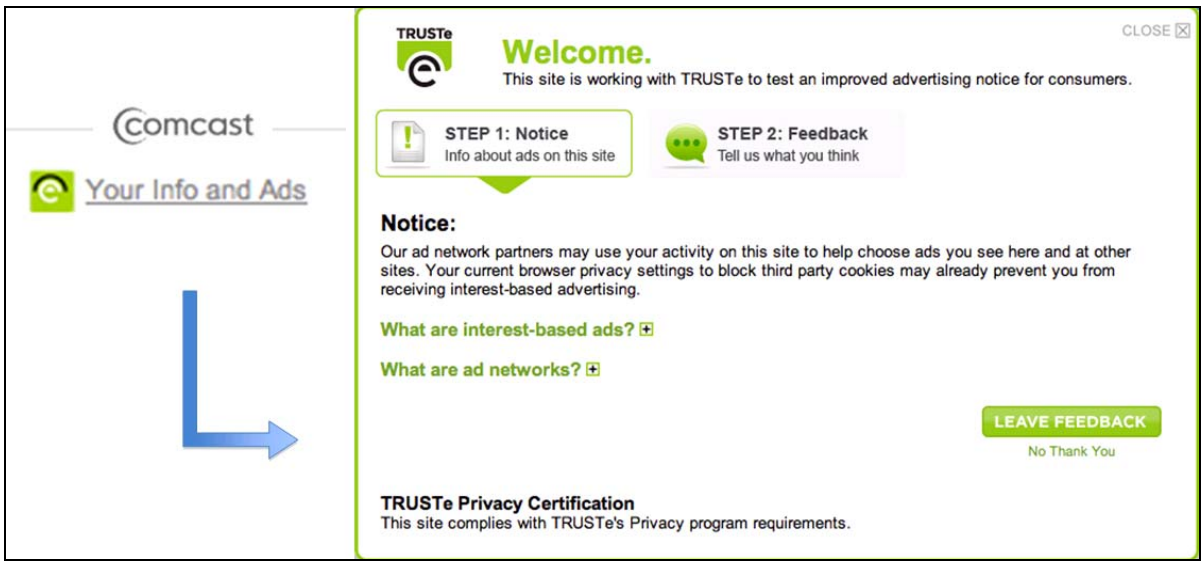

[19] *See* Stephanie Clifford, *A Little 'I' to Teach About Online Privacy*, N.Y. TIMES, Jan. 26, 2010, at B3, *available at* http://nytimes.com/2010/01/27/business/media/27adco.html; Am. Ass'n of Adver. Agencies, Ass'n of Nat'l Advertisers, Direct Mktg. Ass'n, Interactive Adver. Bureau, & Council for the Better Bus. Bureaus, Trade Groups Announce the Selection of the Wording and Link/Icon that Will be Used to Indicate Adherence to Industry Self-Regulatory Principles for Online Behavioral Advertising (Jan. 27, 2010), *available at* http://the-dma.org/cgi/dispannouncements?article=1379.

[20] *See* IAB & NAI, CLEAR AD NOTICE: TECHNICAL SPECIFICATIONS FOR THE IMPLEMENTATION OF THE INTERACTIVE ADVERTISING SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 5-6 (Apr. 2010), *available at* http://iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf.

Websites like Yahoo!, yp.com, and eBay also have already adopted the Power I icon and an explanatory phrase when delivering targeted ads. Clicking on the icon on these websites links to a list of preferences that gives users information about the specific ad and allows them to opt out of future targeted ads. For example, clicking on the icon on yp.com leads to the following screen:




The Power I has not been the only innovation in achieving heightened consumer notice. TRUSTe, a provider of online privacy accreditation services, also has launched a program to allow websites to provide enhanced notice to users and to add better opt-out controls. An example of this program, as adopted by Comcast, is shown here:



If implemented in concert with serious self-regulatory efforts and continued technology advances encouraging their adoption, these programs relying on icons and phrases represent an important step in the evolution of notice and choice from sometimes-convoluted privacy policies to a more visceral, understandable method that better informs consumers about how their information is used by the websites they visit.

### 3. Limiting the retention of search queries and deleting data used for targeted advertising after a defined period

It is axiomatic that if data does not exist, it cannot be misused or used in a way that surprises consumers. Some companies have undertaken efforts to limit the time that they retain certain information about consumers' online activities. For example, the operators of the three most popular search engines have reduced their retention of IP addresses and cookies in server logs within the last two years: Google has reduced its retention period from eighteen months to nine months,[21] Microsoft has reduced its retention period from eighteen months to six months,[22] and Yahoo! has reduced its retention period from thirteen months to three months.[23] Notably, Yahoo! has applied its retention program to both search logs and to adserving log files. There also have been self-regulatory efforts to publicize retention periods to help consumers make informed choices based on how long their information is retained. The NAI, for example, requires its members to retain personal data only as long as necessary to fulfill a "legitimate

[21] Peter Fleischer, Global Privacy Counsel, Jane Horvath, Senior Privacy Counsel & Alma Whitten, Software Eng'r, Google, Another step to protect user privacy (Sept. 8, 2008), http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html.

[22] Peter Cullen, Chief Privacy Strategist, Microsoft, Microsoft Advances Search Privacy with Bing (Jan. 18, 2010), http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx.

[23] Anne Toth, Vice President of Pol'y & Head of Privacy, Yahoo!, Your data goes incognito (Dec. 17, 2008), http://ycorpblog.com/2008/12/17/your-data-goes-incognito.

business need" and to publish their retention periods on their websites.[24] Note, for example, Lotame Solutions, an NAI member which explains that it keeps adserving log data for no longer than nine months.[25]

The shortening of retention periods for data that can be used to personally identify consumers is an important step toward ensuring consumers' privacy in their Internet use.

**4. Minimizing IP address details in web analytics**

Another privacy-enhancing technique is the minimization of IP address details in web analytics. Website owners hire web analytics companies to provide certain details about the usage and performance of their sites, such as the number of unique users, the ability of users to navigate to the content they seek, and the usability of a website in general. Necessarily, companies providing web analytics services are initially sent user IP addresses. Although these addresses do not explicitly identify a particular individual, the potential for identification in some circumstances calls for more conservative practices. FPF recommends that IP addresses logged by web analytics providers be obscured or deleted as soon as possible and previously recommended this practice be adopted by federal government agencies that use such analytics tools.[26]

---

[24] NAI, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT III.2(a)(vi), 9(a) (2008), *available at* http://networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20website.pdf.

[25] *See* Lotame, Privacy Policy, http://lotame.com/privacy (last visited June 14, 2010).

[26] *See* Future of Privacy Forum, Future of Privacy Forum Release Behavioral Notices Study (Jan. 27, 2010), http://futureofprivacy.org/2010/01/27/future-of-privacy-forim-release-behavioral-notices-study FPF's Reply Comments to the Federal Websites Cookie Policy (Aug. 10, 2009), http://futureofprivacy.org/2009/08/10/fpf's-reply-comments-to-the-federal-websites-cookie-policy.

Some companies have taken commendable steps toward minimizing the collection, reporting, and retention of the IP addresses of the users of the websites they track. A number of companies can provide clients with a feature that ensures the IP addresses collected for analytics purposes will be immediately obscured. Encouraging wider spread of such efforts will ensure that analytics and other similar services are able to provide functionality in a manner that maintains user privacy.

**5. Stronger browser privacy controls**

Stronger browser controls are another way to protect online privacy. A substantial majority of consumers interact with third parties over the Internet through a free, commercial web browser. These browsers serve as important gatekeepers between ordinary consumers and third parties to which these consumers transfer information. In their role as gatekeeper, developers of browsers generally increased the number of privacy controls available to users in recent years. These controls, however, were often buried deep within submenus and tabs and largely were unknown to the average user. Even if users were able to find these controls, recent studies demonstrated that users experience substantial confusion about the results of actions they take within their browsers and do not understand how the technology works.[27]

To rectify some of these issues, the major browser developers have designed enhanced privacy options to allow more users to customize and control how their information is shared with the websites they visit. Internet Explorer's InPrivate Browsing, Chrome's Incognito mode, Safari's Private Browsing, and Firefox's Stealther add-on all provide more straightforward interfaces and collections of privacy options that provide users with more transparency and

[27] Aleecia M. McDonald & Lorrie Faith Cranor, *An Empirical Study of How People Perceive Online Behavioral Advertising*, Carnegie Mellon University CyLab Technical Reports (Nov. 10, 2009), *available at* http://www.cylab.cmu.edu/research/techreports/2009/tr_cylab09015.html.

control over how their information is shared and how they will allow websites to interact with their computers. Privacy has also become a competitive element in new browser releases. Mozilla, for example, recently released details about the new version of its Firefox browser that includes a single menu to display what information websites are gathering and allow users to decide which cookies to allow and which to disable.[28] These continued enhancements of privacy controls, and a recognition that consumers may now choose their browser in part based on privacy features, bode well for the continued evolution of comprehensible privacy controls in web browsers.

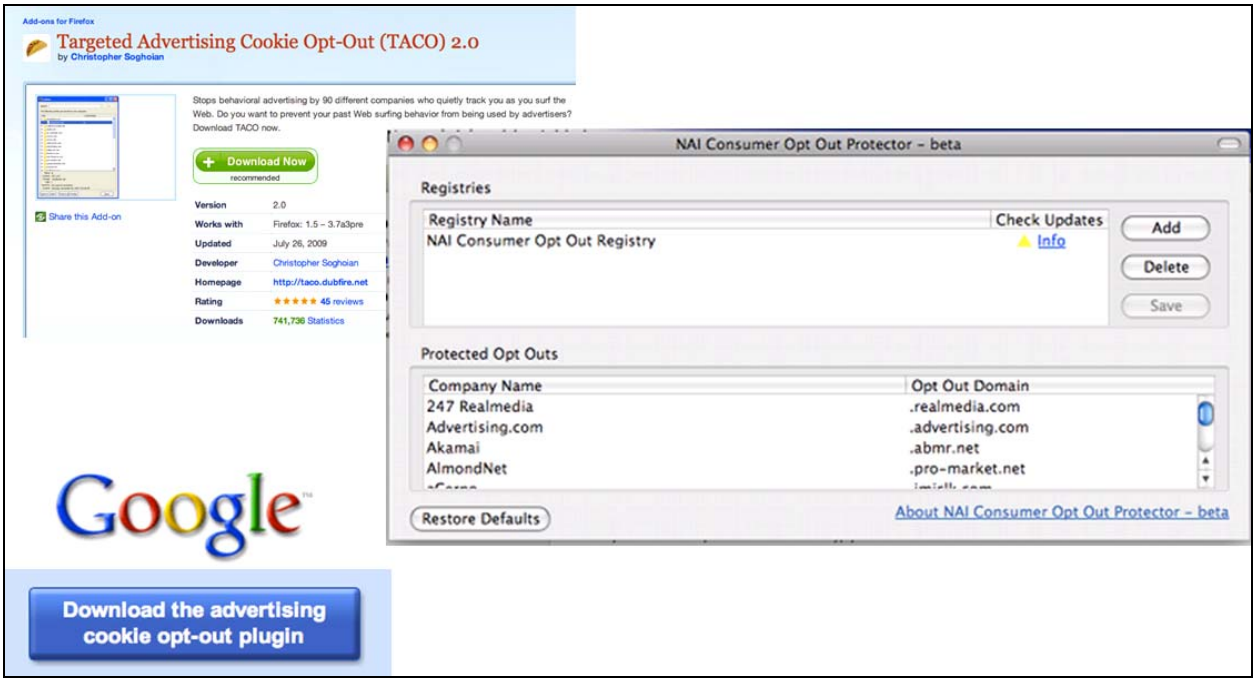
### 6. Plug-ins that ensure opt-out status even after clearing cookies

While many behavioral advertisers have taken affirmative steps to self-regulate, such as through the NAI and IAB, these efforts are limited by the means through which they implement a user's choice to opt out of behavioral targeting of advertisements. Such opt out is generally achieved by placing an "opt-out cookie" on a user's web browser that signals participating network advertising websites not to track that user's activities or place additional tracking cookies. Unfortunately, because these cookies expire after a certain period or are deleted whenever a user clears his or her cookie repository, the user must go through the opt-out process again whenever that opt-out cookie is deleted.

There are, however, technological solutions to achieve a more stable, persistent opt-out status. The Targeted Advertising Cookie Opt-Out ("TACO") plug-in for Mozilla's Firefox browser, the NAI Consumer Opt Out Registry, and Google advertising cookie opt-out plug-in,

[28] Joel Schechtman, *Firefox 4 has simpler design, more privacy control*, ASSOCIATED PRESS (May 11, 2010), *available at* http://news.yahoo.com/s/ap/20100511/ap_on_hi_te/us_tec_techbit_firefox_browser.

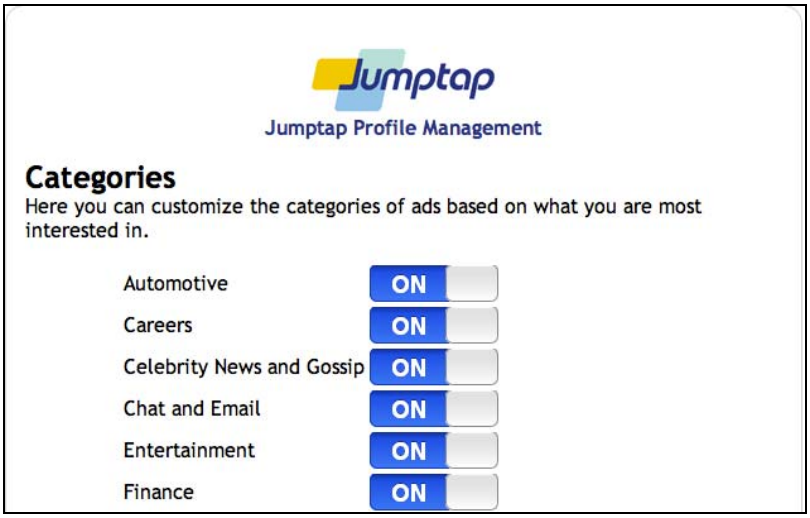
shown below, each ensure that a user's opt-out status is maintained even after opt-out cookies expire or are cleared by the user.



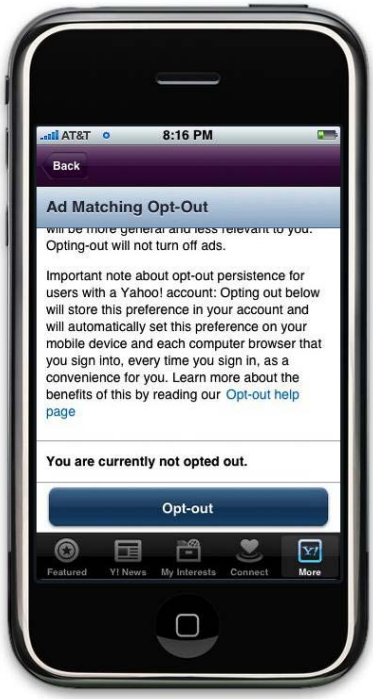

### 7. Creating a mobile opt out and mobile profile viewers that bring new behavioral controls being implemented on the web to mobile devices

With the increased use of smartphones and other mobile devices that can access the Internet, companies are seeing great value in delivering targeted advertisements to mobile device users based on their mobile browsing. Companies deliver such advertising using similar methods to those used when individuals browse from their computers, including the use of cookies. While there has been a concerted effort to develop tools that increase transparency and control for consumers who use computer-based Internet browsers, these tools have been relatively absent in the mobile context. That trend, however, is changing. Jumptap, which

manages a mobile ad network, created the first mobile behavioral profile viewer that allows consumers to edit the categories of ads they will receive, as shown below:

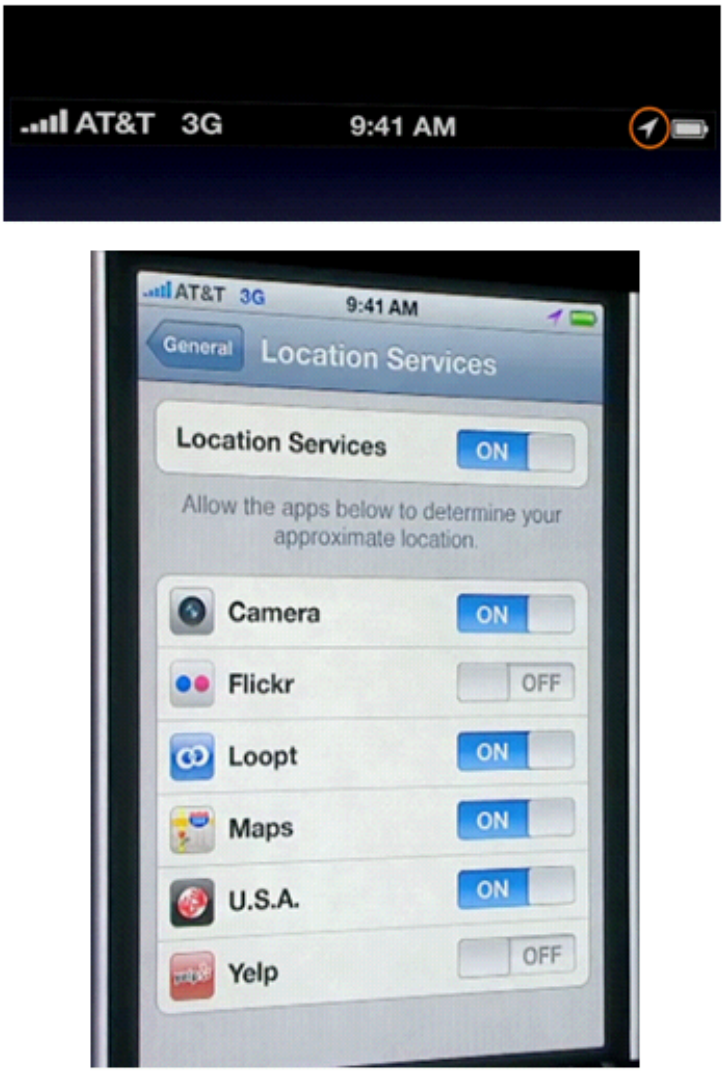



Many of the leading mobile ad networks already offer a mobile cookie opt-out, as noted in the Yahoo! disclosure shown below. The FTC has been clear in its behavioral advertising guidance that consumers should be entitled to opt out of behavioral ads, regardless of the platform involved.

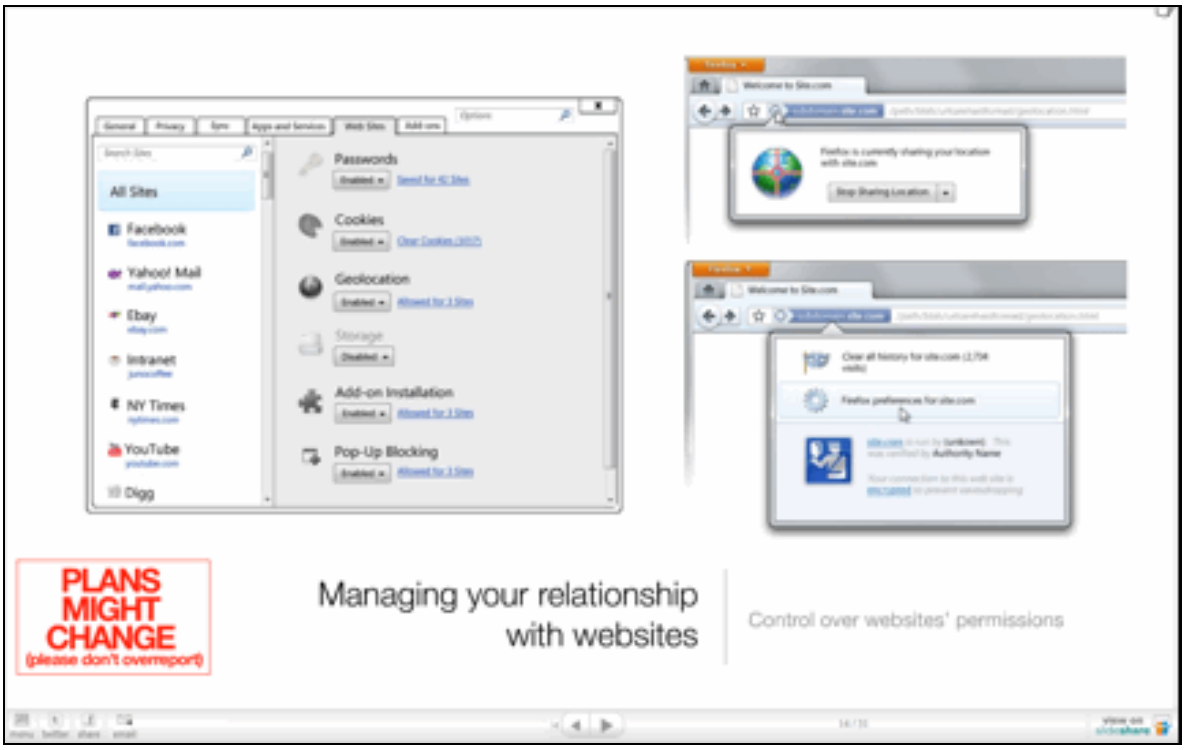


### 8. Indicators showing when one is being geolocated

A significant trend in mobile advertising is the use of a mobile device user's exact geographic location (or "geolocation"), which is calculated and stored by mobile devices on an almost real-time basis, to deliver ads to the user relevant to that specific location. While ads specific to a consumer's location have the potential to deliver great value (such as by providing the consumer with a coupon for a nearby store), in many cases they can be unwanted, especially if the consumer perceives that he or she is being physically "watched" by advertisers. To better inform its customers, Apple included an icon in its new iPhone operating system informing users that their location information is being used, and allows users to control which apps can use that information, as shown here. Verizon has also provided a similar symbol in recent years on many of the smart phones it supports.



Geolocation does not occur only on mobile devices. Some computer-based Internet browsers, such as Firefox, allow websites to request geolocation information that the browser derives from a variety of sources such as by scanning local wireless access points. To alert users when a website requests their location in this manner, the new version of Firefox will now display an icon in the browser address bar, as shown below:




The iPhone's and Firefox's location tracking options are positive advancements in providing transparency and control over users' geolocation information.

### B. Areas Needing Improvement

The efforts described above represent important steps forward in providing consumers with notice, choice, and control over their privacy options, as well as limitations on the retention of data. However, several challenges remain. This section outlines some key issues that FPF believes still need to be addressed.

#### 1. Lack of usability of privacy controls, particularly for social networking

Social networking services have exploded in popularity over the past few years. So too has the amount of information – some of it sensitive personal information – that individuals are willing to post online through these services. As the popularity of these services has grown, social network operators have implemented new and innovative features in their products. With each new feature, however, the complexity of users' privacy controls grows.

The challenge for social networking services is to provide users with more granular privacy controls without the control interface becoming overly complex. While recent changes to privacy settings pages at the leading social networks have been a good step forward, the usability challenge remains clear. The more privacy options available, the more difficult it becomes to design a "usable" interface.

#### 2. Privacy policies are cumbersome and inaccessible to users

As information uses, privacy choices, and privacy controls increase in complexity, so do the length and complexity of privacy policies. Complete disclosure of all aspects of an organization's privacy commitments is a lengthy process, and the number of such aspects is only likely to grow. Yet reading and digesting long privacy policies is impracticable for the average consumer, even assuming they possess the requisite technical and legal sophistication to understand the policies. One study suggests that it would take the average American

approximately 200 hours annually to read all the privacy policies viewed during the course of each year.[29] Thus, further innovations for communicating the essential contents of privacy policies are needed. While the full details of the privacy practices of online companies need to be disclosed for examination by regulators and privacy advocates (as well as interested consumers), there should be better ways to communicate the basics of how an online entity is collecting, using, sharing, and storing data from individuals.

### 3. Lack of transparency and control with respect to certain tracking technologies

Traditional browser cookies are a well-known technology for which there are a variety of privacy controls built into most web browsers. Other technologies exist, however, that are used to track user activity and for which users have little or no ability to control their privacy settings. Two common examples are tracking pixels and Flash cookies.

Tracking pixels, also known as "clear GIFs" or "web beacons," are small, transparent images placed into web pages and HTML-format emails that can track when a user views the web page or opens the email that contains them. These images can be specially coded to identify users individually. It is virtually impossible for the average user to opt out of this type of tracking because, unlike with traditional browser cookies, there is no universal method to identify that an image is a tracking pixel as opposed to any other type of transparent image on a web page.[30] Transparent images are, for example, often used to ensure proper spacing and alignment. While some email software does not automatically load images, if a user wants to

---

[29] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. OF L. & POL'Y FOR THE INFO. SOC'Y, ISSUE 3 (2008).

[30] It is worth noting that in the absence of a persistent cookie to which to connect the fact that a page was viewed or an email was opened, tracking pixels provide limited tracking information. However, their tracking functionality remains enabled even if a user has disabled cookies.

view any of the images in HTML format the user generally must indicate that he or she wishes to view all of the images, thus triggering the tracking pixel.

Adobe Flash is a multimedia software platform compatible with many web browsers that allows the delivery of graphics, audio, video, and interactive controls not supported by traditional HTML-based web pages. Flash cookies are items in persistent storage within the local copy of the Adobe Flash Player installed in a user's web browser. They can be used to store information and track users in a manner similar to traditional browser cookies. While Adobe does provide functionality to purge one's Flash player of Flash cookies,[31] these controls are not integrated into most browsers and traditional browser privacy controls do not currently affect Flash cookies. Some companies have leveraged this gap to misuse Flash cookies and thwart the preferences of users who have intentionally deleted browser tracking cookies. The FTC has confirmed at least one active investigation of this concern.[32]

Adobe does not condone the misuse of Flash cookies in this manner and has been in discussion with browser vendors regarding developing comprehensive browser privacy controls.[33] This is an area, however, where better collaboration between the relevant companies is needed to speed progress.

---

[31] *See* Flash Player Help – Settings Manager, http://macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html (last visited June 14, 2010).

[32] *See* Wendy Davis, Flash of Criticism at FTC Privacy Roundtable (Jan. 28, 2010), http://mediapost.com/publications/?fa=Articles.showArticle&art_aid=121524.

[33] *See* Comments from Adobe Systems Incorporated – Privacy Roundtables Project No. P095416 (Jan. 27, 2010), *available at* http://ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

### 4. Lack of a standardized definition of "personal" or "sensitive" information and related terms

The terms "personal" and "sensitive" information appear frequently in discussions about privacy and in privacy-oriented laws such as state security breach notification statutes. There is little formal agreement, however, about what exactly constitutes the definition of "personal" or "sensitive" information. The state breach notification statutes, for example, all define such information to include at least a combination of an individual's name and at least one of their Social Security Number, Driver's License/ID number, or financial or payment card account number. However, while nearly all jurisdictions' statutes include this base set of "information pairs," many jurisdictions allow additional elements to be combined with an individual's name to constitute personal, personally identifiable, or sensitive information. Furthermore, each of these definitions involves the combination of at least two data elements – name and another item – which in itself can be confusing when trying to determine data protection obligations.

There is also substantial misunderstanding (and perhaps misuse) of the terms "anonymous" and "identifiable." This is particularly true as information systems become more advanced and the ability to "re-identify" data – that is, assign identities to otherwise anonymous elements of a dataset based other characteristics present in the dataset – evolves. A common definition of what constitutes anonymous data is necessary to improve communication with consumers and increase their understanding of privacy choices. This requirement is equally true for what constitutes identifiable data, in part because of problems of re-identification and in part because of the current lack of consensus on what constitutes personal or sensitive information.

This lack of consensus presents substantially confusing messages to consumers. Asking the average consumer to recall whether they have provided a combination of certain data

elements as part of determining whether they want to share their "personal information" is a complex question, and doing so potentially applies only in a single geographical jurisdiction or in a single industrial sector.[34] Uniform standards for personal information, sensitive information, anonymity, and related terms will help consumers better understand not only their choices, but also what a company means when it commits to "protect your personal information." The lack of a standardized definition for these terms hampers the ability of consumers and organizations to communicate about privacy issues. The issue also continues to be a source of tension between U.S. companies and international regulators, as the different methods by which search engines claim to anonymize search logs vary and have yet to satisfy many authorities in the European Union.[35]

### 5. The need for a plug-in to maintain a stable opt-out status

As discussed previously, some vendors have developed plug-ins to ensure that a user's decision to opt out of tracking online is maintained even after opt-out cookies expire or are cleared by the user.[36] Presently, plug-ins are the only solution that will ensure a stable opt-out status. This presents a problem for the average user who is not likely to know that a plug-in is required, particularly given the lack of transparency in how tracking technologies operate as discussed elsewhere in these Comments. Others may not wish to take the additional step of downloading a plug-in. Browser manufacturers can address this issue by using a browser header flag as an opt-out indicator, or by other methods that may be more effective. It seems clear,

---

[34] Health care information, for example, is subject to additional regulation through the Health Insurance Portability and Accountability Act, which has its own definitions of individually identifiable information and protected health information. *See* 45 C.F.R. § 160.103.

[35] *See, e.g.*, Article 29 Data Protection Working Party, EU data protection group says Google, Microsoft and Yahoo! do not comply with data protection rules (May 26, 2010), *available at* http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_26_05_10_en.pdf.

[36] *See supra* Section III.A.6.

however, that without additional efforts – such as those we suggest in Section IV of these Comments – it is unlikely that progress will come quickly in this area.

### 6. Increased data collection by applications

Social media platforms and smart devices have spurred the development of an amazing number and diversity of applications. Many of these are free or nominally priced. Developed by hundreds of thousands of individuals and small businesses around the world, these bits of software have added great value to the interactive environment. But, although some of these companies have grown quickly, many have little capacity to ensure the privacy or security of the data they collect. Large amounts of user data are available to these developers through integration into social networks and smart devices. Since the "app" business models are reliant on the monetization of user data, app developers are incentivized to collect as much data as possible. It is certainly clear that the incentives here should align to promote privacy and trust along with innovation and the development of new applications; it is unclear, however, whether market incentives will do so before substantial harm to consumers occurs.[37]

Privacy presents an interesting economic dilemma in that many consumers would like to have good privacy controls and many firms would like engage in good privacy practices but there is little incentive for an individual consumer or individual firm to do so. For the individual, exercising additional privacy – in the absence of good privacy practices integrated into applications – means completely abstaining from various web applications that have become integral to modern society. For the firm, integrating good privacy controls can be expensive,

[37] As noted above, these smaller actors may lack the resources to ensure the privacy and security of data they collect about users. These smaller actors, therefore, make attractive targets for identity thieves and others looking to misuse data collected about individuals.

reducing its competitiveness among competitors who spend less money on privacy or collect additional information.

### 7. The illusion of privacy control

Partially in response to a call by the FTC for increased self-regulation by the online advertising industry,[38] a number of companies have developed online tools to help consumers control their information. A recent study found, however, that 62% of consumers believe that the mere presence of a privacy policy alone implies certain privacy protections, such as restrictions on the sharing of data with third parties.[39]

This incorrect assumption by consumers highlights a disconnect between website users and operators regarding the effect of privacy policies and privacy controls. The mere *existence* of privacy controls may create a false illusion of privacy protections or of a user's ability to make privacy choices.[40] In fact, those protections may require the user to take additional proactive steps, or the choices a user actually wants to make may not be available. In both cases, the user may come to the incorrect conclusion because of a lack of understanding about how the privacy controls are implemented. This lack of understanding is likely at least partly a result of the complexity and lack of transparency of privacy policies. If users cannot understand the effect of privacy choices and controls, they will not be able to enact their preferences. Thus, online

---

[38] *See* FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://ftc.gov/os/2009/02/P085400behavadreport.pdf.

[39] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities That Enable It* (Sept. 29, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[40] *See, e.g.*, Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, preliminary draft prepared for Workshop on the Economics of Information Security 2010 (Mar. 2010), *available at* http://weis2010.econinfosec.org/papers/session2/weis2010_brandimarte.pdf (draft cited with prior permission) (finding that, paradoxically, the more options for control presented to consumers, the more willing they were to share personal information even though the outcomes and risks of the sharing were the same in both cases).

companies must engage in comprehensive education and awareness campaigns to provide consumers with the understanding they need to make privacy choices online.

## IV. THE ROLE OF THE DEPARTMENT OF COMMERCE IN ADVANCING ONLINE PRIVACY

The preceding discussion demonstrates that industry efforts are helping to advance online privacy while at the same time there is still work to be done to increase transparency and choice. The Department can play a leadership role to promote greater attention to online privacy by companies.

First, the Department should conduct, encourage, and fund research and other collaborative efforts to advance the evolution of technologies and practices that improve consumer transparency and choice. Second, in the forthcoming report to be issued pursuant to this *NOI*, the Department should recommend that the Administration take steps to more aggressively use existing legal tools to investigate and enforce against misuse of personal data, and to thus protect personal privacy online.

### A. The Department Should Conduct, Encourage, and Fund Further Research and Other Collaborative Efforts to Advance the Evolution of Technologies and Practices that Improve Consumer Transparency and Control

One method the Department can use to promote the adoption of privacy-enhancing practices is to conduct, encourage, and fund public, private, and non-profit research that aims to improve consumer privacy. Not only would this help spur further privacy innovations, it would also signal the Department's and the Administration's commitment to the protection of consumer privacy, an increasingly relevant and mainstream issue in this country. The Department can pursue this agenda through a variety of means. Internally, the Department can conduct its own research, such as by leveraging the extensive technical competencies of the National Institute of Standards and Technology ("NIST"). Externally, the Department can fund the research of private and non-profit institutions or provide grants for start-up companies and small businesses that incorporate privacy in their business plans.

Perhaps the most effective way for the Department to encourage the development and adoption of privacy-enhancing practices is to engage in collaborative efforts with industry, advocacy groups, government agencies, and other stakeholders. For example, the Department can convene task forces that include public and private actors to focus on identifying options and solutions to contemporary privacy issues, directly fund Centers of Excellence to conduct research in partnership with industry and academia, and host or participate in symposia and other programs that focus specifically on the areas where a log-jam needs to be broken. The increased cooperation and free flow of ideas resulting from these collaborations can contribute substantially to the development and implementation of privacy practices that benefit consumers.

The Department should focus these efforts on developing privacy-enhancing technologies, developing privacy-enhancing business practices, and standardizing the definitions of "personal" and "sensitive" information and related terms.

#### 1. Developing privacy-enhancing technologies

As described in Section III.A, great strides have been made in developing privacy-enhancing technologies to increase consumer comprehension of how their information is used online and what their privacy options are. Despite their success, however, these technologies only represent preliminary steps in the "featurization" of data use – that is, the full integration of meaningful, understandable privacy notices into online applications and features.[41] In this regard, the demonstrated use of advanced disclosures to better present notice and choice, such as through the use of the Power I icon, is progress but not the end goal. "Evolving" these methods of notice

[41] One proposal for such featurization is the "use-based" model of privacy mentioned in the *NOI*, which would define the types of uses for which advertisers could employ personal information as opposed to regulating what personal information can be collected. *NOI* at 21,229. FPF recommends that the Department *not* settle on any one model of privacy at this point, instead supporting research about multiple models to ensure that it considers all viable options. Proceeding in this fashion will also help ensure the robustness of the model ultimately chosen.

provides the best opportunity to increase consumer transparency and choice, and to consequently develop consumer trust for the future. To that end, the Department should seek to focus further research on the development of evolving privacy-enhancing technologies designed to ensure consumer transparency and choice regarding the online use of their information, building upon the developments already achieved in this field.

One area on which the Department can focus is the development of identity management solutions. As noted in the *NOI*, the Federal Communications Commission's National Broadband Plan recommended developing identity management solutions to assist consumers in managing their data.[42] Online businesses that collect large amounts of personal information from users, such as social networking websites, have also introduced applications and settings that allow users to exercise a certain level of control over their online identities. Recent research has also attempted to explore the feasibility of enacting identity management solutions and the attendant risks to privacy.[43]

At this time when both government agencies and industry are experimenting with these identity management solutions, we are at a critical turning point. Identity controls can either be an enabler of privacy advances, providing both additional value and greater user control over data, or if done improperly can provide a grave threat to users' control over their information.[44] At the same time, there is relatively little known about the effectiveness of available identity management solutions, and what aspects of these solutions are best at enhancing consumer privacy while still maintaining value for business. Therefore, the Department should consider

---

[42] *NOI* at 21,231.

[43] *See, e.g.*, Susan Landau et al., *Achieving Privacy in a Federated Identity Management System*, Financial Cryptography & Data Security '09, *available at* http://labs.oracle.com/people/slandau/Achieving_Privacy.pdf.

[44] *See, e.g.*, *supra* Section III.B.7 on the "Illusion of Control."

sponsoring research or convening a task force that examines recent progress in the development of identity management systems and their benefits to consumers, their effect on the online advertising ecosystem, and their effect on data sharing and personalization business models.

### 2. Developing privacy-enhancing business practices

Many companies fail to commit the resources necessary to ensure online privacy protection. This is often because privacy is an afterthought that follows, rather than is part of, the development of new online products, services, and technologies. To ensure that proper attention is given to privacy, companies must embrace the concept of "Privacy by Design" – considering privacy at every step of the research and development process.[45] The Department should promote "Privacy by Design" as a fundamental for companies engaged in online activities.

### 3. Standardizing the definitions of "personal" and "sensitive" information and related terms

As discussed in Section III.B.4, the lack of standardized definitions for "personal information," "sensitive information," "anonymous," and "identifiable" presents several privacy challenges. Varying definitions increase consumer confusion and make it more difficult for data custodians to understand and comply with their data protection obligations. These differences also make it more difficult for website operators and applications developers to communicate privacy choices to users. The development of uniform definitions and standards for the usage of these terms can help consumers better understand their privacy options and make informed decisions. The Department, leveraging the competencies of NIST, should sponsor research or support a task force to develop such uniform definitions and use standards. These should include,

[45] A proponent of such a system is the Privacy Commissioner of Ontario, Dr. Ann Cavoukian, who developed a Privacy by Design framework that provides a set of guiding principles encouraging information system owners to proactively and pervasively incorporate privacy protections into the design of their systems. *See* Privacy by Design, http://privacybydesign.ca (last visited June 14, 2010).

at a minimum, definitions for the terms "personal information," "sensitive information," "anonymous," and "identifiable." The Department should also recommend to the Administration that it undertake efforts to promote the adoption of uniform definitions and use standards for these terms.

### B. The Department Should Recommend that the Administration Take Steps to More Aggressively Use Existing Legal Tools to Investigate and Enforce Against the Misuse of Personal Data

FPF recommends that the Department, in its forthcoming Report,[46] recommend that the existing legal tools available at the federal level be more aggressively used to investigate and enforce against the misuse of personal data. In addition to the civil authority vested in administrative and independent agencies, the Department of Justice has authority to proceed against criminals involved in spam, spyware, phishing, identity theft, malware, and "malvertising," though enforcement against these crimes has not been as robust as it can be.[47]

For example, malvertising occurs when criminal groups purchase banner ads from unsuspecting ad networks and implant malware in the computer code displaying the ads, after which the ads attack the computers of those who simply view the banners. Despite having an impact that has affected millions of users and thousands of networks, civil enforcement and industry self-regulatory or individual company measures have been unable to respond sufficiently to this concern, due to the need for coordination across many industries and business models.

---

[46] *See NOI* at 21,226.

[47] These are, of course, not the only crimes committed over the Internet. But by addressing these cybercrimes used to perpetrate fraud against consumers online, the Department could provide the needed impetus to convene the key actors needed to advance solutions to these problems before they undermine consumer confidence in using the Internet and slow the growth of electronic commerce.

While improvement in online privacy practices by legitimate companies will go far to build consumer confidence and thus help ensure the continued growth of online commerce so essential to the country's economic well-being, more robust law enforcement against illegal online conduct such as malvertising also must play a critical role in making the Internet a safe place for consumers to share data.

### C. The Department Could Play a Unique Role in Supporting the Role of Chief Privacy Officer

Over the past decade, the role of Chief Privacy Officer has become a critical one for thousands of businesses seeking to ensure and enhance their data practices. Information about this role in the U.S. job market is limited to occasional surveys by the International Association of Privacy Professionals or the Ponemon Institute.[48] The Department could play a key role in identifying the numbers of such professionals across various industry sectors and could help advance the importance of this job function as a central way for companies to advance their data protection practices.

[48] *See, e.g.*, INT'L ASS'N OF PRIVACY PROF'LS, A CALL FOR AGILITY: THE NEXT-GENERATION PRIVACY PROFESSIONAL (2010), *available at* http://privacyassociation.org/images/uploads/IAPP%20Future%20of%20Privacy_Final%20Client.pdf; PONEMON INSTITUTE, PRIVACY & DATA PROTECTION PRACTICES: BENCHMARK STUDY OF THE FINANCIAL SERVICES INDUSTRY (2010), *available at* http://offers.compuware.com/register?cid=70170000000J6xN.

## V. CONCLUSION

FPF commends the Department for its examination of online privacy and looks forward to further participation in the public-private dialogue about ways to improve privacy protections for Americans. We hope that the foregoing illumination of innovative practices and areas for improvement, as well as our recommendations for further Department engagement, are a useful contribution.

June 14, 2010

Respectfully submitted,

_____

Christopher Wolf
Co-Chair, The Future of Privacy Forum
Bret Cohen
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, DC 20004
202-637-8834
202-637-5910 (fax)
christopher.wolf@hoganlovells.com
Counsel for THE FUTURE OF PRIVACY FORUM

Jules Polonetsky
Co-Chair and Director, The Future of Privacy Forum
919 18th Street NW
Washington, DC 20036
202-713-9466
julespol@futureofprivacy.org

Christine N. Jones
General Counsel
cjones@godaddy.com

14455 N. Hayden Road
Suite 219
Scottsdale, AZ 85260

D 480.505.8812
F 480.624.2546

June 7, 2010

U.S. Department of Commerce
National Telecommunications Administration
1401 Constitution Avenue, N.W., Room 4725
Washington, D.C. 20230

Re: Internet Policy Task Force
Information Privacy and Innovation in the Internet Economy
Notice of Inquiry

Dear Sir or Madam,

Please accept these comments in response to your Notice of Inquiry dated April 23, 2010.

The Go Daddy Group, Inc. is an Arizona company which consists of eight ICANN-accredited registrars, including GoDaddy.com, Inc. Today, Go Daddy is the world's largest domain name registrar, with over 41 million domain names under management. We are also a leading provider of secure website hosting, and other products and services that enable individuals and businesses to establish, maintain and evolve a presence on the Internet.

Go Daddy's position as the industry leader in the domain name registration and web hosting space gives us unique insight into the current challenges facing businesses that collect and use consumer information online. Go Daddy not only collects and utilizes the personal information of its millions of customers, but it hosts millions of websites through which its customers collect and use the personal information of millions of other online consumers. We are therefore responsible for the privacy and data security of the information of an enormous amount of Internet users, and we take our role extremely seriously.

In the absence of comprehensive federal privacy legislation, Go Daddy has successfully worked within and expanded upon existing privacy standards and guidelines to establish a wide array of security measures that protect the personal information of our customers. As recommended by the Federal Trade Commission, we believe that all companies collecting or storing consumer data should establish reasonable privacy

and security measures to protect such information, and should retain such data only as long as necessary. The FTC also mandates the use of appropriate data security technology and continuous internal employee training regarding privacy and security concerns, and Go Daddy has proactively implemented such measures.

Whenever possible, we allow our customers and users of our websites to opt-out of various types of information collection, and we have voluntarily instituted affirmative opt-in preferences for marketing and other types of optional communications and information collection programs. We do not sell our customers' information to third parties for any purpose, and we do not utilize or disclose the consumer information collected by our customers on their hosted websites. We educate and encourage our customers to utilize similar online privacy practices with respect to their own businesses and websites. We also offer a variety of online security products to help individuals and businesses protect their data.

**The Existing "Notice and Choice" Framework is Sufficient to Protect Consumers' Privacy Rights, Particularly With Respect to Online Behavioral Advertising**

Go Daddy believes that the existing privacy notice and choice framework is sufficient to protect consumer privacy rights, so long as it is consistently applied and vigorously enforced. We understand that the success of our business relies almost entirely on the trust of our users. To the extent that websites do not provide adequate notice of their privacy practices, or give users a choice as to how their information is used, their businesses will quickly fail. Thus, our approach to privacy, and the approach we advocate for our customers, combines front-end transparency, meaningful choice, and user education with back-end protections for data that limit how much information and for how long personal identifiers are maintained.

Go Daddy is particularly interested in the application of the notice and choice principles to online behavioral advertising. Online behavioral advertising supports the advertising and revenues necessary to encourage free Web content, while greatly reducing the amount of unwanted and irrelevant advertisements received by Internet users. The limitation of such advertising could undermine the viability of many online sites that provide free Internet content and services, resulting in the suppression of innovation, the limitation of choice, and an increase in prices for consumers. We therefore believe that behavioral advertising should be expressly permitted in any future federal privacy legislation.

Although Go Daddy supports the ability of online advertisers to make use of behavioral advertising, we are aware of the potential privacy concerns arising from this practice. We are also well-versed in the numerous

precautions and security measures that are in place to guard against the misuse or leaks of data collected through behavioral advertising.

First, there is a minimal risk of significant privacy breaches or data leaks associated with behavioral advertising. Online advertisers engaged in behavioral advertising do not collect sensitive personal information, such as user names, credit card numbers, Social Security numbers, credit histories or financial account information. Moreover, information collected is not linked to any specific individual. The information collected through behavioral advertising is connected only to unique codes identifying specific computers ("IP addresses"), and is not connected to specific individuals.

Second, as recommended by the Federal Trade Commission, all companies collecting or storing Internet user data should establish reasonable security measures to protect such information, and should retain the data only as long as necessary. The FTC also mandates the use of appropriate data security technology and continuous internal employee training regarding privacy and security concerns.

Third, companies engaged in behavioral advertising should provide clear, easy-to understand notice to affected Internet users before using collected data, and ensure that opt-out procedures exist and are user-friendly. Many behavioral advertisers currently allow the user to "opt-out" of the program; however, Internet users may not readily know how to opt-out or it may seem overly burdensome to them. Go Daddy supports mandatory disclosure of the specific networks with which the site intends to share the consumer's information, and the use of prominent, understandable, easy-to-use opt-out procedures, consistent with the existing notice and choice framework.

**Go Daddy Supports the Enactment of Federal Consumer Privacy Legislation That Would Preempt Conflicting State Law and Could Be Used to Work Toward International Harmonization**

Although Go Daddy has successfully implemented self-regulatory privacy measures, as an interstate and global business we support the need for comprehensive federal privacy legislation that is generally consistent with other privacy laws around the world.

Currently, numerous state, federal and international laws and regulations impose a mixture of consumer privacy obligations on companies that collect information via the Internet. Stringent privacy and data protection laws passed in certain states, most recently Massachusetts and Nevada, purport to apply to all companies that collect personal information from residents of those states, regardless of the enacting state's general or

personal jurisdiction over the collecting entity. Thus, a sole proprietorship based in Arizona is "prohibited" from collecting personal information from even one Massachusetts resident unless the Arizona entity has ensured its compliance with the Massachusetts data security law. Similarly, U.S. businesses that collect the personal information of residents of other countries, most notably in the EU, are purportedly required to comply with the laws of those jurisdictions.

It is extremely difficult for private sector entities, particularly the small and medium-sized businesses which form a vast majority of online commerce, to sift through the morass of federal, state and international laws to determine which standards apply to them. The result is an uneven set of privacy protections for consumers and a stifling effect on interstate and international business. Go Daddy therefore supports the enactment of federal consumer privacy legislation, based on the notice and choice framework, which would create uniform U.S. privacy standards and could be used to work toward international harmonization.

Any proposed federal privacy legislation should require organizations to take reasonable steps to safeguard personal information, appropriate to the sensitivity of the information. We further believe that such legislation should apply to the collection of personal information both online and offline, in hard or soft copy. To avoid a continuation of the current state-by-state application of privacy laws in the U.S., we believe that any federal legislation should provide a baseline standard of protection that preempts any conflicting state or local law. Enforcement should be limited to experienced, competent consumer protection agencies, and penalties should be clearly defined.

Thank you for the opportunity to provide our perspective on these important issues. The practical application of proposed legislative and regulatory measures related to consumer privacy is critical to our business and to the businesses operated by our millions of customers.

Very truly yours,

GO DADDY.COM, INC.

Christine N. Jones
Executive Vice President, General
Counsel and Corporate Secretary

CNJ:sd

**U.S. Department of Commerce**
**Docket No. 100402174-0175-01**
**Information Privacy and Innovation in the Internet Economy**

## Comments of Google Inc.

Google thanks the Department of Commerce – including the Secretary, the National Telecommunications and Information Administration, the International Trade Administration, and the National Institute of Standards and Technology – for its welcome focus on privacy and online innovation.

It is difficult to overstate the social and economic benefits of the Internet for the United States and for the world. More than any technology in history, it has empowered entrepreneurs to bring their ideas directly to market – without tolls, without gatekeepers, without limitations. And by bringing the world's knowledge to the fingertips of each connected individual, the Internet has begun to unleash the true power of information to help consumers, create jobs, ensure government transparency, and achieve other societal benefits.

The Department of Commerce has a broad mandate to advance economic growth, jobs, and opportunities for the American people, as well as cross-functional responsibilities in trade, technology, entrepreneurship, economic development, environmental stewardship, and statistical research and analysis. The Department also has a strong history of thoughtful Internet policymaking. In the 1990s, the Department played a leadership role in the federal government's e-commerce activities, which encouraged and spurred responsible private sector leadership on issues ranging from privacy, private international law, and Internet governance. The Department's role and track record make it ideally suited to play a central role in developing the policies that will continue to organize, govern, and nurture the Internet.

The Department's Notice of Inquiry is timely and important. Existing regulatory frameworks for privacy, both domestic and international, are incomplete and sometimes in tension with one another to the detriment of both Internet users and online providers.

Google therefore urges the Department to work to develop comprehensive, baseline privacy rules that both help establish user trust and support the global data flows necessary for building new content and services in the data-centric Web. Such a framework also offers a consistent platform for providers to develop innovative, flexible tools that empower users to make privacy choices and self-regulatory structures that can keep pace with changing technology. The Department has a unique opportunity to shape this unified, comprehensive privacy framework in the U.S. and to encourage consistent, pro-innovation rules internationally.

Google has been a leader in developing user-friendly tools to inform and empower our users, including promoting data portability, creating educational privacy videos, developing an Ads Preferences Manager that allows users to see and control what interests are associated with their browser, and providing a centralized dashboard designed to help users view their information and control their individual privacy settings. To protect our users' communications, we encrypt all Gmail traffic by default, and we remain the only major search provider to allow users to encrypt search queries. These types of privacy tools educate and empower consumers, provide enhanced transparency, improve security, and offer meaningful choice and control. We have attached to this submission our recent privacy comments filed with the Federal Trade Commission, which expand on these tools and Google's approach to privacy.

In the comments below, we apply some of what we have learned about privacy to address the strengths and weaknesses of existing domestic and international privacy regulations and their impact on users and innovation. We then suggest ideas for how to conceive a comprehensive, baseline privacy framework and about how the Department can play a central role both here and abroad in developing this framework.

## Domestic Privacy Regulation

### Although the U.S. privacy system needs a comprehensive vision, the system has protected online users and encouraged innovation

Although Google believes that the U.S. would benefit from a unified, principles-based legal framework specific to privacy, we nevertheless believe that there are real and effective protections established under U.S. privacy laws and regulations. Moreover, Internet innovation has flourished in the United States in part *because* of the flexible nature of U.S. privacy laws and an enforcement framework that places substance over form. Accordingly, we believe that before policy makers discuss what could be improved in the domestic arena they must start with the very real successes of the current system.

Between sectoral laws, Federal Trade Commission policy and enforcement, state consumer protection laws, and self-regulation, the U.S. has assembled a system that protects user privacy and supports innovation. In fact, the success of this system is perhaps the best evidence that user privacy and data innovation are not mutually exclusive.

Increasingly, privacy is not merely a laws-based construct, but rather one that is driven by technological innovation and evolving consumer expectations. As Professors Kenneth Bamberger and Deirdre Mulligan recently explained in the *Stanford Law Review*, while the U.S. may suffer from a incomplete set of "privacy on the books" (the privacy laws that establish minimum standards for the protection of information) it has developed a flexible and powerful tradition of "privacy on the ground" – the practices and policies devised and implemented to meet evolving consumer expectations, as well as comply with existing privacy laws.

Adherence to privacy laws in a rapidly changing environment is necessary but by itself will not address consumer expectations. Certain approaches, however, provide a better framework to facilitate adaptation in light of evolving consumer expectations. The Gramm-Leach-Bliley Act (GLBA), for example, requires financial institutions to protect the "security and confidentiality of

customer records and information" while eschewing specific technological mandates that would effectively wed financial institutions to specific technology solutions. Under the GLBA Safeguards Rule, financial institutions have the flexibility to implement privacy and security protocols that address new and emerging threats to the security and confidentiality of customer records and information. A more prescriptive approach – *e.g.*, mandating the use of specific technologies or administrative protocols – would likely constrain the ability of financial institutions to design and implement solutions that are attuned to the unique privacy challenges presented by specific products and services.

The FTC, too, has used its authority to stop unfair and deceptive trade practices to develop flexible, standards-based privacy rules that reflect consumer expectations. Under its existing statutory authority, the FTC has penalized bad actors, enforced privacy promises, and sent important signals about evolving standards for proper notice, choice, consent, and data security. The FTC communicates its expectations clearly, effectively, and prospectively to protect consumer privacy without unnecessarily disrupting legitimate business practices and innovation.

In its enforcement role, the FTC has sought to articulate consumer expectations in the privacy and data security arena – asserting itself in cases where specific practices failed in its view to satisfy evolving consumer expectations concerning privacy and data security. As Professors Bamberger and Mulligan noted, "a key to the effectiveness of FTC enforcement authority is the agency's ability to respond to harmful outcomes by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change – the very opposite of the rule-based compliance approach frequently embodied in regulation."

The FTC's guidance in privacy and data security enforcement compels both the subjects of such enforcement actions and others in the industry to embrace forward-looking and creative solutions to new and emerging privacy and data security issues. Simultaneously, the Commission seeks to educate consumers about emerging privacy issues. Finally, the Commission and staff use roundtables and town hall meetings to engage in a discussion with industry and advocates, and to offer flexible guidance based on information about evolving user needs and provider practices discussed in those settings. Public dialogue with industry and advocates helps to develop consensus about emerging issues and to create incentives for industry to identify appropriate solutions. Its self-regulatory guidance for the online advertising industry, for instance, has helped spur broad industry support for improved advertising notice and opt-out functionality.

To provide greater context, it is instructive to compare Internet innovation in the U.S. and the European Union. For instance, many of the Internet advertising companies in the U.S. were established at a time when European regulatory models already presented a barrier to entry in terms of the need for implementing varying and complex data protection legislation. In fact, the European Commission itself admitted, in 2003, that the European data protection regime had failed to anticipate new technological developments. Noting the huge changes in "the means of collecting personal information," the European Commission wondered "whether legislation can fully cope with some of these challenges." This is precisely the advantage of the flexible U.S. approach.

**Despite successes, further consistency and comprehensiveness in U.S. privacy regulation will help strengthen user privacy and promote continued innovation**

Although we believe that privacy regulation and enforcement mechanisms in the United States have both encouraged Internet innovation and evolved to meet consumer expectations, there are improvements to the U.S. system that the Department can help promote. Inconsistency and gaps in the rules create unnecessary costs and burdens to innovation and undermine user trust.

Generally, Internet users neither expect nor want different baseline privacy rules based either on the type of provider processing their information, the type of device or service that is being used, or the local jurisdiction in which they or the provider reside. In many respects, our current legal framework often creates precisely these distinctions – upsetting users' reasonable privacy expectations and complicating the competitive marketplace with inequitable rules. For instance, privacy can be implicated by offline practices just as much as in online environments. Proposed privacy legislation at both the state and federal level, however, often ignores the former while regulating the latter. A comprehensive approach to privacy must focus on both offline and online privacy and must seek to avoid wherever possible artificial distinctions.

The Electronic Privacy Communications Act starkly illustrates the problems created by privacy laws that are oriented toward technologies rather than baseline standards. Enacted in 1986, ECPA made assumptions about a static technology marketplace that bears little resemblance to the way in which individuals communicate, interact, and engage on the Internet in 2010. The advent of "cloud computing" – where users store their data with online providers and access them via the Internet – is leading to a vast migration of data from personal computers, filing cabinets, and offices to remote third-party servers. ECPA, however, affords lesser protections to e-mail communications based on where messages are stored, whether messages have been opened, and how long messages have existed. Such distinctions belie consumer expectations concerning the privacy of e-mail communications. The Digital Due Process Coalition, of which Google is a leading member, has proposed ways to update ECPA to ensure that its privacy protections are consistent with privacy expectations.

In addition, state laws occasionally impose rigid technology mandates that embody a "checklist" mentality to privacy and data security that stymies innovation and does not serve online users. In Nevada, for example, a business entity that either transfers "personal information" outside of its secure system or moves storage devices containing personal information beyond its physical or logical boundaries must use encryption to protect this information. Even if less expensive and more effective technologies become available, Nevada statutorily prohibits businesses from deploying such technologies to protect personal information. If, however, a business accepts payment cards from Nevada residents, the business must comply with the current version of the Payment Card Industry Data Security Standard, which does not necessarily mandate encryption. In a borderless environment such as the Internet, it is often impossible to ascertain the state residency of a specific user, much less deploy a specific technology solution based on nuances in state laws. Although well-intentioned, these laws often provide few appreciable benefits to consumers while imposing substantial burdens on and creating significant legal risks for Internet companies.

As we outline below, the Department can play a vital role in bringing greater consistency and comprehensiveness to domestic privacy regulation by formulating a usable, pro-innovation, pro-consumer framework for privacy together with the ongoing efforts at the FTC and in Congress.

## International Privacy Regulation

### Inconsistencies in the international patchwork of data protection rules have economic costs and impact free expression without corresponding benefit to user privacy

*Economic cost*

It is difficult to quantify the economic impact of inconsistent privacy regulations, but there can be little doubt that the growth of online, data-intensive services will suffer. Information, when collected and used responsibly and transparently, can offer tremendous value to users. Google, for instance, has used non-personally-identifiable data collected from users of our search service to add new features – such as spelling correction and suggested results – and to develop entirely new services, such as Flu Trends. Google engineers discovered that certain search terms are good indicators of flu activity, and developed Google Flu Trends using aggregated Google search data to estimate flu activity. This allows health officials, the media, and the public to learn about local flu outbreaks sooner than using traditional public health methods. Researchers have used Google Trends data and other sources like Twitter to develop economic trend data ahead of official numbers. The value of innovative services like this would be lessened or lost completely by rigid or inconsistent data protection rules.

Researchers have drawn similar conclusions. Canadian and U.S. academics recently found that E.U. data protection laws reduced effectiveness of online advertising, as measured by purchase intent, by over 65% compared to other countries. While there may be important user benefits to more restrictive data use policies not addressed by this study, policy makers should take a close look to determine if user privacy can be protected at lower cost to business and innovation.

The difficulties and costs of international compliance are most obvious for global cloud-based providers. Cloud computing providers, including Google, allocate storage and processing resources in the network as efficiently as possible through an essentially global infrastructure of data centers. The most prominent international data protection laws were, in contrast, developed in an era of bulk data transfers, stable databases, and location-specific processing. The Department should work with its international colleagues toward a unified and flexible set of multilateral agreements and national standards that preserve user privacy and trust and encourage the growth of the cloud.

*Impact on global free expression*

Google acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression.

Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors. While we cabin this right

in important ways – including individual liability for defamation or harmful speech – it is invaluable to the ability to exercise freedom of expression.

As the Web evolves, free expression can be affected by rigid application of access rights and mandated opt-in policies for information collection. For more than a decade, scholars such as Fred Cate have discussed the potential tension between the U.S. First Amendment protection of free information flow and some international models of data protection. Moreover, while appropriate in certain circumstances, broad opt-in requirements can create perverse incentives for companies to collect more identifying information than necessary and to obtain "consent" in inappropriate or confusing ways. If all online behavior were traced to an authenticated identity to preserve proof of consent or allow rights of access, the free expression afforded by anonymous web surfing would be jeopardized.

International privacy rules have unfortunately been applied in ways that implicate free expression rights. As we have recently seen in several different cases, liability for third party intermediaries under data protection law in some countries remains unclear. An Italian court recently held three Google executives criminally liable for a user's uploading of an illegal video – a result at odds with widely accepted theories of intermediary liability in the U.S. and elsewhere. As the Center for Democracy and Technology noted in a recent report:

> Protecting intermediaries from liability is critical for preserving the Internet as a space for free expression and access to information, thereby supporting innovation and economic development goals. User-generated content sites in particular have become vital forums for all manner of expression, from economic and political participation to forging new communities and interacting with family and friends. If liability concerns force private intermediaries to close down these forums, then the expressive and economic potential of [information and telecommunication] technologies will be diminished. Governments everywhere should adopt policies that protect intermediaries as critical actors in promoting innovation, creativity and human development.

Different interpretations of third party liability create uncertainty, provider risk, and threats to free expression that chill innovation and growth of Internet services.

*International harmonization*

Compliance with differing standards imposes costs without obvious user benefits. International data protection law is far from harmonized, and attempts to improve consistency have been disappointing. The European Commission directive on data protection has been implemented variously in the member states, and interpretation of national law by data protection authorities have created even greater variations. Global companies that operate in Europe are subject to different compliance regimes in each of the Commission's 27 member states. Many such countries require elaborate filings and prior approvals for data transfers – even when using a mechanism that has been pre-approved by the European Commission. As noted in one recent paper, "The International Law Commission (ILC) has stated that 'the international binding and non binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles' of data protection; however, it is doubtful whether such principles have won broad recognition among States."

The Department of Commerce's experience with negotiating and maintaining the U.S./EU Safe Harbor Framework and its leading role at Asia Pacific Economic Cooperation makes it the appropriate United States Government agency to lead the U.S. in discussions toward greater global privacy harmonization. Moreover, the Department can encourage global recognition of the real strengths of the current U.S. system of "on the ground" enforcement and flexible standards.

We encourage the Department to play a leading and active role in establishing a global privacy framework that encourages innovation and allows for the global flow of data. There is widespread recognition that industry and users need a widely accepted and practical international standard of privacy protection if online commerce is to flourish. The APEC Privacy Framework is a good step toward helping member countries develop privacy laws and regulations that achieve effective privacy protection and continuity for cross-border information flows. We encourage similar efforts to create a set of global privacy principles.

Similarly, the Organization for Economic Cooperation and Development is this year marking the 30th anniversary of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The review of these Guidelines, which have served as the foundation for virtually all privacy laws around the world, offers another important opportunity for the Department of Commerce to lead a thoughtful effort to continue protecting privacy through the harmonization of standards and the enhancement of mutual recognition among member countries.

## Towards a Comprehensive, Baseline Privacy Framework

### The Department should develop and encourage the adoption of a comprehensive framework for unifying legal standards and creating a platform for responsible innovation

The solution to the challenges posed by existing incomplete and inconsistent privacy standards is a unified, comprehensive, and flexible privacy framework that can encourage harmonization of law and multilateral agreements on data transfers and enforcement. Developing such a framework will be a long process and we look forward to working closely with the Department on this issue. To begin, however, we can articulate several foundational characteristics of such a framework.

*It must be comprehensive*

To protect users and offer consistency to providers, the privacy framework must cover all collection and use of data, all providers, and all manner of privacy harms. While not a complete list, the framework should include the following:

- **Even-handed application.** A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline data collection and processing should, where reasonable, involve similar data protection obligations.

- **Recognition of benefits and costs.** As with any regulatory policy, it is appropriate to examine the benefits and costs of regulatory initiatives in this area, including explicit

attention to actual harm and compliance costs.

- **Security.** We pride ourselves at Google for industry-leading security features, including use of encryption for our search and Gmail services. The privacy framework should promote reasonable security principles – developed under evolving standards formulated by responsible industry actors and experts and reflective of current best practices. This will offer users a consistent, dependable and enforceable level of protection while offering clear, flexible guidelines for providers.

- **Clear process for compelled access.** As we have discussed above, the U.S. law governing government access to stored communications is outdated and out of step with what is reasonably expected by those who use cloud computing services. The problems in the law threaten the growth, adoption, and innovation of cloud technologies without a corresponding benefit. As part of the Digital Due Process coalition, we are working to address this issue. A privacy framework should also include clear rules for civil litigant and other compelled access.

*It must be a baseline on which providers can innovate*

Perhaps most importantly, a pro-innovation privacy framework offers providers the flexibility to both develop self-regulatory structures and individually innovate in privacy practices and tools. The advertising industry and online publisher efforts to develop self-regulatory rules for interest-based advertising (IBA, for short), for example, are a strong example of the need for and utility of industry-driven efforts.

Beyond cooperative industry efforts, baseline, principles-based rules give room for individual providers to innovate in the privacy space. Google, for its part, offers a number of industry-leading privacy tools:

- Prior to the industry IBA effort, for instance, Google launched its own IBA product with a number of groundbreaking privacy features in place. Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google advertisement. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether.

- Google also offers leading options for data portability. For Google, providing our users with control over their personal information must also mean giving them the ability to easily take data with them if they decide to leave. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, our "Data Liberation Front" allows our users to "liberate" data if they choose to switch providers or to stop using one of our services.

- Google developed the Google Dashboard to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts. With the Dashboard, a user can see and edit the personally identifiable data stored with her individual Google account.

As noted above, more information on our innovative privacy tools is available in the attached comments, which we recently filed with the FTC.

Continued innovation in the privacy space is vital for users. Unfortunately, compliance-based rules can lock providers into a specific privacy model. A principles-based model encourages innovation and competition in privacy tools.

A baseline framework needs to encourage the development of innovative tools like these. We believe that stable, baseline principles set by regulation can permit flexible, adaptive structures to develop on top – much like the stable protocols and standards at the physical and network layers of the Internet allows flexible and innovative development at the content and application layers. With comprehensive, baseline privacy legislation establishing ground rules for all providers, self-regulatory standards and best practices of responsible industry actors will evolve over time. On top of that structure, individual providers will be free (and encouraged) to create innovative privacy tools and policies rather than stick with potentially outdated compliance structures.

*How the Department can lead*

The Department can lead in several important areas including the following:

- **Leverage its intra- and inter-agency competencies.** The Department is well-positioned to draw from relevant expertise at NTIA, ITA, and NIST. It can also take this expertise to help develop a privacy framework and inform the ongoing efforts at the FTC and in Congress.

- **Continue to work with international partners.** The Department should continue working with national data protection authorities as well as other foreign agencies and representatives to build international consensus around a privacy framework that recognizes the value of data and the need for consistency and, where consistency cannot be achieved, mutual respect and recognition.

- **Draw from experience and promote dialog.** The Department has a long history of seeking neutral economic and technological evidence. It should draw on this expertise to encourage innovation and competition in pro-privacy tools; to support and develop objective forums for gathering, analyzing, and reporting data on economic impact of privacy regulation; and to host discussions involving government, industry, and non-governmental organizations about emerging technology and associated privacy issues.

* * *

Google thanks the Department for this opportunity to comment, and urges its continued involvement in the privacy space. The Internet, cloud services, and data innovation will drive the U.S. and world economies for years to come. Just as the Department showed global leadership in early Internet regulatory policy, it should lead in the creation of sensible and strong baseline privacy principles. Google stands ready to assist the Department in these and any other efforts to help develop and implement a comprehensive, baseline framework for privacy.

Sincerely,

Pablo L. Chavez
*Director of Public Policy*
*Google Inc.*

Attachment: Comments of Google Inc. in FTC Privacy Roundtable Project

April 14, 2010

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-135 (Annex P2)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Email Address: privacyroundtable@ftc.gov

*VIA EMAIL DELIVERY*

Re: Privacy Roundtables – Comment, Project No. P095416

Dear Mr. Clark:

Google would like to thank the Federal Trade Commission for organizing and hosting its recent "Exploring Privacy" roundtable series and for the opportunity to participate in two of the sessions. The roundtables facilitated critical discussions among consumers, industry, advocacy groups, and academics about challenging privacy issues in the increasingly rich Internet environment. The roundtables also laid an important foundation for the work ahead.

Google believes that, going forward, consumer privacy protection will require a multi-faceted solution that includes industry commitments, enhanced statutory protections, and – with a critical role for the FTC – global engagement. Specifically, Google supports:

- **Strong industry commitments to ensure transparency, user control, and security in Internet services for consumers.** Self-regulatory standards, such as the recent work done in online behavioral advertising, have encouraged companies to innovate in the area of privacy and have enhanced user choices in the environment as a whole.

- **Comprehensive privacy standards and strengthened protections from government intrusion.** Google has long supported comprehensive federal privacy legislation to establish baseline privacy protections for consumers. In addition, Google recently announced its support for the reform of federal law governing government access to online records as part of the Digital Due Process coalition (www.digitalddueprocess.org).

- **FTC leadership in the shaping of global privacy standards.** The FTC, in conjunction with the Commerce Department and other stakeholders, has a unique opportunity to develop a workable set of global privacy standards that are comprehensive, flexible, and

> effective. The current patchwork of rules and enforcement across multiple jurisdictions does not provide adequate protection for consumers or sufficient certainty for companies offering services on the global Internet.

We offer these points at a critical inflection point for the Internet. Below, we first discuss some of the ways in which privacy and security manifest at Google. We then suggest some considerations for the Commission as it moves forward. We hope our contributions at the roundtables and our comments below are helpful to the Commission in its ongoing effort to steer a course for privacy in the modern economy.

**Google's approach to privacy**

To give context for our discussion below, we first discuss how Google thinks about privacy internally. Google's motto for product development is "focus on the user and all else will follow." Google has been a leader in developing user-friendly tools to inform and empower our users, including data portability (www.dataliberation.org), educational videos (www.youtube.com/user/googleprivacy), an Ads Preferences Manager that allows users to see and control what interests are associated with their browser (www.google.com/ads/preferences), persistent opt-out cookies (www.google.com/ads/preferences/html/opt-out.html), and a centralized "dashboard" designed to allow users to access their information (www.google.com/dashboard). As Alma Whitten, Google's lead privacy engineer, recently wrote, privacy is "something we think about every day across every level of our company. Why? Because privacy is both good for our users and critical for our business."

> These types of privacy tools educate and empower consumers, provide enhanced transparency, and offer meaningful choice without constraining innovation through rigid standards. Our approach aims to serve the privacy interests of our users as well as our collective interest in maintaining an open, innovation-friendly environment that will continue to drive the U.S. economy for years to come.

On International Data Privacy Day 2010, building on our existing privacy framework, we announced our privacy principles, intended to guide our efforts in pursuit of innovation that respects user privacy. In brief, these guiding principles are: (1) use information to provide our users with valuable products and services, (2) develop products that reflect strong privacy standards and practices, (3) make the collection of personal information transparent, (4) give users meaningful choices to protect their privacy, and (5) be a responsible steward of the information we hold. The principles are located at www.google.com/corporate/privacy_principles.html.

In our experience, designing for transparency and user control in a product is critical in the fluid Internet environment. Making progress requires insight into dynamic user needs and nimbleness to respond quickly to user criticism. At Google, we strive to do this across the range of our products. In fact, in just the last year, we sought to tackle three broad privacy issues that face our industry: (a) transparency and choice in the online advertising ecosystem, (b) easy data portability for cloud-based services, and (c) a comprehensive and useful dashboard of privacy controls for a suite of disparate web services.

**Transparency and choice for interest-based advertising**

In March 2009, Google launched its first interest-based advertising (IBA) product with a number of groundbreaking privacy features in place. As we told our users:

> Many websites, such as news sites and blogs, use Google's AdSense program to show ads on their sites. It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful.

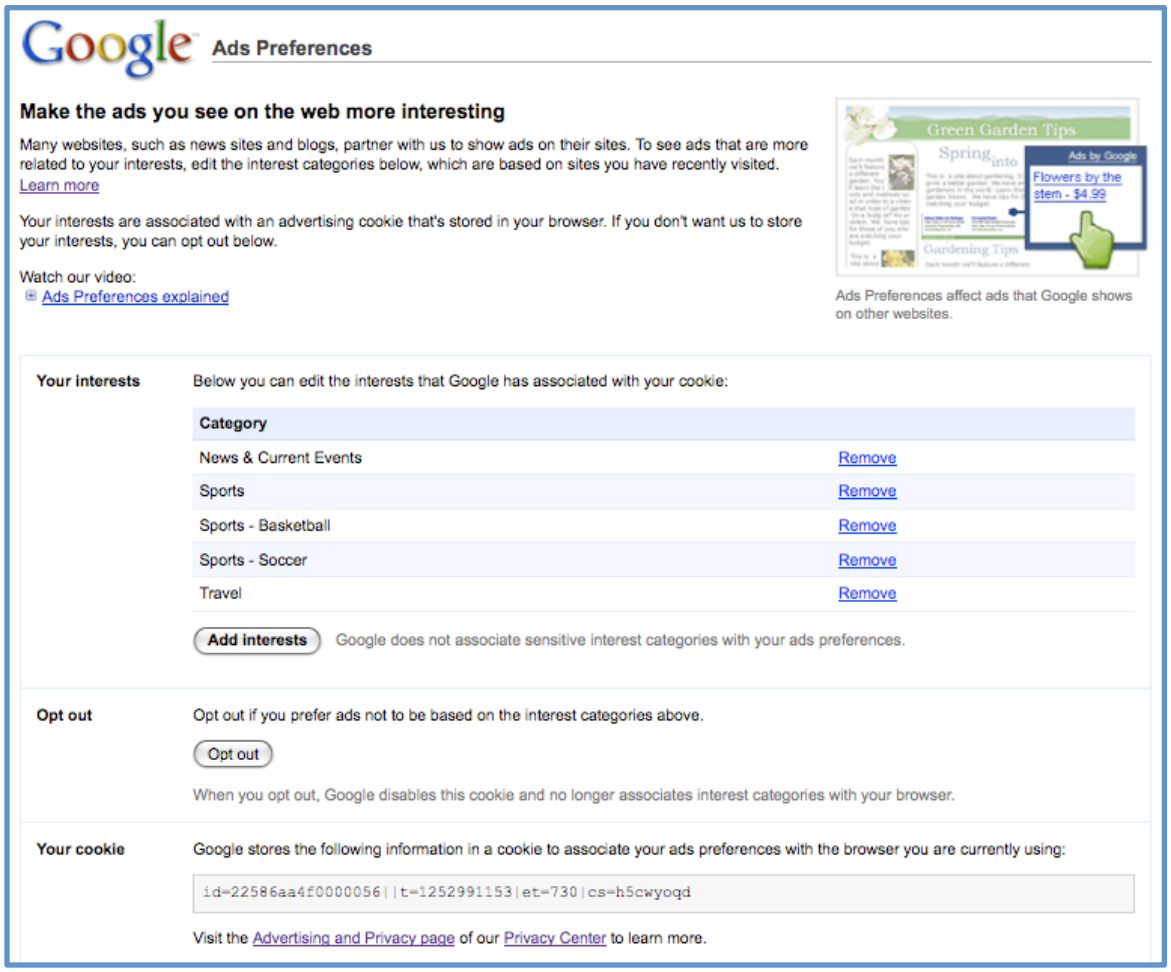
Google's interest-based ads contain notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether.



With our launch of the Ads Preferences Manager (www.google.com/ads/preferences), Google became the first major industry player to empower users to review and edit the interest categories that are associated with their browsers. The Ads Preferences Manager enables a user to see the interest categories Google associates with the cookie stored on her browser, to add interest categories that are relevant to her, and to delete any interest categories that do not apply or that she does not wish to be associated with. Google does not serve interest-based ads based on sensitive interest categories such as health status or categories relating to children under 13.

The Ads Preference Manager also permits users to opt out of interest-based ads altogether. Google implements this opt-out preference by setting an opt-out cookie that has the text "OPTOUT" where a unique cookie ID would otherwise be set. And Google's engineers also developed tools to make our opt-out cookie permanent, even when users clear other cookies from their browser (see

www.google.com/ads/preferences/plugin/). We are encouraged that others are using the open-source code for this plug-in, released by Google, to create their own persistent opt-out tools.

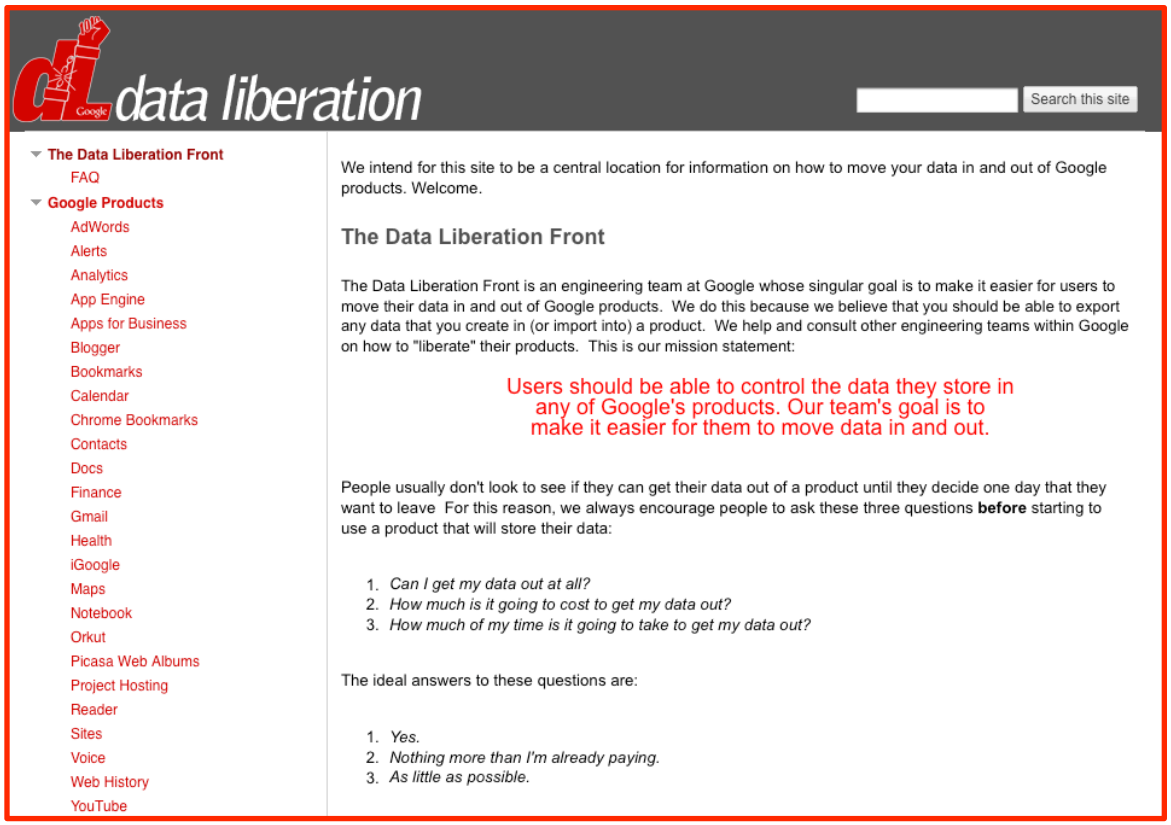



We have recently begun to get information about how users are interacting with the ad preferences manager. While our data is preliminary, we have noted that for every user that has opted out, about four change their interest categories and remain opted in, and about ten do nothing. We take from this that online users appreciate transparency and control, and become more comfortable with data collection and use when they feel it happens on their terms and in full view.

**Data portability**

Providing our users with control over their personal information must also mean giving them the ability to easily take data with them if they decide to leave. Starting with our Gmail service and now covering more than 25 Google products where users create and store personal information, a cadre of Google engineers – self-named the "Data Liberation Front" – has built tools to allow our users to "liberate" data if they choose to switch providers or to stop using one of our services. The critical insight of the Data Liberation Front engineers was to recognize that users should never have to use a service unless they are able to retrieve the content they created, get it out easily and for no more than they're already paying for the service.

Every user of Gmail, Picasa, Reader, YouTube, Calendar, Apps for Business, Docs, iGoogle, Maps, and many other products already have access to data portability tools, and the team continues to work on additional products and services. Detailed information for users is available at www.dataliberation.org.



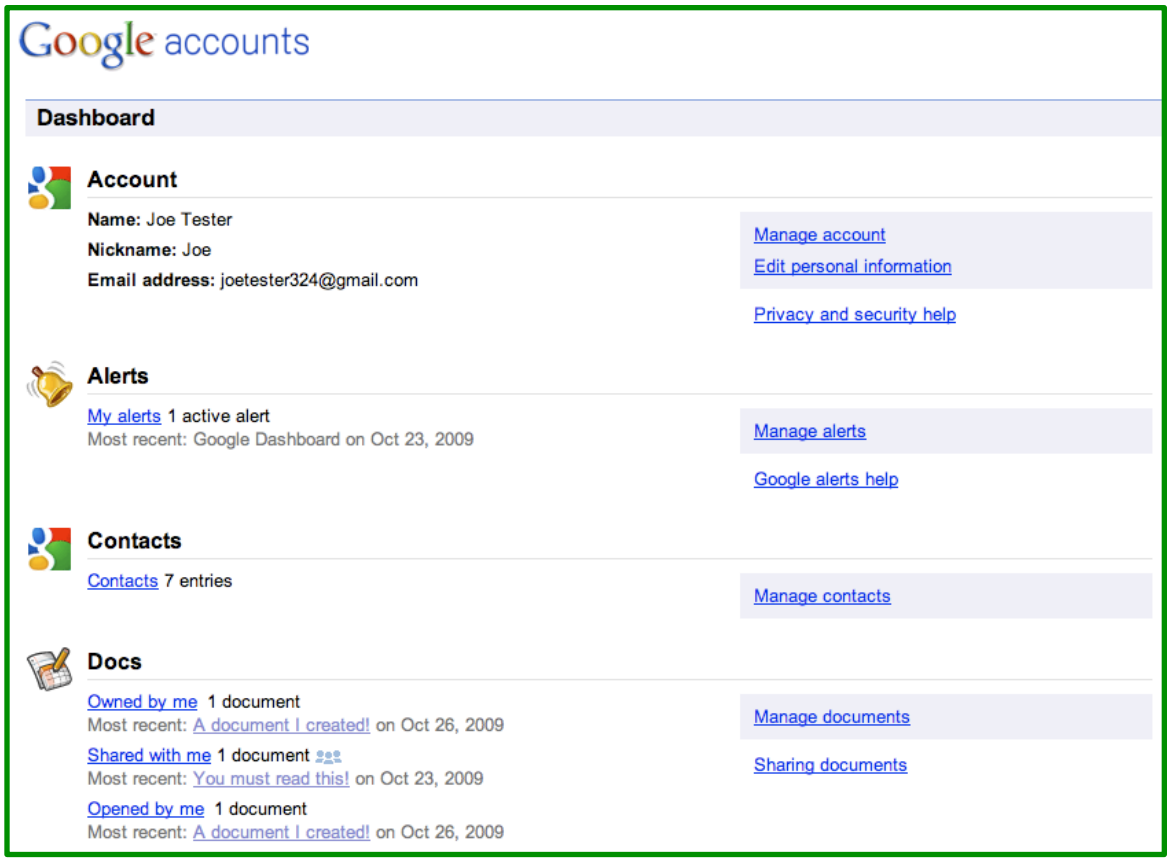

Data portability has benefits for our users and for Google. First, our product teams know just how easy it is for their users to move to a competitor's product, and understand that their success depends upon continuing to be responsive to privacy and product concerns and acting quickly to address them. Second, allowing our users the freedom to leave honors our commitment to put users in control.

In considering the input received by the privacy roundtables and refining its approach to consumer privacy, Google urges the Commission to consider the role that data portability can play in ensuring that consumer facing businesses remain accountable for their privacy choices. The FTC should encourage this kind of "user empowerment by design" as an effective means of ensuring respect for user privacy without chilling innovation.

**The Google Dashboard**

Google developed the Google Dashboard (www.google.com/dashboard) to provide users with a one-stop, easy-to-use control panel to manage the use and storage of personal information associated with their Google accounts. With the Dashboard, a user can see and edit the personally identifiable data stored with her individual Google account. A user also can change her password or password recovery options using Dashboard, and click to manage various products' settings,

contacts stored with the account, or documents created or stored through Google Docs. Dashboard also lets a user manage chat data, by choosing whether or not to save it in her Gmail account.




## Providing stewardship through security

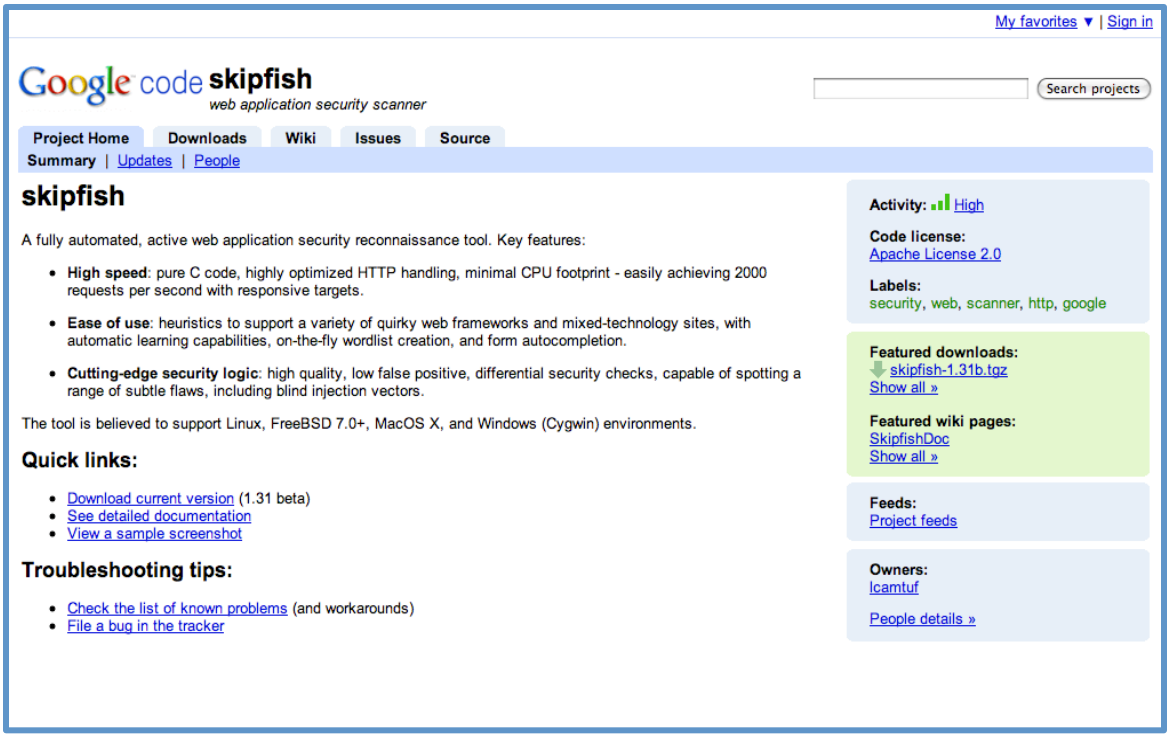
Along with transparency and user control, security plays an important role in maintaining user trust. Google faces complex security challenges while providing services to millions of people every day. We have a world-class team of engineers dedicated to helping secure information, who work regularly with our product managers and engineers to provide design reviews, security consulting, and training and education about security issues.

Security is at the core of our design and development process. For example, Google recently became the first major webmail provider to offer session-wide SSL encryption by default. And last month Google launched a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been hijacked will be notified and given the opportunity to change her password, protecting her own account and her Gmail contacts.

Similarly, we built Google Chrome with security in mind from the beginning, including features such as:

- Safe Browsing, which warns a user before he visits a site that is suspected of phishing or containing malware;
- Sandboxing, which helps prevent web browser processes from harming one another or a user's computer, and
- Automatic updates that deliver security patches to users as quickly as possible.

Google also conducts extensive security research and provides free security resources to the broader Internet community. We make security tools available for free to webmasters to help them operate more secure sites, as well as to application developers to help them build more secure applications. For example, we recently released a tool called "skipfish" under an open source license to help identify web application vulnerabilities through fully automated, active security reconnaissance.




## Policy recommendations

Google is encouraged to see the deep commitment of the FTC to privacy, as represented by its thoughtful approach to these roundtables. As we learned at the roundtables, there is much to be proud of in terms of existing U.S. consumer privacy protections: Congress has set important rules governing data collection, use, and security in many sectors, and the FTC and states have used their general consumer protection authority to protect privacy. Responsible businesses, with guidance from government and advocates, have developed self-regulatory codes that reflect respect for user privacy and security. Moreover, this has been accomplished in ways that have not inhibited innovation and growth in the Internet economy.

We also continue to believe that the principles of transparency and user control are of foundational importance in the existing privacy environment and should continue to be at the core of privacy. While we recognize that traditional fair information practice principles (FIPPs) may need to be

updated, Google is concerned about proposals to discard the notice and choice paradigm altogether. Notice and choice – where "notice" is robust and easy-to-understand and choices are empowering and meaningful – remains a powerful model for the protection of privacy. Moreover, it allows important decisions about product functionality and data uses to remain in the hands of consumers.

We also learned in the roundtables some important lessons about how industry and regulators can improve on the existing framework and adapt it to changing use patterns and conditions. Ensuring adequate privacy and continued innovation will require new ideas and renewed effort.

**The role for industry self-regulatory principles**

We believe that there is an important role for the development and enforcement of industry self-regulatory privacy principles – especially for business models and industries that are inherently fast-moving and innovative. Combining principles with a baseline uniform legislative foundation, discussed below, ensures accountability to consumers for privacy practices. This approach also preserves companies' incentive to innovate, because it reduces the fear that unintentional missteps will result in disproportionate penalties.

Thus, for example, we agree with the Commission's conclusion that self-regulation is the preferred approach for online interest-based advertising, and we support the FTC's efforts to push the industry toward enacting meaningful and enforceable standards in this area. We are also encouraged by recent work by the Interactive Advertising Bureau, Network Advertising Initiative, and others to develop self-regulatory principles for online behavioral advertising. Such self-regulatory efforts could be helpful in other areas of the online ecosystem as well, as they can be developed and adopted in pace with technology and usage.

**Updating privacy laws for the global Internet**

Google supports the passage of a comprehensive federal privacy law that would accomplish several goals, including:

- Building consumer trust;
- Establishing a baseline set of privacy principles, on which self-regulatory efforts could build;
- Establishing a uniform framework for privacy, which would create consistent levels of privacy from one jurisdiction to another; and
- Enacting penalties to deter bad behavior and punish bad actors.

In addition to a baseline standard for transparency and user control, a comprehensive privacy law should include uniform data safeguarding standards, data breach notification procedures, and stronger procedural protections relating to third party access to individuals' information.

As information flows increase, and more and more information is processed and stored in the Internet "cloud," there is a greater need for consistency and trust over the security of online data.

In this vein, stemming from our support for stronger procedural protections relating to government access to information, Google is an active member of Digital Due Process (www.digitaldueprocess.org), a coalition of online businesses, electronic communications services

providers, and leading civil liberties organizations seeking modest but critical reform of federal laws relating to the privacy of electronic communications.

The changes recommended by the coalition are necessary to assure that users of cloud computing services are protected against unreasonable searches and seizures of digital content, and to ensure that U.S. providers of such services can compete effectively with offshore providers. The FTC, too, should encourage the Administration and Congress to update the Electronic Communications Privacy Act to ensure consistent government standards for online consumers. As a law enforcement agency with direct experience in obtaining access to individuals' personal information in connection with investigations, the FTC could play an important part in ensuring adequate and coherent reform.

**International engagement**

Though getting privacy right in the domestic context is critical, this task cannot take place in a vacuum. It is essential that U.S. policy makers take into account – and meaningfully engage in – the international effort to develop and harmonize data protection policy. This is especially true given the importance of the Internet to the world economy.

The wisdom gained through the roundtables offer useful insight into consumer privacy protection as international privacy organizations and regulators revisit the FIPPs. The Commission, along with the Commerce Department and other U.S. representatives, should make full use of the opportunity to influence the global privacy regulatory debate. We support the Commission's active participation in international discussions with this goal in mind.

Maintaining a regulatory environment that encourages responsible privacy practices while also promoting continued Internet innovation will require the leadership of broad-minded, forward-looking U.S. regulators, including the FTC. The international regulatory patchwork makes it increasingly hard for companies to operate internationally, even while commerce is becoming increasingly global. United States leadership in creating a uniform, flexible, and comprehensive approach to privacy protection that effectively educates users, vests them with meaningful control, and earns their trust could help remove artificial barriers to the free flow of information.

**Free expression and privacy**

Google acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression.

Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors. While we cabin this right in important ways – including individual liability for defamation or harmful speech – it is invaluable to the ability to exercise freedom of expression.

As the Web evolves, free expression can also be affected by mandated opt-in policies for information collection. While appropriate in certain circumstances, broad opt-in requirements can

create perverse incentives for companies to collect more identifying information than necessary and to obtain "consent" in inappropriate or confusing ways. If all online behavior were traced to an authenticated identity, the free expression afforded by anonymous web surfing would be jeopardized.

## Conclusion

Google wishes to thank the FTC for considering these comments as it contemplates its future efforts to protect the privacy of consumer data. We hope that our privacy efforts, as described here, can inform those efforts and help in the Commission in its daunting task. Google will continue working with the FTC to think deeply about the acceptable treatment of user data both across jurisdictions and across the private and public spheres.

Should you wish to contact us regarding our comments, please do not hesitate to contact me by email at pablochavez@google.com or by phone at 202.346.1237.

Sincerely,

Pablo L. Chavez
*Managing Policy Counsel*
*Google Inc.*

# Department of Commerce
# Docket No. 100402174-0238-02 RIN 0660-XA12
# Information Privacy and Innovation in the Internet Economy
# Notice of Inquiry Comments
# 14 June 2010

# I. Introduction

GS1 US is a not-for-profit organization established over 35 years ago to administer and manage Universal Product Codes, also known as U.P.C.'s. Since then, our membership and mission have expanded considerably.

Our method of identifying products and capturing product data has evolved into what is now known as the GS1 System, the world's most widely used supply chain standards, which include:

- a sophisticated array of numbering formats (identification numbers) for **identifying** different objects;
- a variety of bar codes and the Electronic Product Code (EPC), for **capturing** the identifying numbers; and
- data synchronization and electronic information exchange, for **sharing** the data.

GS1 US member companies represent more than 200,000 American businesses in more than 20 industries including consumer packaged goods, apparel, government, aerospace, retail, foodservice, healthcare, fresh and packaged foods, consumer electronics and high-tech. Some of the world's largest corporations participate in our boards and work groups, motivated by the knowledge that GS1 standards help their companies reduce costs and increase both the visibility and security of their supply chains.

GS1 US is one of 108 country-based Member Organizations of GS1. GS1 is a global organization dedicated to the development of standards and solutions to improve the efficiency and visibility of supply and demand chains, both globally and across industries. More than one million companies use GS1 standards to do business across 150 countries. GS1 and its subsidiaries and partnerships connect companies with standards-based solutions that are open, consensus-based, and universally endorsed.


GS1 US is <u>not</u>:

- a software provider
- a hardware provider
- a commercial solutions provider
- a technology company
- a trade organization
- a government agency

GS1 plays a proactive role in standards development by supporting research at leading academic laboratories around the world. Its Electronic Product Code was the result of such research as well as the work of several hundred companies represented in what became the second largest consortium at MIT, trailing only the World Wide Web Consortium.

GS1 knows firsthand the difficulties in developing and introducing new technologies. Few people now remember the swirl of controversy that surrounded the introduction of the now ubiquitous bar code in retail settings. Opponents of the use of bar codes warned of dire consequences for consumers and sought to prevent the use and deployment of bar codes; today it is hard to imagine losing the benefits of bar codes such as faster checkouts and the lower prices enabled by improved supply chain management.

Controversies such as those involving the introduction of bar codes have helped GS1 to understand the importance of broadly inclusive processes in developing appropriate policies. With that in mind, we commend the Department of Commerce, and other government agencies such as the FTC and the FCC for their expansive efforts to involve the public in important policy reviews. We support the view, expressed in the NOI, that recent technological developments, new applications, changing attitudes and expectations of privacy along with the growth of global connectivity make it timely to review existing privacy policies to ensure they meet the needs of the 21st century. GS1 is committed to participating in this process and pleased to provide its views on this important topic.

# II. Key Considerations in Developing Policy

The core mission of GS1 is to create and implement standards and policies that will facilitate the growth of global commerce. We firmly support the global flow of information. But we realize that commerce cannot thrive in an environment where there is no effective fabric of trust and where consumers do not participate because they lack confidence that they will be fairly treated and that their personal information will be appropriately protected.

Therefore we fully subscribe to the goals which the Department has set out for privacy policies: that they will enhance: "[1] the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy; [2] the public confidence necessary for full citizen participation with the Internet; and [3] uphold fundamental democratic values essential to the functioning of a free market and a free society."

Given our global presence and the experience of our members, we would like to highlight several considerations:

- It is becoming increasingly important to develop policies while considering the global context and the need to harmonize policies to the extent possible consistent with fundamental values;

- Information is the lifeblood of commerce. Any restrictions must consider and reflect the benefits that will be foregone as well as the potential harms they are designed to avoid. We do not mean to imply that there are not justifiable restrictions, but the policy goal should be to find an appropriate balance between sometimes conflicting values. In determining that balance, policymakers should recognize the importance of the free flow of information for economic, social and political reasons;

- It is critical for policymakers to take a long view. The success of Privacy Guidelines issued by OECD and APEC is based in part on the focus on lasting principles applicable in a wide variety of circumstances. Lasting policies are based on careful analysis, not anecdote or headline;

- Electronic commerce has the potential to improve the living conditions of people around the world. But progress depends on our capacity to innovate. Without innovation, there is little chance that the next generation will inherit a better world.

Given its global view and its role in supporting innovation and commerce, we are pleased that the Department of Commerce has taken a leading role in this review of privacy policy.

# III. Self Regulation

Too many policy debates pit proponents of new laws and regulations against advocates for self-regulation as if policy makers need to choose one path or another, embracing regulation and legislation or leaving the field open for private parties to make choices unencumbered by governmental action. This is not the real choice faced by policymakers. The real issue is determining the appropriate mix of these policy tools, which requires analysis, rather than sloganeering. Policymakers have recognized that mixed systems of laws and regulation combined with self-regulation can provide more efficient and effective means of achieving policy goals. This has been true in the realm of privacy policy in the U.S. for many years as well as in other areas where there are important competing interests that need to be appropriately weighed.

In determining the appropriate mix of policy tools, we do believe there are important needs served by clear and well-crafted laws and regulations. They can and should reflect lasting and publicly supported principles and provide clarity in the "rules of the road". They should establish boundaries while maximizing the ability of private parties to innovate and to make decisions based on their unique circumstances.

But we also believe strongly in the potential for self-regulation within the boundaries set by law. As laws and regulations become more and more detailed they become harder and harder to know, to understand, to obey, and to enforce. They inevitably leave gaps—inevitably because the world is constantly changing. But to the extent that laws set clear boundaries and reflect established principles, they can be complemented by effective self-regulation. Self-regulation has some clear advantages over ever more detailed legal dictates:

- Because "one-size fits all" policies often fail to meet their objectives because of the wide variation among those subject to the policies, it would be in the interest of policymakers to be able to "customize" policies. But laws and regulations are not designed for customization. Those subject to rules are the most knowledgeable parties about their internal plans and procedures and can structure them appropriately to accomplish policy goals;

- Those subject to the rules have the strongest incentives to find the most efficient and effective means of accomplishing policy goals;

- Self-regulation encourages innovation by the entities subject to it rather than simply turning over decisions to governmental entities. As the open standards movement demonstrates, there are substantial advantages in defining standards while encouraging innovation on top of those standards. Similarly, the open source movement demonstrates the value of recognizing the contributions that come from the widest possible range of sources;

- By encouraging those subject to policies to take responsibility through self-regulation, policymakers can focus on setting boundaries, overseeing behaviors, and enforcing those laws and regulations which set boundaries and which are not as amenable to self-regulatory regimes.

Self-regulation is consistent with the basic principles of devolution, attempting to drive decisions down to the lowest possible level because of the value of localized expertise and the strong incentives for effectiveness and efficiency that can be found at the local level. We would encourage the Department to recognize the utility of self-regulation and to incorporate it as a vital part of the privacy framework.

# IV. A Recent and Ongoing Study in Government – Industry Cooperation for Principles-based Self Regulation

Over the last several years, GS1 has been working with the European Commission on a largely self-regulatory project to create a Framework for privacy impact assessments (PIAs) to help enterprises evaluate new radio frequency identification (RFID) applications. The Framework initiative has occurred under the umbrella of the European Union's *Directive on Data Protection* and the *European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio frequency identification.* While the process of developing and implementing the PIA Framework is not yet complete, it has provided a number of useful lessons about the importance of government – industry cooperation, the role of self-regulation within a larger legal context, and the benefits of a principle-based approach:

`

Government – industry cooperation

- The process benefited from a willingness of various industry sectors to work together to create a PIA Framework of general applicability and one that could be customized to meet the needs of a particular industry sector. The consultative process that was established to create the PIA Framework was a broadly inclusive one involving non-governmental entities, academics etc., all of whom provided valuable feedback;

- The process for developing the PIA Framework also involved feedback from the data protection officials from the various countries of the European Union operating through the Article 29 Committee.

Principles-based approach

- The PIA Framework establishes guidelines for PIAs that address the full range of privacy principles, including notice, choice, responsible uses, data sharing, accountability, and others;

- The process encourages building in privacy protections in applications (privacy by design) rather than having privacy measures bolted on to applications after their implementation.

Self regulation

- The draft PIA process establishes appropriate internal review and approval procedures and processes for new RFID applications, involving not only operational personnel responsible for initiating the proposed application but also other appropriate management personnel;

- The process incents enterprises to become more self aware and conscious of privacy issues that might arise and to make more educated determinations on how they might be addressed.

The process has also confirmed a potential tension that is recognized in the NOI when multiple jurisdictions have different policies for the same activity. It is possible that a company proposing a new RFID application might have to submit its PIA for that application to dozens of different authorities throughout Europe for review. This could create unnecessarily duplicative work for the

entity submitting the PIAs as well as for the data protection authorities. Such burdens are disproportionately felt by small and medium-size enterprises (SMEs).

But even more potentially damaging would be conflicting rulings from various national authorities based on differences in national law making it difficult if not impossible for the petitioning company to operate centralized applications and to act, as is increasingly required, on a global basis.

# V. Inconsistent or Conflicting Privacy Frameworks Create Barriers to Innovation and Deployment of New Technologies

In Section 2 of the Notice, the Department addressed the issue of the impact of diversity in state privacy policies. GS1 US has considerable experience in this area and is convinced that any potential gain in privacy protection in any single state jurisdiction is outweighed by the negative impacts of increased compliance costs, barriers to technology development and deployment, and increased customer confusion, particularly when state laws are technology specific.

GS1 Member Organizations work with members from over a hundred countries with vastly different legal and regulatory regimes. Yet an increasing number of our members offer goods and services globally and require the development of standards and systems that will work both locally and globally. These standards and systems are often subject to review and approval at many levels of government— for example local, state and national in the U.S., sub-national and national in Europe and Asia, and European-wide in Europe.

Inconsistent or conflicting privacy frameworks raise the cost of compliance which ultimately affects prices to consumers. But in some cases, inconsistent or conflicting rulings can actually make the development and deployment of new technology impossible. This can happen, for instance, if a local jurisdiction passes legislation that restricts or prohibits the use of a technology, or places inordinate burdens on it that cannot economically be met.

We strongly favor privacy policies that are technology neutral. New technologies entering the market already must overcome many obstacles, including the incumbent technologies they seek to replace. Handicapping new technologies with policies that burden them and are not applied to existing technologies may prove too much of a barrier to overcome, and, in any case discourage investment and deployment. Furthermore, technology specific policies may become obsolete overnight as new technologies arise.

Legislation recently considered in one state in the U.S. would have created a legal requirement that notices be provided to consumers about the use of RFID technology. We believe that notice is, and should remain a critical element of privacy frameworks and have included a notice requirement in the EPCglobal guidelines for RFID implementation.

But the proposed legislative notice was very specific. It would have established in law a requirement that the notice include a reference to a finding by that particular state government. It would have been economically infeasible to display such a notice but, more importantly, the notice invited every other jurisdiction to establish their own notice requirements or defer to the first state that acted, substituting speed to regulate for careful legislative review and action. Of course, it would be theoretically possible to manufacture different versions for each state but it would be akin to requiring a different cereal box for each state.

The uncertainty about varying legal and regulatory requirements has discouraged potential users of RFID technology. Investment has been delayed, deployment postponed, and research deferred.

Continuing uncertainty has had a chilling effect even given the demonstrable benefits of using the technology to improve efficiency, reduce costs, etc.

We offer this example not with a view that privacy issues are irrelevant or should not be addressed, but to emphasize the impact on innovation. One positive effect of the NOI would be a heightened focus on the need to harmonize or make interoperable differing policy frameworks regarding privacy.

# VI. Information and Communications Technologies Operate Globally and Policies Must Be Harmonized to Reflect the Increasing Globalization of Both Commerce and Innovation

There are a number of useful precedents that demonstrate the means for and the beneficial results of policy harmonization. As an example, OECD accomplished foundational work in privacy through the development of its 1980 Privacy Guidelines. The Department's role in the development of the OECD guidelines and the 2005 Asia Pacific Economic Cooperation Privacy Framework provides a valuable legacy for the Department's present work in privacy.

The fact that the OECD's 1980's work—which predated the commercial internet, the explosive growth of e-commerce, and the emergence of broadband and mobile connectivity-- remains a foundation for today's privacy discussions is a testament not only to the thoughtfulness of the participants, but also to their focus on guiding principles and inclusive policy making processes.

The membership of the OECD and APEC consists of governments. Yet their privacy policymaking process brought together a wide variety of stakeholders including consumers, privacy advocates, academics, businesses in a mutually respectful environment where all interests could be examined. At the same time, the efforts did not seek detailed and prescriptive rules but guidelines that could be implemented in many different circumstances in countries with vastly differing legal systems and institutions. They recognized the importance of allowing policies and practices to emerge which could be evaluated in light of the guidelines and which could be reviewed and adapted as technologies and uses change over time. The guidelines were technologically neutral but the principles remained applicable whether the information was contained on paper records or in the sometimes evanescent digital "breadcrumbs" that may follow one's path on the World Wide Web.

In 2003, the GS1 EPCglobal entity created *Guidelines on EPC for Consumer Products* for the use of EPC-enabled RFID technology. EPCglobal brought together a large and disparate community involving a membership that comes from 108 different countries. Drawing upon Fair Information Practices, EPCglobal instituted a self-regulatory system to create an environment of trust for consumers and businesses. Based upon the collective experience of its membership it customized the privacy protections included in the Fair Information Practices to the particulars of the technology and its applications and established processes to review the *Guidelines* if significant changes in circumstances occur.

We believe that the Fair Information Practices have served us well. Notice (clear, accessible, comprehensible, and meaningful) and choice (effective, and easily implemented) will continue to be critical components of any long lasting privacy regime in part because notice and choice reflect the existence of rights and responsibilities for all parties to a potentially privacy affecting transaction. But the dramatic changes in our world reinforces the need for policymakers to step back, reconsider, and if necessary, amend present policies to better meet the challenges of the 21st century.

The NOI raises the possibility of a "use-based" model for privacy protection. At its core, we see the use-based model as reflecting an important insight—the parties most familiar with their plans and procedures should be incented to create and implement the most efficient and effective means of achieving well defined policy goals such as the protection of privacy. Defining the high level principles and setting any critical boundaries through rules of the road are by and large governmental functions, but decisions about their implementations in day to day processes and procedures should devolve to those closest to the specific facts with the strongest incentives to do things right.

# VII. Connecting the Dots: Government's Expanding Data Collection

In Section 3, the Notice asked for comments on the impact of laws that permit governments to have access to personal information. While this question was posed in the context of international privacy laws and regulations, we believe that the issue applies to actions by governmental entities in the U.S. as well and is particularly timely.

One of the responses to the fears of global terrorism has been to dramatically increase the collection, sharing, and processing of information that might allow the government to anticipate and prevent terrorist acts. In today's dangerous world, intelligence and law enforcement officials are justifiably concerned with "connecting the dots". As is true with other privacy issues, this important effort to protect the national security raises potential conflicts with the protection of individual privacy. One fruitful area of investigation in constructing a privacy framework for the 21st century is the development of appropriate rules and procedures for government access to the vast amounts of data now being generated and collected in the private sector. Businesses everywhere would benefit from clear rules on what constitutes due process for government access to data in the face of challenges both domestic and foreign.

# VIII. Privacy Enhancing Technologies and Aggregated Data

In Section 6, the NOI justifiably calls attention to the importance of privacy enhancing technologies and information management processes in the development of a 21st century privacy framework.

GS1 believes in the importance of developing these technologies and has been supporting related research at academic laboratories around the world.

We do believe, however, that government has an important role to play, particularly with respect to data de-identification and data re-identification.

Many of the great policy challenges facing our nation will depend on exploiting huge amounts of aggregated data. Just one example is comparative effectiveness research in healthcare. The ability to mine data from millions of de-identified/anonymized medical records to determine what medical treatments work and what treatments do not work is critical to increasing the effectiveness of medical interventions as well as controlling healthcare costs. Yet aggregating and mining such data, based upon sensitive medical records, poses real privacy risks, risks highlighted by recent research that shows the potential for re-identification of supposedly anonymized data.

In the past government has supported the creation of standards for the protection of information such as the digital encryption standard. This standard, the result of collaboration among the government's most sophisticated technical agencies, was adopted to protect governmental

information but was available for use by the U.S. private sector. Because creating an effective means of de-identifying large data sets presents substantial technical challenges and because the government would be a principle beneficiary of any successful de-identification effort, there is a strong argument for governmental support.

Creating a successful system for de-identification—long lasting, impervious to known challenges, easily and cost effectively implemented in a variety of settings without access to specialized expertise-- might be likened to the Grand Challenges that have helped spur technological development in areas such as the development of autonomous vehicles. Given the extraordinary benefits that appear to be achievable using aggregated data, de-identification deserves the Grand Challenge label and the associated governmental support.

One other comment should be made in connection to privacy enhancing technologies. It is well understood that corporations have an economic incentive to utilize data they generate to increase sales and profits. Corporations have economic incentives to protect privacy in order to develop strong bonds with their customers, providing more attractive goods and services, and to protect their brand equities, but these incentives could be strengthened. A new policy framework should examine the potential to increase the economic incentives for adoption of privacy enhancing technologies and further strengthening of privacy protections. There may be analogies in the example of using procurement policies to encourage smart building design or more sustainable computing devices that suggest new ways of using economic incentives to promote innovation in privacy protection by the private sector.

# IX. Small and Medium-Sized Entities and Startup Companies

In Section 7, the Notice asks for comments on the impact of privacy laws on SME's.

As we noted over 200,000 companies, most of them SME's, participate in GS1 US. While they differ in many respects, they all depend on the confidence of their customers and have strong incentives to treat them in a way that they continue to be their customers. This clearly includes obeying laws and regulations regarding privacy.

A crucial difference between SMEs and larger commercial entities is their relative lack of resources for compliance with legal and regulatory requirements. In drafting the proposed PIA described in Section 5 above, we attempted to reduce, as much as possible the burden placed on the entity that is proposing a new RFID application. We would recommend as strongly as possible that evaluating the actual burden of compliance be a critical part of any privacy framework.

# X. The Importance of Consumer Education

The role of government and the private sector in educating the public about privacy has received little attention. Yet in other areas of societal concern, preventing identity theft or reducing teen smoking, for example, public education has played a meaningful role. There do not appear to be similar efforts to help the public understand the increasing challenges they face regarding the protection of their personal privacy, the choices they have available, or ways they can make more informed decisions. Identifying the locus of such a public education effort and providing opportunities for the private sector to assist might have outsized benefits for its minimal costs.

# XI. The Role of the Department of Commerce

We have the greatest respect for the efforts of the Federal Trade Commission, in particular, to protect consumer privacy. As can be seen in this Notice, however, the Department of Commerce brings an important and different perspective to discussions of privacy policy and innovation in a global context. We commend the Department's initiative and support its continued participation in the development of a privacy framework for the 21st century. We are pleased to be able to provide our comments in this important effort and stand ready to continue to support this process in whatever ways possible.

For more information, please contact:

Elizabeth Board
Executive Director, GS1 Global Public Policy
1101 30th St., NW Suite 500
Washington, DC 20007
elizabeth.board@gs1.org

www.DiscoverRFID.org
www.GS1US.org
www.GS1.org
www.EPCglobal.org
www.EPCglobalUS.org

Hewlett-Packard Company
3000 Hanover Street
Mail Stop 1050
Palo Alto, CA 94304-1112
www.hp.com

May 11, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear NTIA,

Larry Irving
VP, Global Government Affairs
Tel. +1 202 637 6751
larry.irving@hp.com

Scott Taylor
Chief Privacy Officer
Tel. +1 650 857 7469
staylor@hp.com

Hewlett-Packard Company (HP) appreciates the opportunity to provide feedback as part of the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy."

HP is headquartered in Palo Alto, California, and is a global provider of computing and imaging solutions and services, conducting business in over 170 countries around the world with more than 300,000 employees globally and 2009 revenues of $114.6 billion.

Respecting our customers' privacy has been in our DNA since the inception of the company and an integral part of our success. We firmly believe that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust.

Only by ensuring the privacy and security of all the customer information that we handle can we rightfully gain and maintain that trust. From becoming one of the earliest U.S. companies to participate in the U.S.-EU Safe Harbor program in 2001, to working collaboratively with industry, regulators and consumer advocacy groups, HP is committed to advancing forward-looking, workable privacy initiatives that respond to consumer needs and advance innovation.

We will provide brief comment and thoughts on all eight of the areas raised in the Notice of Inquiry.

## 1. The U.S. Privacy Framework Going Forward

*(whether the existing U.S. policy framework provides sufficient guidance to the private sector to enable organizations to satisfy applicable U.S. laws and regulations; whether there are particular modifications to U.S. privacy laws that would better support innovation)*

HP has been very public in calling for omnibus U.S. federal privacy legislation. We firmly believe that it is time for the U.S. to establish a comprehensive, flexible, and harmonized

legal framework for protecting consumer privacy. Recent research shows trends that consumers want it, we believe companies need it, and the economy will be better for it.

HP is a strong proponent of effective corporate self-regulation. We believe that the future of e-commerce depends on companies acting in an accountable and responsible manner to advance consumer needs. At the same time, however, we recognize that consumer privacy presents a series of challenges that have not yet been fully addressed. For example, the patchwork of state-based privacy regulations in existence today confuses consumers as to the extent of their protections in any given context, and forces companies to contend with a mix of differing and often conflicting regulations.

Further, heightened consumer concerns about existing privacy threats – from spyware to phishing, spam to data breach, and any number of other challenges – risk undermining the economic health of e-commerce and innovation. No one is served – not consumers, not governments, and certainly not corporations – by a lack of customer confidence in the security and privacy of personal information in existing products and new innovations.

HP believes that the U.S. should take steps to consider a comprehensive federal approach to protecting consumer privacy – one that provides a workable *national* standard in lieu of the current patchwork of state laws. This national baseline should be built on fundamental, sound privacy principles that include:

- transparency and consumer choice;
- use and obligations;
- scalability and flexibility;
- information security;
- accountability; and
- strong enforcement.

We are not looking for the government to dictate the terms *or technologies* for protecting privacy. Rather, we would continue to urge policy makers to examine ways of establishing a workable benchmark that unifies the divergent regulations currently in existence, responds to the very real needs of anxious consumers, and, at the same time, is flexible enough to accommodate future technological innovations.

**2. U.S. State Privacy Laws**

*(how different state-level laws and regulations affect companies' compliance costs, product development processes, business activities, and the ability to work online; what approaches do companies take to comply with the myriad laws)*

Many of the state laws and statutes (e.g., data breach notification laws) have created solid foundations for improved organizational behavior and consumer protections. But as the number of state laws and statutes grow, so does the complexity in business compliance processes and costs. We believe that many of the best practices that exist in state laws should form the basis of federal legislation to ensure a predictable and uniform standard across the U.S.

**3. International Privacy Laws and Regulations**

*(how international data privacy laws and regulations affect global Internet commerce, companies' compliance costs and product development processes, and Internet users; what hurdles do businesses face in complying with different foreign laws concerning privacy and data protection; what lessons have companies learned from the U.S.-EU Safe Harbor Framework that could be applied in the global context)*

As a large multinational corporation, we have to think and operate globally. We have found the best approach to privacy is a consistent standard that is based on solid external criteria, such as the EU Directive, OECD principles and Fair Information Practices. It would create greater compliance risk and increase operational costs for us to manage privacy differently for each country/region. This is one of the reasons HP was among the first companies to self-certify in 2001 to the U.S.-EU Safe Harbor Program. The work that the Department of Commerce achieved with the European Union to establish this program was critical to our company. It not only provided a bridge, but it enabled us to set a higher, global standard within our company for privacy.

In an Internet age, data flows are global and it becomes critical to innovation that we are able to reconcile emerging privacy frameworks or regimes. This is why HP is encouraged by new, emerging privacy frameworks, including Binding Corporate Rules in Europe and Cross Border Privacy Rules in APEC. We commend the strategic leadership of the Department of Commerce in establishing APEC Cross Border Privacy Rules, and encouraging a dialog between the APEC Privacy Sub-group and the Article 29 Working Party. Most recently, the Department's support of the Galway Project on Organizational Accountability, led by the Centre for Information Policy Leadership, and your encouragement of the Use and Obligations Model, developed by the Business Forum for Consumer Privacy, are examples of the influence and leadership you can provide in aligning the global and domestic agenda.

If we are able to keep these new frameworks and concepts aligned, at least in basic approach, it will enable organizations to uphold and demonstrate capacity against clear, outcomes-based expectations and manage higher levels of compliance and accountability.

**4. Jurisdictional Conflicts and Competing Legal Obligations**

*(whether companies face any jurisdictional conflicts as a result of complying with privacy laws, how they reconcile such conflicts, and, what, if any, effect they have on trade and foreign investment)*

As stated previously, HP has created global policies and implementation standards that align to the EU Directive, Safe Harbor, and most other recognized principles. Although this makes our policy more stringent than many country laws, it aligns to our core values and a uniform approach is easier to administer. As new laws and frameworks are established worldwide, anything that can be done to align and minimize jurisdictional conflicts will benefit companies in managing compliance and creating a predictable environment that encourages innovation.

**5. Sectoral Privacy Laws and Federal Guidelines**

*(given the U.S.'s sectoral approach to privacy regulation, how does the sectoral approach affect consumer experiences, businesses practices, or the development of new business models; are there alternatives or supplements to the sectoral approach)*

The major sectoral programs, HIPAA and GLBA, have provided consumer protections for privacy and data protection, but they clearly do not extend across all industries. As mentioned above, we support omnibus federal privacy legislation in the U.S. As this legislation is developed, it needs to take into account, co-exist with, and complement those sectoral laws.

**6. New Privacy-Enhancing Technologies and Information Management Processes**

*(what is the state of development of technologies and business and business methods aimed at improving companies' ability to monitor and audit their privacy compliance)*

The new applications, business models and technologies that have emerged with the Internet provide tremendous benefits to consumers and are critical to economic growth and prosperity. Yet, these same innovations create new issues for privacy and cybersecurity. Recent research and events have shown that a number of unanticipated privacy and data security issues have begun to erode consumer confidence and trust. This creates a compelling challenge as organizations work to balance innovation and the protection of data and individual rights. Just promising to try harder is not going to be good enough. We have to get smarter and ensure that we can provide meaningful protection.

Current laws and regulations struggle to keep pace with new forms of data collection, use and storage. As consumers, advocates and regulators become more aware and more concerned about these issues, organizations will need to do more to consider the privacy risks created through innovation.

New organizational accountability frameworks are emerging that set expectations for companies to design privacy enablers and risk mitigation into every stage of product development. It is often referred to as "Privacy by Design."

HP's Privacy team has partnered with our R&D Labs to develop and deploy a Privacy by Design program to ensure that our more than 300,000 employees understand privacy implications as they conceive and develop products and programs that will collect or use personal data. The program is not just about compliance. It integrates ethics- and values-based considerations to ensure we align to company codes of conduct and consumer expectations. Most product designers – or marketing managers – are thinking about the next innovation – not about what we at HP have termed "PUF" – potentially unwanted functionality. But employees – whether they are designing a new product or launching an email marketing campaign – need to understand how to put policies, obligations, and values into effect, and to do so prior to design or deployment.

Not all innovative ideas become reality, so we need to break-down product or program development into simple stages. In the design and development stages, privacy organizations should provide proactive guidance so privacy considerations can inform early planning. This has traditionally been difficult for companies and can result in a

program being delayed or cancelled later based on privacy concerns. Early guidance related to privacy becomes a tremendous asset to an organization because it ensures privacy pitfalls can be avoided. In the deployment, maintenance, and end-of-life stages, a privacy team needs to do more than just guide. They must provide assessment mechanisms to ensure compliance with local laws, and company obligations, policies, and values. We have learned that this assessment needs to be as contextual as possible. For example, the way we need to assess privacy compliance in a global email marketing campaign is very different than assessing privacy compliance in a new PC or web-enabled printer.

To help manage this, HP has deployed an interactive, online tool that is available to every employee from our intranet. The tool, which we call "The HP Privacy Advisor," starts by asking the user a series of simple questions. As the employee answers each question, additional dynamically generated questions are posed based on the collective intelligence and risk factors that result from how prior questions were answered. Essentially, it is an intelligent privacy impact assessment that is relevant to the employee using it and scales to cover simple and complex programs. One of the greatest benefits is educating employees about privacy requirements in the context of their specific programs. Through the process, employees learn about privacy issues and can modify their approaches to ensure compliance. The assessment results are documented and reviewed by the Privacy team. Consultation is provided as necessary, and if any issues exist, approval is required prior to deployment. After a product or program launch, additional workflow is triggered to ensure deployment is consistent with expectations and that end-of-life actions are taken when appropriate.

The HP Privacy Advisor serves as the front-end process to our Integrated Assurance Management Program, which includes annual risk identification processes, ongoing monitoring, audit, and formal remediation and tracking.

By using technology, we are better positioned to guide our employees to think about privacy in the right context and at the right time. We are also able to see trends, issues and opportunities in a real-time manner. This minimizes unanticipated effects and balances our ability to innovate and ensure responsible practices when using data.

### 7. Small and Medium-Sized Entities and Startup Companies

*(how do existing privacy laws affect small and medium-sized entities and startup companies)*

The harms that can arise from a lack of appropriate privacy or security protocols transcend business of all types and sizes. If a business, for example, handles highly sensitive personal data, the impact of poor privacy or security controls will be the same to the impacted individuals regardless of whether it is a small or large company that mishandled the personal data and caused the issue. Scalability of legislation is critical, but we need to ensure that the scalability relates to "how" an organization achieves a result, not "what" needs to be achieved. The same basic rules and principles ("what") should apply to all organizations, but "how" a small company implements may be very different than a large company. If we separate the "what" from the "how," we will ensure consistent expectations and leave organizations with the flexibility for achieving that expectation.

**8. The Role for Government/Commerce Department**

*(how should the DOC Task Force help address barriers to increased innovation and consumer trust in the information economy)*

The Department of Commerce has for many years played a critical leadership role domestically and internationally for privacy. We need only look to the U.S.-EU Safe Harbor program, the leadership in the 1990s on the future of privacy, the APEC Pathfinder Project, and the recent efforts to advance the cause of privacy and innovation. HP believes that the Department of Commerce should continue to provide leadership within the domestic agenda and with our major trading partners internationally. The Department is best positioned to advocate policy that will create meaningful consumer protections and at the same time allow for innovation and economic growth. HP stands ready to continue supporting your efforts.

If you have any questions or if you would like to discuss this matter further. Please don't hesitate to contact us.

Best regards,

Scott Taylor
Chief Privacy Officer
Hewlett Packard Company

Larry Irving
VP, Global Government Affairs
Hewlett Packard Company

International Business Machines Corporation
1301 K Street, NW, West Tower, Suite 1200
Washington, DC 20005

June 14, 2010

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01
*Submitted online to: privacy-noi-2010@ntia.doc.gov*

Dear Sirs and Madams:

IBM is pleased to respond to the Commerce Department's Notice of Inquiry on Information Privacy and Innovation in the Internet Economy. We commend the Department for seeking a wide range of views on this rapidly-evolving and important set of issues.

We welcome discussion -- and could provide input on -- many of the topics included in the Notice. However, for brevity and focus these comments directly address a few key topics: the importance of privacy issues to contemporary economic growth and progress; the value of strong international engagement by the Department of Commerce on these issues; and the importance and increasing sophistication of privacy by design and practice, and how government can appropriately support it. We have also indicated support for the separate response filed by the Centre for Information Policy Leadership.

Our comments and perspective are necessarily informed by IBM's own experience in business, technology and privacy, so we begin with a description of the company's longstanding engagement in this area.

**IBM's Engagement in Privacy is Comprehensive and Longstanding**

IBM helps organizations become more innovative, efficient and competitive through the use of business insight and advanced information technology solutions. Our capabilities include business process and IT services, cloud computing solutions, software, hardware, fundamental research and financing.

Approximately 400,000 IBMers work across the globe, engaging with and helping many thousands of clients, communities, universities and other important constituencies to integrate information technology into virtually all of the globe's key systems -- such as public health, transportation, energy, food supply chains and beyond. We operate as a globally integrated enterprise, which -- key to the subject of the Department's inquiry -- involves the processing of information across national borders in support of research, technology development and deployment, sales, HR and other key functions.

We thus submit these comments from the perspective of a technology and business innovator; a professional services company; a large employer; and a company that depends on the ability to access and use data in markets around the globe.

IBM's response also draws upon our company's longstanding commitment to, and engagement in, information privacy policy and compliance:

- Forty years ago, in the earliest years of computing, IBM worked with Professor Alan Westin of Columbia University to formulate and adopt one of the first, if not the first, organizational privacy policies, governing the entirety of our operations and adjusting over time to support our compliance with the myriad of privacy laws and expectations that exist across the globe.

- In the 1990s, as the Internet emerged as a transformative and widely-accessible platform for computing and innovation, IBM promoted information practices to support transparency and accountability on the Web, becoming one of the first companies to publicly post its privacy practices on its Web site and helping to launch industry trust initiatives such as TRUSTe and BBBOnline.

- In 2000, IBM became one of the first major companies to appoint a senior-level chief privacy officer, and IBMers helped to launch the now 7,000-member International Association of Privacy Professionals. That same year we offered our strong support to the Commerce Department's effort to negotiate the EU-US Privacy Safe Harbor and we became one of the first companies to enroll in the program.

IBM has also supported and informed passage of key privacy laws and guidelines in the United States and elsewhere when, in our belief, direct government regulation was needed to help protect individuals from harm and to help keep organizations accountable for how they handle personal information. For example,

- In the 1980s we supported enactment of the Electronic Communications Privacy Act.

- In the 1990s we supported enactment of the health privacy law HIPAA.

- In 2005 IBM was one of the only corporations who supported enactment of the Genetic Information and Nondiscrimination Act.

- And we were supportive of the 2005 enactment of Privacy Principles by APEC, the Asia-Pacific Economic Cooperation Forum.

IBM's corporate citizenship in privacy and data protection has resulted in external recognition including:

- For the past three years, US consumers have named IBM the IT company Most Trusted for Privacy in the TRUSTe/Ponemon annual survey (in 2010 IBM was #3 overall, and was the only business-to-business brand in the top 10).

- IBM won the 2009 Privacy Innovation Award from the International Association of Privacy Professionals, for innovation in privacy-enabling technology, and in 2007 its chief privacy officer was recognized with the IAPP's Vanguard Award.

**Progress and Economic Growth Depend on Meeting Privacy Expectations**

Today, IBM continues to collaborate with forward-looking governments and private-sector organizations on privacy and data protection policy and practices.

For example, we participate in and support APEC's work to develop a program for accountable global data flows; we support the Galway Accountability Project and as well the aspiration by an influential international group of data protection authorities to enunciate global privacy principles via the Madrid Declaration; and we have shared our experience and views in recent workshops and discussions sponsored by the Commerce Department and the US Federal Trade Commission. Our experts are engaged in leadership and advisory roles in a wide range of private-sector initiatives including informing the work of the Centre for Information Policy Leadership, Center for Democracy and Technology, Center for Strategic and International Studies and Markle Foundation.

Within IBM, we have implemented a comprehensive accountability program to govern the company's collection, use and sharing of personal information. This program comprises all of the elements recommended by the Galway Accountability paper and other leading experts:

- High-level organizational accountability and comprehensive enterprise policies that reflect contemporary values and environment.

- Mechanisms to put such policies into effect, including employee education and a global program (supported by a "smart" online tool) that enables all process and IT application owners to do a privacy risk self-assessment, and that provides the corporate privacy office visibility to process-level actions.

- Regular performance reviews performed by business controls and audit teams.

- Transparency provided by 24/7 visible posting of employee and public-facing privacy policy statements, and a globally-consistent access process for employees and other individuals.

- Redress available to individuals via their inquiry directly to IBM via a dedicated privacy address or IBM's longstanding employee hotline, as well as via TRUSTe.

We are engaged in this fashion -- in external collaborations and comprehensive internal governance -- because IBM recognizes the importance to business of addressing privacy expectations.

As described by the Department's Notice of Inquiry, the development and deployment of information technology have enabled people and organizations to realize a wide range of benefits. As important elements of our infrastructure have become (and are becoming) more instrumented, interconnected, and intelligent, so too has our society realized measurable economic benefit.[1] The emergence of cloud computing as a more flexible and efficient model for delivering computing is a significant development.

With nearly 2 billion people on the Internet (and counting), and with more and more of the world's systems becoming digitally aware, there is greater diversity of the forms and shapes data is taking – transactions of every kind, rich media, social media.[2] Already, 30 percent of the data in the world consists of medical images.[3] With more planet-wide sensors than ever – a billion transistors for every human – ever more data is being generated and at far greater speeds.[4]

Data, coupled with analytics, can do very positive things for individuals and for society. Childhood cancer is a relevant case study: fatality rates have declined more than 50% in just a generation, in part due to high participation in clinical trials (67% of children, vs. 5% of adults) and accompanying data analytics that accelerated development of effective

[1] Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

[2] September 30, 2009, http://www.internetworldstats.com/stats.htm

[3] January 12, 2010, http://www.ibm.com/smarterplanet/us/en/events/sustainable_development/12jan2010/index.html?ca=v_sustainabledevelopment

[4] ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/oiw03021usen/OIW03021USEN.PDF

treatment.[5] Childhood cancer 5-year survival rates are now approximately 80%, versus the near-death sentence such cancers posed 30 years ago.[6]

Experts at IBM[7] believe that other significant progress in the next several decades – in business, science and society at large – will come from insights gleaned through real-time analysis of data (or, "smarter data"). We are just beginning to realize these possibilities.

- Through smarter data, we can make sense of information in all its forms – structured and unstructured, text and multi-media, personal and non-personal data, from physical infrastructures to social networks. For instance, a European railway has been able to weigh 56,000 variables – including the railroad's rolling stock, changing weather patterns and passenger demand – to assemble and schedule more than 5,000 passenger trains per day, improving operating efficiency by 6% with an estimated annual savings of 20 million euros.

- Through smarter data, we can also see how one piece of information relates to the things around it. Any data point, by itself, is just about useless. But when one analyzes it in context and in real time, one can make better predictions -- like a Spanish oil and gas company that is using predictive analytics to parse large volumes of seismic data, boosting the success rate of its exploratory efforts.

- Smarter data delivered in real time via new computational models like stream computing lets us keep pace with a world where risk and opportunity are constantly in flux. Rather than relying on snapshots of the past, our decisions can be real-time, fact-based projections of a likely future. This is what a Canadian hospital treating high-risk newborns is doing, as its doctors use patterns within an array of physiological data to detect life-threatening infections up to 24 hours sooner.

Technology advances historically have enabled industry and government leaders to unlock value in new business models and applied innovations. As they do so, security and privacy tend to follow as issues to be addressed: How to secure newly-valuable information or other assets or operations; who gets to see which information and under what conditions. How our society answers these questions, juxtaposed against robust and accountable data uses, will in significant ways influence future economic growth.

[5]Simone & Lyons, Superior Cancer Survival in Children versus Adults, Huntsman Cancer Institute http://www.iom.edu/~/media/Files/Activity%20Files/Disease/NCPF/Manuscript.ashx

[6] National Cancer Institute Fact Sheet, http://www.cancer.gov/cancertopics/factsheet/Sites-Types/childhood

[7] References available from IBM, http://www.ibm.com/smarterplanet/us/en/business_analytics/ideas/index.html?re=spf

**International Privacy Engagement by the United States Is Key**

In a globally-connected Internet economy, cross-border data flows and access will become a necessary enabler of economic growth and productivity. Current statutory regimes in Europe and several other countries were conceived in the early days of computing and today impose significant procedural hurdles to such cross-border data flows. For some smaller organizations they may pose a more significant impediment.

It is to be expected that governments, cultures and organizations will vary in their approach to information privacy. But since information flows enabled by the Internet and other networks are now instant and global, some types of cross-border data flows that are supported by inter-governmental cooperation -- similar to the EU-US Safe Harbor model, potentially -- are needed in order to promote organizational transparency and accountability while enabling efficient operations.[8] In other words, data should be free to move across borders and organizations, so long as there are accountable processes in place to promote compliance with the policies that apply to such data at the point at which it was collected or created.

It is therefore important for leading government institutions to be part of multi-party global discussions on data protection and international data flows, with a focus on enforcement coordination. The Department of Commerce has had a longstanding role in such discussions, and should continue and strengthen its involvement.

Particularly important is the APEC cross-border data flow initiative that is currently underway and in which IBM is pleased to participate in the pilot program involving several companies. The Department is in an ideal position to press for completion and launch in 2011, when the United States is the host country of APEC, of a "globally certified" program for organizations that have met certain criteria. Such a program, much like the EU-US Safe Harbor, would allow for companies to access data across borders, so long as they remain accountable for such data.

A broader set of sustained international dialogues on information privacy and data flows is also important, as these issues will require continued exploration and updating of norms, laws and practices in light of rapid change occurring in business and technology. These dialogues optimally will involve multiple representatives of government (privacy regulators, economic ministries, law enforcement and national security), industry and

[8] As stated by the Chairman and CEO of IBM,

> A company's standards of governance, transparency, privacy, security and quality need to be maintained even when its products and operations are handled by a dozen organizations in as many countries. A reliance on hierarchies contained within one function, enterprise or nation must be supplemented by new ways of establishing trust, based on shared values that cross borders and formal organizations.
>
> - Samuel J. Palmisano, "The Globally Integrated Enterprise," *Foreign Affairs*, May 2006.

civil society. The Department of Commerce, along with other agencies of the United States government, should actively participate in these dialogues.

**Promoting Privacy by Design Should be a Goal**

Privacy by Design (PbD) is an important concept that can be part of a comprehensive approach to supporting privacy in an environment of technological change and information-intensive innovation. IBM believes that PbD is accomplished at several levels (technology, process and products/services):

- Core technologies can protect privacy if they are developed and deployed (e.g. homomorphic encryption, which allows for manipulation of securely encrypted personal information without viewing of the actual data, thereby allowing for value to be derived from data in a privacy-friendly way).

- Key technologies can be designed to enable privacy (e.g. privacy-sensitive identity management).

- Organizational processes can be designed and implemented in such a way as to handle information, with discipline and accountability, in ways that comply with the privacy policies that apply to that information. For example, IBM has a global privacy assessment process and supporting tools, supported by oversight and consultation from the corporate privacy office and by independent review/auditing by internal and external audit and controls teams.

- Products and consumer-facing services can be configured to be privacy-enabling/friendly, albeit with some limitations given the limitations of notice/consent.

Governments can support and encourage Privacy by Design by:

- Supporting research into the development of Privacy by Design core and key technologies, such as the previously mentioned homomorphic encryption, as a means of promoting and supporting innovation in this area.

- Leading by example, by deploying (and procuring) privacy-enabling processes and technologies to the degree possible, consistent with mission.

- Following the principle of technology neutrality and openness in establishing policies that support Privacy by Design.

**Conclusion**

While the emergence of an information-and-intelligence-infused global commons -- what IBM calls a smarter planet -- offers enormous hope for societal progress in health care, transportation, energy and other important spheres, its promise will only be realized if we address the important issues of privacy and security. In that spirit, IBM appreciates the

opportunity to provide this response to the Notice of Inquiry, and we look forward to further collaboration with the Commerce Department and others on these important issues.

Sincerely,

Harriet P. Pearson
Vice President, Security Counsel & Chief Privacy Officer
IBM Corporation

Intel Corporation is pleased to file comments on the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy." Intel commends the Department for conducting this inquiry and for their critical efforts on addressing privacy and innovation.

Our comments will address Intel's beliefs that: (1) there is a need for preemptive, comprehensive privacy legislation; (2) such legislation should be based on a robust reading of the OECD Fair Information Practices; (3) legislation should be technology neutral and allow for regulatory flexibility to address changing business practices; (4) the Department should encourage the adoption of the principle of Privacy by Design; (5) the Department should promote the accountability model for privacy protection; and (6) the Department should be commended for its work on the APEC Cross-Border Privacy Rules and should set a goal for adoption of those rules in 2011.

## I. Need for Federal Privacy Legislation

Intel is a company that believes in the importance of innovation to help solve important social issues of our time, and to provide real benefits for the lives of individuals. Through our experience in technology innovation, we see a world undergoing a dramatic evolution. Individuals are more connected, and a global flow of data is required for today's information economy. Information technologies are providing tremendous capabilities for virtually every aspect of our lives - how we work, play, socialize, and educate. With the opportunities that accompany this new digital society also come new risks, including more sophisticated computer-related threats, many of which directly affect user privacy.

Companies worldwide need to be able to work with each other to bring innovative solutions to the global market. In the technology sector it is rare when one company can work in isolation, whether they are creating hardware components, portions of the software stack, or services layered on top of the hardware and software. Companies need access to the best available people, processes and technology, irrespective of country of origin, to continue the innovations necessary to drive the global digital infrastructure, and remain competitive in the global marketplace. Laws and regulations impacting the ability to collaborate and share information across country boundaries need to keep pace with our technical need for such international collaboration. At the same time, in addition to these technical preconditions, building trust in the digital economy is an essential component of driving the global digital infrastructure forward. Building a trusted global environment in a systemic way not only benefits consumers and increases their trust in the use of technologies, but is vital to the sustained expansion of the Internet and future ecommerce growth. Intel strongly believes that comprehensive and preemptive U.S. federal privacy legislation is a key mechanism for building this consumer trust in the Internet and ecommerce.

II. OECD Fair Information Practices

Intel supports federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines. The principles in these guidelines are as follows:

1) **Collection Limitation Principle** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.
2) **Data Quality Principle** – Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3) **Purpose Specification Principle** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4) **Use Limitation Principle** – Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with principle 3, above, except: (a) with the consent of the data subject, or (b) by the authority of law.
5) **Security Safeguards Principle** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6) **Openness Principle** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7) **Individual Participation Principle** – An individual should have the right: (a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her; (b) To have communicated to him or her, data relating to him or her (i) Within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her; (c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d. To challenge data relating to him/her and, if the challenge is successful to have the data erased, rectified, completed or amended.
8) **Accountability Principle** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

III. "Use and Obligations" Model

Intel supports what is known as a "use and obligations" model, which has been thoroughly explained in The Business Forum for Consumer Privacy's paper entitled "A Use and Obligations Approach to Protecting Privacy," *available at* http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf. The "use and obligations" framework states that the way an organization *uses* data determines

the steps it is *obligated* to take to provide transparency and choice to the consumer, to offer access and correction when appropriate, and to determine the appropriateness of the data — with respect to its quality, currency and integrity — for its anticipated use. It imposes on organizations obligations based on five categories of data use: (1) fulfillment; (2) internal business operations; (3) marketing; (4) fraud prevention and authentication; and (5) external, national security and legal.

We believe that federal legislation should incorporate such a model, and we believe that the Department, with its understanding of the complexities of different business models, is well-positioned to promote with policymakers an understanding of the benefits to innovation and the growth of e-commerce of such an approach.

## IV. Technology Neutrality and Flexibility

Intel encourages the Department to promote legislation that is technology neutral and gives flexibility to the FTC to adapt the bill's principles to changes in technology. Maintaining technology neutrality in the legal framework provides protection for individuals in a rapidly evolving technological society, as the creation of legislative and regulatory requirements will invariably trail innovation of new technology. Therefore, a focus in the application of principles, neutral to the technology used, enables a flexible, effective and timely response.

## V. Accountability

Accountability is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation.[1] Though definitions of what is meant by "accountability" vary across these instruments, a useful approximation is the following:

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.*[2]

---

[1] The accountability principle is included in:

- Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)
- Asia Pacific Economic Cooperation Privacy Framework (APEC Privacy Framework)
- The European Union's Directive on the Protection of Personal Data
- Canadian private-sector privacy law: The Personal Information Protection and Electronic Documents Act (PIPEDA), and
- The Safeguards Rule of the Financial Services Modernization Act of 1999, commonly referred to as the Gramm Leach Bliley Act.

[2] Center for Information Policy Leadership, submission for Galway conference convened with the OECD in Dublin, Ireland.

Accountability requires an organization to make responsible, disciplined decisions regarding privacy and security. It shifts the focus from an obligation on the individual to have to understand complicated privacy notices to an organization's ability to demonstrate its capacity to achieve specified objectives. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles which have privacy and security integrated as foundational elements. Intel and other like-minded companies are currently committing significant resources to "being accountable" in this way now.

We encourage the Department to promote an accountability model and to educate policymakers on the benefits of such an approach.

## VI. Privacy by Design

Over the past several years, regulators in multiple jurisdictions have called for more formalized and widespread adoption of the concept known as "Privacy by Design." Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation.

The consensus view of these regulators – including the European Article 29 Working Party, the FTC, and the European Data Protection Supervisor – has been that the voluntary efforts of industry to implement Privacy by Design have been insufficient. Intel believes that a Privacy by Design principle should encourage the implementation of accountability processes in the development of technologies. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a Privacy by Design accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

Thus, we would encourage the Department to take a leadership role in promoting a principle requiring that organizations should ensure that privacy is included as a principle in product and service development processes.

## VII. APEC Privacy Framework

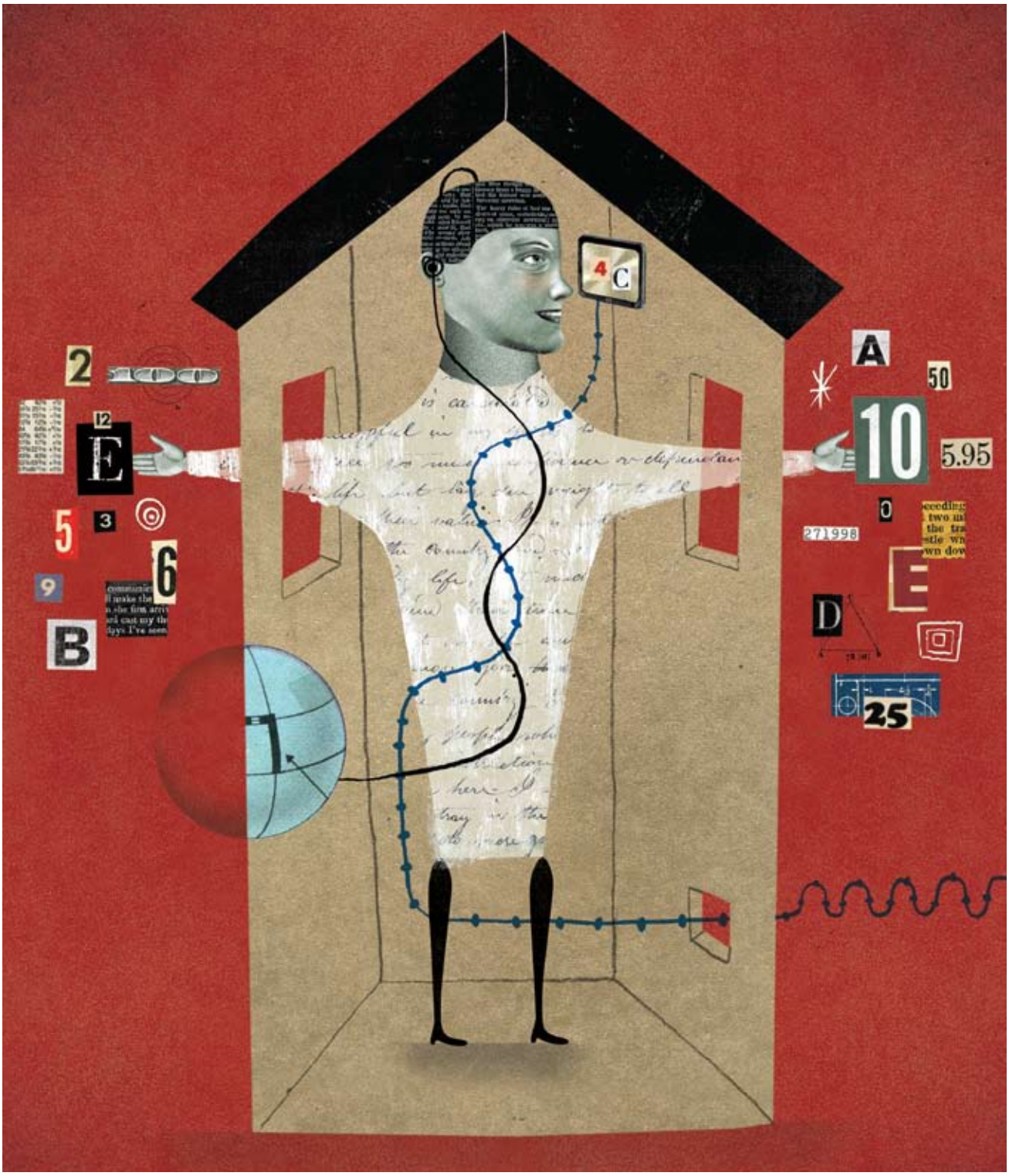
Intel commends the leadership of the Department of Commerce for its ongoing work within the Asia Pacific Economic Cooperation (APEC) to develop and implement a privacy framework. Since the APEC Ministers endorsed the Privacy Framework in 2004, the Department, in conjunction with other federal agencies, has taken a leadership role and made great progress to develop a system of Cross-Border Privacy Rules that would ensure accountable cross-border flows of information while both protecting consumers and allowing for the benefits of ecommerce. As the U.S. hosts APEC next year, we encourage the Department to continue its active leadership within APEC with the goal of ensuring adoption of the cross-border privacy rule system in 2011 during the U.S. host year.

## VIII. Conclusion

Intel again thanks the Department for their leadership in this important issue. We are supportive of the Department playing a role in this debate, and we look forward to continuing our engagement in helping to think about ways to improve the overall protection of privacy and the promotion of innovation and ecommerce.

# A CALL FOR AGILITY:

## The Next-Generation Privacy Professional




International Association of Privacy Professionals

# A CALL FOR AGILITY:
## The Next-Generation Privacy Professional

International Association of Privacy Professionals

## Table of Contents

# A Letter from the IAPP


It is with great pleasure that we present to you the first whitepaper to be published by the IAPP on the future of the privacy profession.

"A Call for Agility: The Next-Generation Privacy Professional" is the culmination of months of coordinated effort between IAPP leadership and many of the top minds across the global privacy community — the executives, academics, officers, and regulators that helped shape and continue to define the laws, technologies, and practices that are the core of work. Most importantly, this paper reflects the real experiences and thoughts of you, our members, through the member survey process that the IAPP undertakes each year.

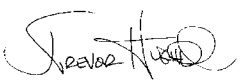
Over the past 10 years the IAPP has reperesented the ever-growing privacy community as the largest association of privacy professionals. We are committed to developing and offering educational resources, professional development programs, and forums for debate and discussion among businesses, governments, and nonprofits in the global privacy arena. We now look with great interest and enthusiasm to what we all will face in the next 10 years.

We trust that you will find the contents of this report both a worthy tribute to the history we have made together as well as an enlightened look toward the challenges only now emerging — and those we have yet to encounter. We encourage you to leverage the insights described here in planning your privacy programs and building your teams for future success. And we invite you to join us as we continue to define, promote and improve the privacy profession globally in the coming years.

Sincerely,

**Nuala O'Connor Kelly, CIPP/G**
Chief Privacy Leader
and Senior Counsel
General Electric Company
President, IAPP

**Harriet Pearson, CIPP**
VP Security Counsel and
Chief Privacy Officer
IBM Corporation
Chair, Project Advisory Board



**J. Trevor Hughes, CIPP**
Executive Director
IAPP

# Acknowledgements

"A Call for Agility" represents the combined expertise and perspective of a diverse group of authors, contributors, and advisors without whom the report you now hold would not have been possible. The IAPP wishes to express its sincere thanks to these many talented individuals for their generous contributions of time and insight:

- To the research project chair: Harriet Pearson, CIPP, Vice President Security Counsel and Chief Privacy Officer, IBM Corporation, and to the report's author, Jay Cline, CIPP, Minnesota Privacy Consultants

- To the project advisors: Dean Forbes, CIPP Senior Director, Merck & Co., Inc.; Jeff Green, CIPP/C, Vice President, Global Compliance and Governance and Chief Privacy Officer, RBC Financial Group; Kirk Herath, CIPP/G, Vice President, Chief Privacy Officer and Associate General Counsel, Nationwide Insurance Companies; and Zoe Strickland, GIPP/G, Vice President, Chief Privacy Officer, Walmart Stores

- To the project contributors: Martin Abrams, Senior Policy Advisor, Hunton & Williams LLP; Bojana Bellamy, Director of Data Privacy, Accenture (UK) Limited; Agnes Bundy Scanlan, Esq. CIPP, Chief Regulatory Officer, TD Bank North America; Joyce Brocaglia, President & Chief Executive Officer, Alta Associates; Ann Cavoukian, Ph.D., Information & Privacy Commissioner, Ontario, Canada; Peter Cullen, CIPP, Chief Privacy Strategist, Microsoft Corporation; Malcolm Crompton, CIPP, Managing Director, Information Integrity Solutions Pty Ltd.; Michelle Dennedy, Vice President Security and Privacy Solutions, Oracle Corporation; Sandra R. Hughes, CIPP, Global Privacy Executive, Procter & Gamble Company; Alexander W. Joel, Civil Liberties Protection Officer, Office of the Director of National Intelligence; James Harlan Koenig, CIPP, Practice Leader, Privacy & Identity Theft, PricewaterhouseCoopers LLP; Deirdre K. Mulligan, Assistant Professor, School of Information, Faculty Director, Berkeley Center for Law and Technology; Brian O'Connor, Chief Security and Privacy Officer, Eastman Kodak Company; Nuala O'Connor Kelly, CIPP/G, Senior Counsel, Information Governance & Chief Privacy Leader, General Electric Company; Richard Purcell, CIPP, Chief Executive Officer, Corporate Privacy Group; and Jennifer Stoddart, Commissioner, Office of the Privacy Commissioner of Canada

## Purpose and Methodology

The International Association of Privacy Professionals commissioned this work on the occasion of its tenth anniversary in March, 2010. The purpose of the project is to take a step back and help privacy professionals see the changing opportunities that lie before them. A panel of advisors gave of their time generously to offer insights and to guide the approach and methodology used in this paper.

Many privacy professionals and noted experts were interviewed for this report. Data was also drawn from the IAPP's Privacy Professional's Role, Function and Salary Survey (2010, IAPP), Benchmarking Privacy: an Executive Summary published by the IAPP and the Ponemon Institute, as well as other sources.

- The IAPP's "Privacy Professional's Role, Function and Salary Survey" (2010, IAPP) included a total of 23 items, and was fielded electronically in December of 2009 to approximately 6,000 IAPP members. More than 880 individuals completed the survey for a response rate of 14.8%. To maintain complete confidentiality, the survey instrument did not capture individual or company specific information of any kind.

- "Benchmarking Privacy: An Executive Summary" surveyed in total 336 IAPP member organizations. Each organization selected for participation included a privacy officer or the equivalent plus staff members within that group. The recipients were IAPP members and senior privacy officials in both the public and private sectors. The survey was sent by mail, and data was gathered during two periods between August 1, 2008 and mid January 2009.

## Executive Summary

The next 10 years will see more types of data collected from more people, and more privacy laws in more places. A deepening and broadening of data protection regulations in the industrialized world will spread to emerging markets and place a higher premium on legal and compliance acumen. In addition, an expansion of health information networks, smart grid networks and cloud computing platforms will make industry and technology expertise a more indispensable part of practicing privacy.

Privacy career opportunities will abound. A rise in privacy awareness among small- and medium-sized businesses, government agencies and other organizations—as well as ongoing maturation of roles pertaining to information governance, risk management, data security, and compliance—will create new career paths and opportunities for privacy professionals. Indeed, the diversity of the skills that today's privacy professional has had to develop will prove useful to a number of other organizational functions. Nothing will remain static in this field, and demand will not slow down. Even amidst economic uncertainty, heightened information risks resulting from ongoing cyber crime and other threats will tend to insulate budgets dedicated to the protection of valuable personal data, and undergird strong growth in the profession.

Despite these promising opportunities, the privacy professional's success in the next decade will demand greater adaptability and most importantly, agility. The agile privacy professional is the next-generation privacy professional: an expert practitioner who is keenly attuned to cultural and regional distinctions as these continue to grow in an increasingly interconnected data economy; who can migrate and adapt to different roles within an organization and offer value at each; who exhibits both comfort and grasp of legal/compliance and technical disciplines; and who instills direction and leadership of privacy management within the organization.

# Introduction

In the heady days of the dot-com boom, a new profession was born. The emergence of the Internet and new privacy regulations in Europe and North America by the late 1990s had ushered into the executive suite a new arrival: the chief privacy officer. Called something different in different organizations, those chosen for this new leadership role quickly sought one another out. From this early camaraderie emerged the International Association of Privacy Professionals. The IAPP soon became the focal point for fostering the support and growth of the nascent privacy profession. Through its conferences and Certified Information Privacy Professional credentials, the IAPP gave a structure to this new discipline.

Much has changed in a decade. The information revolution has intensified, connecting people and machines worldwide through Web-enabled devices. Public-sector initiatives aimed at preventing terrorism and fighting global crime rings perpetrating identity fraud have led to the expansion of governments' accumulation and use of personal data. Moreover, a patchwork quilt of local, national, and supranational privacy and security regulations now blankets the industrialized world. Reflecting the privacy and information policy issues spawned by this historic transformation, the number of privacy professionals has grown at double-digit rates and continues to increase despite a protracted economic downturn. And while privacy professional jobs initially were clustered in a few geographies, the IAPP's increasingly international membership shows that the phenomenon of the privacy professional has spread to more than 50 countries.

What will the next 10 years portend for those earning their living enabling organizations to address privacy expectations and compliance obligations? This whitepaper offers an informed and actionable set of insights on this question.

Supplementing an association-wide membership survey, a blue-ribbon panel of seasoned privacy professionals, academics, consultants, and other advisors drew upon its collective sense of important trends in business, regulation, and technology to project the likely paths privacy professionals will take—and what it will take to navigate them.

A diverse array of professionals will benefit from the insights presented on the following pages:

- Privacy professionals who seek guidance in planning for the experiences and skills they will likely need in the years to come;
- Executive leaders with overall responsibility for human resources, legal, risk management, and technology—the leaders to whom today's privacy professionals often report—will use this document to inform organizational and leadership development;
- Prospective privacy professionals (individuals new to the field or transitioning from related fields such as legal compliance, information auditing, information security, etc.) desiring more context about privacy as a growing profession;
- Recruiters and human resources professionals looking to place candidates in a job market that continues to grow;
- Press and media seeking to cover privacy and related topics; and,
- Regulators, legislators and policy executives who increasingly interact with privacy professionals.

# The Emergence of a New Profession: Drivers of Change

The privacy profession is burgeoning today due to three formative developments: the dawn of the Information Age, the regulatory tsunami, and increased data collection. The globalization of commerce and business operations has intensified the impact of these changes.

## *Driver One: The Dawn of the Information Age*

Advances in information technology have for more than a century prompted debate in the West about how society can maintain personal privacy amidst the changes. It was the spread of the use of the photographic camera that famously led the future U.S. Supreme Court Justice Louis Brandeis to note in an 1890 edition of the Harvard Law Review, "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" The subsequent inventions of the radio, motion picture, and television prompted further public commentary about privacy. In spite of these developments, however, nothing resembling a privacy profession had materialized.

Similar ongoing developments throughout the twentieth century set the stage for a late-century revolution of sorts. For decades, organizations had been reaping the benefits of information technology-fueled productivity enhancers, and some sectors—most notably credit reporting, financial services, and data brokerage—had amassed huge quantities of consumer data. Meanwhile, households were steadily integrating personal computers into daily life. The widespread availability by the mid-1990s of the World Wide Web sparked a revolution in both of these worlds. Ordinary people armed with a desktop computer and dial-up modem could now access a rapidly proliferating network of information previously only available in libraries and filing cabinets. And organizations of any size could now conduct a wide range of business operations—including e-commerce direct to consumers instantaneously and globally. The world is still adjusting to this computing revolution...

Social commentators dubbed this emerging era "the information age." Indeed, the world had begun amassing information on an unprecedented scale. Whereas data processors in the early 1990s measured their capacities in bytes, by decade's end they had shifted that reference point to terabytes—one trillion bytes.

This rapid accumulation of digital data expanded beyond hardbound, encyclopedic reference materials. Data about individuals' behavior and preferences became much more available and easy to collect on the Web. This trend, at this point in time, became the principal driver in creating what would become a global privacy profession.

Academics and civil liberties advocates warned about the impact of this accelerated accumulation of personal information. Professor of Law Emeritus Alan Westin was one of them. In 1967, Westin published what would become known as the seminal treatment of information privacy in the modern era, the book Privacy and Freedom. In 1972, he followed with Databanks in a Free Society, and his public-opinion surveys—conducted regularly over several decades—by the 1990s indicated a growing loss of consumer confidence in institutions' protection of private data.

Several other notable academics contributed to a growing body of published work on privacy issues and risks during the 1970s and 1980s. Paul Sieghart, a British human rights lawyer and author, published Privacy and Computers in 1976 and Canadian David Flaherty authored a study on government data banks, Privacy and Government Data Banks: An International Perspective. Lastly, Frits Hondius of the Council of Europe wrote Emerging Data Protection in Europe, the purpose of which

was to "describe the dawn of a new corpus of law in Europe called "data protection".

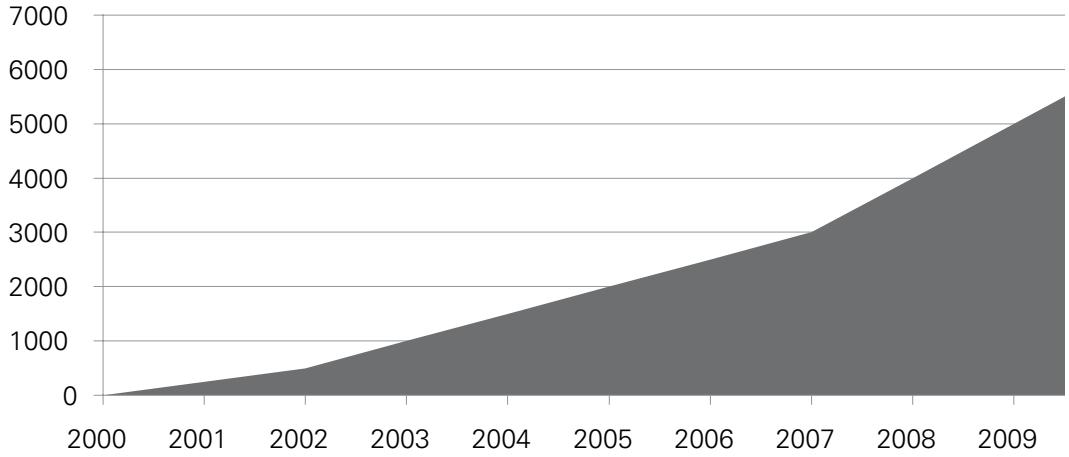
Another privacy pioneer, Washington, DC attorney Ronald Plesser, who began overseeing government-wide compliance with federal privacy law in 1975, warned of the dangers of combining federal and commercial databases. During this pivotal period, several privacy advocacy groups added their voices to the debate:

- The American Civil Liberties Union Privacy and Technology Project, 1986-1993
- The Australian Privacy Foundation, 1987
- Privacy International, London, 1990
- Privacy Rights Clearinghouse, San Diego, 1992
- The Electronic Frontier Foundation, Washington D.C., 1993
- The Electronic Privacy Information Center, Washington, D.C., 1994
- The Center for Democracy and Technology, Washington, D.C., 1994

During the same time period, the Arkansas-based databroker Axciom Corp planted a seed for the nascent privacy profession when, in 1991, it became one of the first organizations on record to appoint a chief privacy officer, Jennifer Barrett. A handful of other credit-reporting agencies and financial institutions also appointed privacy officials, further underscoring the increasing need for a senior professional focused on privacy issues in data management.

In the ensuing years, further technological developments have continued to drive the evolution of the privacy profession. Online social networks, networked digital health records, genetics-based tests and medicines, smart appliances and grids, and cloud computing are among the more noteworthy examples. People and devices are collecting and sharing more personal data than ever before. The dawn of the Information Age has become the late morning, and everyone is wide awake.

**IAPP Members**



## *Driver Two: The Regulatory Tsunami*

A surge in regulatory developments in the 1990s drove waves of compliance needs that affected numerous organizations. Most of this impact concerned private sector organizations though some countries, often those that started early, addressed the public sector first then later extended into the private sector.

The European Union Data Protection Directive (95/46/EC), was and remains a regulatory epicenter. Enacted in 1995 and effective in 1998, the EU Directive drove the harmonization of data privacy regulation across the newly formed EU. It also "exported" these obligations through its most distinctive feature: a prohibition on the transfer of personal data from the European Economic Area to other jurisdictions required that the transferring organization either have appropriate contractual measures in place, make use of standard contractual clauses and/or ensure that the information was received by organizations in jurisdictions deemed by E.U. officials to be 'adequate'. At the time, very few countries outside of the E.U. had formalized an equivalent manner of data protection legislation with the notable exceptions of Australia and New Zealand, each of which enacted privacy laws in the late 1980s which were modeled around the Organization for Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" (also known as the OECD Principles).

Beginning in 2000, the legislatures of Canada, Argentina, and Australia passed comprehensive privacy laws. At the same time, the U.S. Department of Commerce negotiated the Safe Harbor Agreement with the European Commission that would enable U.S. companies in most sectors to maintain streamlined compliance with EU transborder data privacy requirements.

The influence of the European approach to privacy regulation continues to be felt beyond the bloc's borders of the twenty-seven EU member states. Russia, India, South Africa, and the Philippines, for example, have studied and in some cases adapted elements of the EU approach in developing their domestic privacy laws.

**Early Privacy Regulation Milestones**

Several scholarly and regulatory milestones established the foundations of the 1990s wave of privacy regulations.

| | |
|---|---|
| 1890 | The Right to Privacy by Louis Brandeis and Samuel Warren |
| 1948 | Article 12 of the Universal Declaration of Human Rights |
| 1960 | Privacy by William Prosser |
| 1966 | U.S. Freedom of Information Act |
| 1967 | Privacy and Freedom by Alan Westin |
| 1970 | U.S. Fair Credit Reporting Act |
| 1973 | Fair Information Practice Principles defined by the U.S. Health, Education & Welfare Privacy Commission |
| 1974 | U.S. Privacy Act |
| 1978 | France Data Protection Act |
| 1978 | First International Conference of Data Protection and Privacy Commissioners |
| 1980 | Organization for Economic Cooperation and Development (OECD) "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" |
| 1981 | Council of Europe Convention on the Protection of Personal Data |

Europe was not the only regulatory epicenter of the 1990s. The United States—which had inherited a history of privacy concerns distinct from Europe's—was also active. The U.S. Congress passed a succession of privacy laws and requirements that applied to individual business sectors. For example, the Health Insurance Portability and Accountability Act of 1998 (HIPAA) applied privacy and security requirements to the U.S. healthcare and health information management sectors; the Children's Online Privacy Protection Act of 2000 (COPPA) established certain restrictions on the marketing of products and services to children aged 13 and under; and the Financial Services Modernization Act of 1998 (also known at the Gramm-Leach-Bliley Act or GLBA) articulated guidelines around the collection of personal data in the banking and insurance industries in the U.S. Continuing this sector-by-sector approach, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM) regulating U.S.-based electronic mail marketing, and Fair and Accurate Credit Transaction Act (FACTA) in 2003, which amended the Fair Credit Reporting Act of 1970 (FCRA) overseeing credit reporting agencies.

Together, the European and American privacy laws enacted between 1995 and 2003 constituted a significant regulatory wave focused on foundational privacy protections. Many organizations suddenly found themselves in need of privacy professionals.

U.S. legislative activity was simultaneously accompanied by a cluster of voluntary self-regulatory initiatives. A group coordinated by Ronald Plesser—the Individual Reference Services Group— by 1997 had adopted privacy principles to govern the data brokerage industry. The Direct Marketing Association (DMA) also was in the process of requiring members to use its "suppression" lists of consumers who had opted out of direct marketing.

This period also witnessed the emergence of trust seal programs and services. TRUSTe launched its seal in 1997, and the Better Business Bureau began offering its BBBOnline seal in 1999. Similarly, a group of large U.S.-based multinationals formed the Online Privacy Alliance in 1998, agreeing to abide by a set of common privacy principles. These quasi-regulatory initiatives contributed to a demand for privacy professionals in the United States, even within sectors not directly regulated by the federal government. Similar efforts emerged in Europe, with the EuroPriSe seal program offering certification for IT products and services, and in Asia with the Asia Trustmark Alliance.

The enforcement efforts of the Federal Trade Commission (FTC) and the state attorneys general were also a factor contributing to a greater demand for privacy professionals in the United States relative to other regions. Between 1998 and 2003, using its authority under Section 5 of the FTC Act, which prohibits unfair or deceptive practices, and statutes such as the Fair Credit Reporting Act (FCRA) and COPPA, the FTC investigated and negotiated consent agreements with several organizations for allegedly making statements about their privacy and security practices that departed from their existing practices or violated applicable rule requirements. "The Commission carefully considered information gathered from consumers, businesses, privacy advocates, and other regulators through public workshops and other means, and recognized industry self-regulation as an 'important and powerful mechanism for protecting consumers', but also brought a compelling message regarding privacy compliance for consumers and companies through its education and enforcement activities," explains Dean Forbes, a former FTC prosecutor who worked on the agency's initial privacy and security enforcement actions and is now senior director in the privacy office at Merck, the pharmaceutical company.

Forbes cites as an example a 2000 FTC Report to Congress about online profiling which commended an innovative self-regulatory proposal intended to address privacy concerns

expressed by consumers, but also called for Congress to enact legislation that would complement industry self-regulation and provide privacy protection for consumers with regard to such practices. The agency created the Advisory Committee on Online Access and Security, comprised of industry, government, and consumer advocacy leaders, in an effort to further understand certain Fair Information Practice Principles going beyond "notice" and "choice." Moreover, the agency quickly sought to bring enforcement actions and also designed readily available consumer and business education materials that addressed privacy and security issues for adults and children. The FTC's initiative in this area created a need for U.S.-based organizations to direct resources toward aligning privacy notices with data practices.

**FTC Enforcement Actions Addressing Privacy and/or Security Practices**

| Year | Organization Name |
|---|---|
| 1999 | GeoCities |
| 1999 | Liberty Financial Companies, Inc. |
| 2000 | ReverseAuction.com, Inc. |
| 2000 | Equifax, TransUnion and Experian |
| 2000 | Rennert, et al |
| 2000 | Toysmart.com |
| 2000 | Performance Capital Management, Inc. |
| 2001 | Bigmailbox.com, Inc., Monarch Services, Inc., et al. (Girls' Life), Looksmart Ltd. |
| 2002 | Eli Lilly |
| 2002 | Microsoft |
| 2002 | Quicken Loans, Inc. |
| 2003 | National Research Center for College and University Admissions |

*Source: www.ftc.gov*

### *A Second Wave of Regulation*

The initial wave of privacy regulation, self-regulation, and enforcement between 1995 and 2003 yielded to an aftershock of regulatory activity that continues to this day. In the United States, the second wave of privacy regulation shifted to an acute focus on information security management and data retention. California's breach-notification statute (SB-1386, passed in 2003) triggered, in the subsequent three years, similar legislation in nearly every other U.S. state, most notably in Massachusetts as recently as March 2010. As a result, hundreds of organizations disclosed data security lapses and suffered reputational and financial damage. Thousands more took steps to respond to this new set of enterprise risks. Heightened management attention to these risks often resulted in expanded duties for privacy professionals.

The popularity of breach-notification regulation eventually spread to the European Union, which in 2009 amended its Telecommunications Directive to require breach notification. Also in 2009, the U.S. Congress amended HIPAA to include health information breach-notification provisions via the Health Information Technology for Economic and Clinical Health Act (HITECH). Lastly, Germany adopted breach-notification requirements in 2009, and the French Senate began considering similar rules.

Back in the United States, the information security programs of the payment card brands merged in 2006 into the Payment Card Industry (PCI) Data Security Standard (DSS). The card brands directed their initial focus on enforcement within the United States. Information security legislation passed by the Minnesota, Nevada, and Massachusetts legislatures during this time supplemented the private industry PCI standard, raising the specter of another impending wave of state-level regulations. Meanwhile, new electronic discovery rules approved by the U.S. Supreme Court in late 2006 increased the need for organizations to conduct data inventories and implement data-retention policies.

During this timeframe, the diverse cultures of Asia began to develop a common path on privacy. The Asia-Pacific Economic Cooperation (APEC) privacy framework became the most noteworthy development of broad significance to the region. Approved in 2004, the framework blended fair information principles similar to the OECD guidelines with a harms-based approach to regulatory enforcement. The framework and accompanying commentary provided a source of privacy rulemaking and industry self-regulation for this region.

Some Asian countries have since focused legislation on the information security aspects of privacy. India, for example, in early 2009 enacted comprehensive legislation covering the security of personal information. China followed in late 2009, passing a national level duty to protect personal information. While much of Asia has yet to make a full entrance into the privacy regulatory landscape, its first common steps greatly expanded the horizon of interest for the privacy profession and introduced an approach based less on privacy as a human right than as a useful objective.

In Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) came into force in stages, beginning in 2001. The act was passed as part of the government's Electronic Commerce Strategy , a policy initiative said to have been motivated by the desire to make Canada a world leader in electronic commerce. It was followed by the Personal Health Information Protection Act of 2004 (PHIPA), Ontario's health-specific privacy legislation, which governs the way personal health information may be collected, used, and disclosed.

The diverse approaches to privacy regulations around the world led to the creation of harmonizing initiatives. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in 2006 released the Generally Accepted Privacy Principles (GAPP Framework) which have become a leading standard for audit and consulting firms.

**Today's privacy professionals—many of whom have been hired to help their organizations meet regulatory compliance needs—entered the profession while many of these rules were still being written. To this end, privacy regulation promises to continue to be a driver of change for the profession.**

## *Driver 3: The Rise of Governmental Data Collection*

Since before the times of Ancient Rome governments have sought to keep a census of their citizens. This need and ability of governments to collect information about people residing within and passing through their borders developed over time, in different ways, in different regions. But it was in the West where citizens first expressed their desire to institute a control on this power. Indeed, several of the first privacy-related statutes—Article 12 of the 1948 Universal Declaration of Human Rights; the 1966 U.S. Freedom of Information Act and subsequent FOI acts in Canada, the UK, and Australia; and the 1974 U.S. Privacy Act—were focused on the government sector.

As noted previously, these government-focused regulations were the origin of many of the first professionals dedicated full time to protecting personal privacy. Certain agencies—particularly those that interact with citizens directly, such as the U.S. Internal Revenue Service, Postal Service, and Census Bureau—were also working to address broader privacy trends. The roles of privacy professionals in such agencies mirrored those of their industry counterparts: conducting personal data inventories, developing policies and procedures, and completing privacy-impact assessments, for example. These roles continue to this day, and the number of professionals has grown.

They address new legal requirements, such as the U.S. eGovernment Act and develop best practices. Indeed, in the 2010 IAPP Privacy Professional's Role, Function and Salary survey, the government sector accounted for the second-highest number of respondents, most of whom hail from citizen-facing agencies such as the Internal Revenue Service (IRS), Department of Homeland Security (DHS) and the Veterans Affairs Administration (VA). The nature of government data collection and its impact on the privacy profession would take a turn soon after the arrival of the millennium. The September 11, 2001 terrorist attacks and subsequent bombings in London, Madrid, Bali, and other locations, brought into fresh relief for Western publics the power of governments to collect personal data. Following the 9/11 attacks, the U.S. government sought information from airlines, data brokers, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial network, among others, to identify the attackers and prevent future attacks. Massive new databases were proposed. The USA Patriot Act in particular facilitated information collection and sharing among federal agencies. Indeed, prior to the Patriot Act, the Federal Bureau of Investigation (FBI) had been issuing approximately 8,500 National Security Letters each year to obtain information from corporations and others. Following the act, that average jumped to about 50,000.

Similarly, the Third Pillar of the European Union – involving police and judicial cooperation in criminal matters – saw an increase in data collection and sharing among European governments for counterterrorism purposes.

One of the most visible icons of this new era was the surveillance camera. Led by the city of London in the United Kingdom – which had installed an estimated 1.5 to 4 million cameras principally to prevent domestic attacks by operatives of the Irish Republican Army – other cities, including Paris, Copenhagen, Oslo, New York, Washington, DC, Chicago, Winnipeg, Vancouver, and Sydney deployed thousands of new cameras in their public spaces in the years following the 9/11 attacks.

How did the rise of counterterrorism data collection change the privacy profession? In the United States, it added, albeit gradually, a new type of government privacy professional: the civil liberties and chief privacy officer whose key mandate encompasses counter-terrorism and related privacy issues. In 2003, the U.S. Department of Homeland Security became the first agency to be required by statute to appoint a chief privacy officer. It appointed Nuala O'Connor Kelly, current president of the IAPP. Similar positions were subsequently created at the Department of Justice and Office of the Director of National Intelligence. These roles, and the staff that now support them, provide an oversight function that goes beyond compliance with government privacy laws and begins to address some of the public concerns raised in the aftermath of 9/11. While other government privacy professionals continue the yeoman work of administering privacy compliance, these new roles are more visible to Congress and policymakers globally. As Western governments continue to mount coordinated defenses against terror attacks and explore new ways of collecting and sharing information, their citizens will turn to the privacy profession for guidance and support.

### *Other Driving Factors: Globalization and Economic Uncertainty*

While technological advances and new regulations were shaping the need for a new profession, the globalization of world commerce continued, bringing new considerations to the fray. European and American organizations began outsourcing data and call center operations to emerging-market nations, Asia increased investments in the West, large-scale mergers and acquisitions and a heightened competition for all global markets began accelerating the pace of change. "There are few U.S.-only corporations anymore," notes Peter Cullen, CIPP, chief privacy strategist of Microsoft. "Almost all companies of any size now have an international partner somewhere in its value chain."

The economic slowdown that began in the West in 2008 and expanded worldwide by 2009 forced corporations to do more with less, to streamline, consolidate, and gain efficiencies. Privacy professionals were called upon to optimize the value of their organization's data, for example, by facilitating cross-border transfers of data, and by accomplishing their goals with limited resources.

The combination of these two powerful trends — economic activity spreading rapidly across borders and the pressures of doing more with less brought on by the worldwide recession — have pushed information privacy practices into an ever increasing focus. The privacy profession's origins in technology, regulation, and counterterrorism within the context of expanding globalization will continue to shape the trajectory of the profession.

## Today's Privacy Professional: At a Crossroads

As addressed in this paper, three dynamics have largely shaped the privacy profession to date: the dawn of the information age, a tsunami of privacy regulation, and the rise of governmental data collection. In addition, growing scrutiny of data security breaches and an increasingly intertwined global economic marketplace have exerted additional influences on the scope of the privacy role.

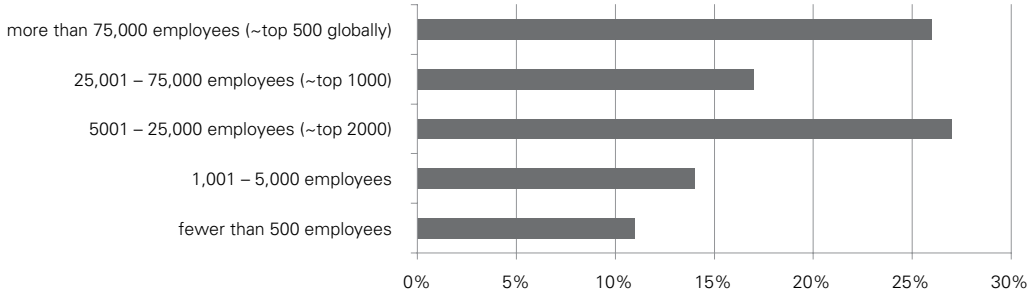
The profile of today's privacy professional suggests a role in transition. This change is being driven by a number of factors: Organizations of a growing variety of sizes are employing privacy professionals ("organizational diversification"); the profession is expanding outside its North American locus ("regional diversification"), privacy professionals are being positioned at many organizational levels and in a variety of functions ("migration across the organization"); and while most professionals see their responsibilities changing or expanding in the coming year many common tasks remain intact ("stabilization of daily privacy tasks").

### *Organizational Diversification*

In the first 10 years of the privacy profession, large organizations—those ranking in the equivalent of the top 2,000 companies worldwide—employed the lion's share of privacy professionals. In the 2010 IAPP salary survey, three quarters of respondents worked for organizations with more than 5,000 employees. This is likely because only large organizations thought they could afford a privacy leader.

But even this is starting to change. As the risk of noncompliance rises for organizations of all sizes, small- and medium-sized organizations are starting to adjust their cost-benefit analysis on hiring data protection and privacy experts. "I think we are already seeing a trend where many medium-sized firms now also rely on a privacy professional," notes Zoe Strickland, CIPP/G, chief privacy officer at Walmart.

**Today's Privacy Professionals are Concentrated in Large Organizations**




*Source: Benchmarking Privacy: An Executive Summary and Forbes Magazine Global 2000.*

It's a trend that seems likely to continue and grow further. According to credit card issuer VISA more than 80 percent of credit card breaches occur at the smallest level merchant. Each breach carries with it the potential for fines originating from the payment card brands, as well as more costly compliance obligations. Smaller companies that provide services to larger corporations are also falling within the purview of the larger corporations' vendor-assurance programs, which are dictating privacy requirements to them.

"At IAPP events we're already seeing more people from small- to mid-size organizations," added Sandy Hughes, CIPP, global privacy executive at Procter & Gamble and past president of the IAPP.

This shift could significantly change how the privacy profession meets and learns and what issues become its top priorities. The complex organizational challenges of large multinationals may be joined by the more tactical and sector-specific realities of the small business.

## *Regional Diversification*

In the first decade of the privacy profession, most professionals were employed by North American organizations. This may seem counterintuitive given that EU member states were the first to enact national data protection laws. Why wouldn't Europe dominate the profession? Some observers have noted that North American businesses, particularly those in the United States, have a commercial custom of collecting more information about people than their European counterparts and therefore have more information risk to be managed.

"Our benchmarks show that European companies collect less personal information about customers," Larry Ponemon, founder of the Ponemon Institute, explained in a related study, "and [they] are less likely to use this information for unrelated, secondary purposes."

So the North American appetite for data may have led to a high concentration of privacy professionals on the continent. But some suggest the numbers could be deceiving.

Bojana Bellamy, Accenture's global data privacy compliance lead, offers another perspective. "European companies do employ privacy professionals and have done so for 10 years," she said. "But the role is not at the level of the U.S. based CPO." In Europe, it is more legally and compliance focused, she says, often sitting in the legal department or mid-level management. Although I do believe this is starting to change - following some high profile data breaches in Europe the role has become higher level and more strategic."

Deirdre Mulligan, a former privacy advocate and current assistant professor at the University of California School of Information, agrees. Says Mulligan, "to a greater extent than in other geographies, the most strategic and high-level privacy officers tend to work for U.S.-based organizations where they are tasked with creating and deploying sophisticated information-governance strategies for highly visible brands."

"There are interesting directions being taken right now in the transatlantic debate," notes Malcolm Crompton, managing director of Information Integrity Solutions and former privacy commissioner of Australia. "A new dynamism is emerging—a more questioning approach on what might work because there is a feeling that more work is needed."

Nonetheless, the profession continues to evolve. The number of non-U.S. members of the IAPP has increased over the past several years. Moreover, the respondents to the IAPP salary survey showed an even greater diversification outside the U.S. The adoption of breach-notification requirements across Europe and Asia could accelerate the diversification of the profession, as organizations become compelled to make their data practices more transparent to the public. If the center of gravity of the privacy profession shifts from Washington and Ottawa toward Brussels, Buenos Aries, and Beijing, the profession will likely get an injection of fresh new ideas on how to conduct privacy assessments, how to document and communicate privacy policies, how to hold vendors accountable, and even how to define what privacy is.

"When I'm speaking to business partners about the importance of privacy," said Sandy Hughes, "the argument of ensuring trust among constituents seems to resonate more in the U.S., in my experience, than in Europe or Asia where whether a country has a law or not seems to be the first concern."

"In Europe, satisfying laws and regulations seems to be the primary focus. Similarly, in Asia, a common first response to a privacy requirement of mine is 'well it isn't against the law' to do such and such. However, when I share data that shows consumers do care about privacy the trust argument does work outside the U.S."

"We share more fundamental values about respect for fellow human beings than we differ over," notes Nuala O'Connor Kelly. "There is a "We share more fundamental values about respect for fellow human beings than we differ over," notes Nuala O'Connor Kelly. "There is a common desire for decency in the private zone that we can all build upon."

"I never use the word 'privacy' in Asia," explains Michelle Dennedy vice president of security and privacy solutions, Oracle Corporation. "'Information strategy' works better."

In Canada, privacy regulation is based on an ombudsman model, where the emphasis is less on court action than on dialogue, guidance and the search for better business practices.

"Indeed," says Canadian Privacy Commissioner Jennifer Stoddart, "One of the most interesting trends in that country is the evolution of 'soft law.' Emerging in the space between the traditional legislative and judicial branches of government, soft law uses tools as model codes, best practices, informal dispute resolution processes, and alternate modes of redress."

"It's widely argued that the adversarial court system is no longer as appropriate for the kinds of issues we face," notes Stoddart. "It's too cumbersome and costly, and the courts may not be set up to grasp the intricate, specialized issues that are our bread and butter."

The profession could be ripe for a paradigm shift as it becomes fully international.

## *Migration Across the Organization*

The first companies to appoint chief privacy officers in the late 1990s and early 2000s typically placed these leaders within senior positions but with limited budget and staff. A lot has changed in 10 years. While large multinationals and government agencies still employ high-ranking CPOs, more than half of the respondents to the 2010 IAPP salary survey indicated that they were positioned below the director level in their organizations. This suggests that there is no longer a single recipe model for privacy professionals' placement within an organization. It could also be indicative of a growth in privacy departments across multiple levels.

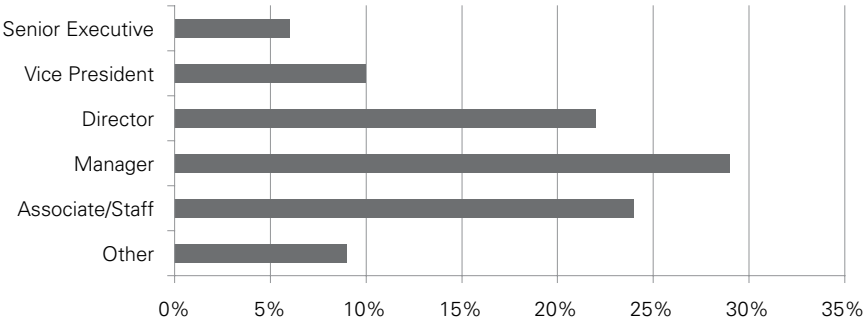
"It takes a team to develop and then to support an organization's implementation of information privacy policies," adds Harriet Pearson, CIPP, vice president security counsel & chief privacy officer at IBM. "Our team members come from a wide range of disciplines and levels, but we're united by our common strategy."

Today's privacy professionals also find themselves in a variety of departments. Three reporting structures are emerging as dominant:

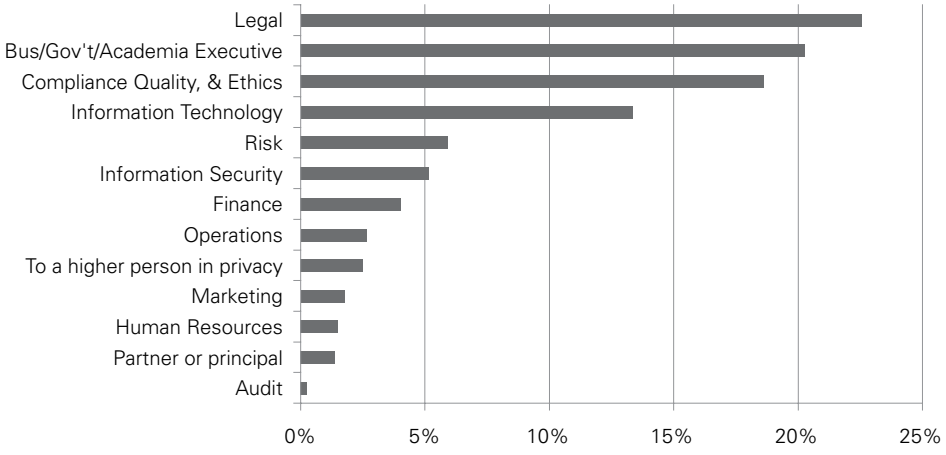
- reporting up through the general counsel
- reporting up through a business executive
- reporting up through the chief information officer

The heightened risk of privacy noncompliance —of data breaches in particular—has probably contributed to the focus on the legal and compliance areas.

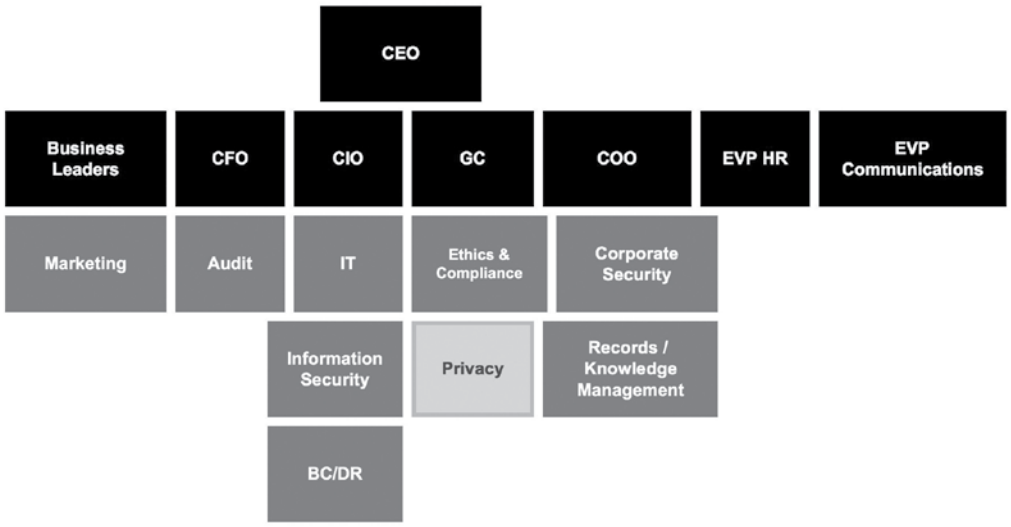
**Today's Privacy Professionals are Positioned at All Levels in the Organization**




**Privacy Professionals Report through a Variety of Functions**

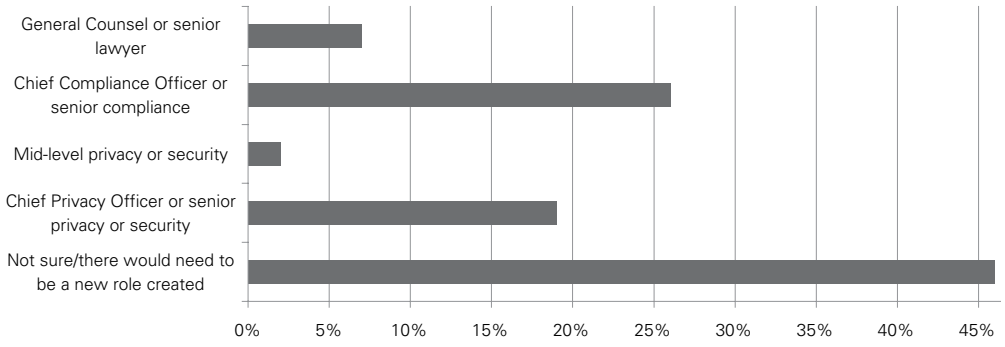


Many corporate privacy professionals find themselves within a structure similar to that depicted below, where privacy reports in through legal or compliance and information security reports in through the CIO.




But the information governance organizational structure is in flux, and as a result, today's privacy professional is at a crossroads. Indeed, 53 percent recently reported that they expect their job responsibilities will change in the next year or two. Most believe that promotion possibilities depend upon the creation of a new role in the organization. Short of creating a new role, privacy professionals responding to the IAPP salary survey indicated a desire to assume responsibility for data security as well.

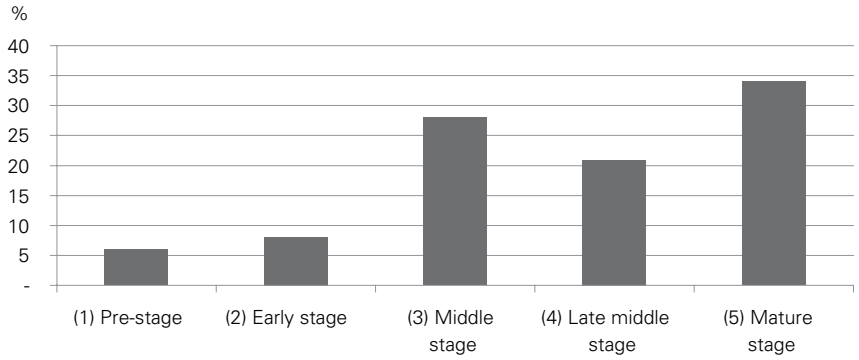
**Likely Next Promotions of Today's Privacy Professionals**



## *Stabilization of Daily Privacy Tasks*

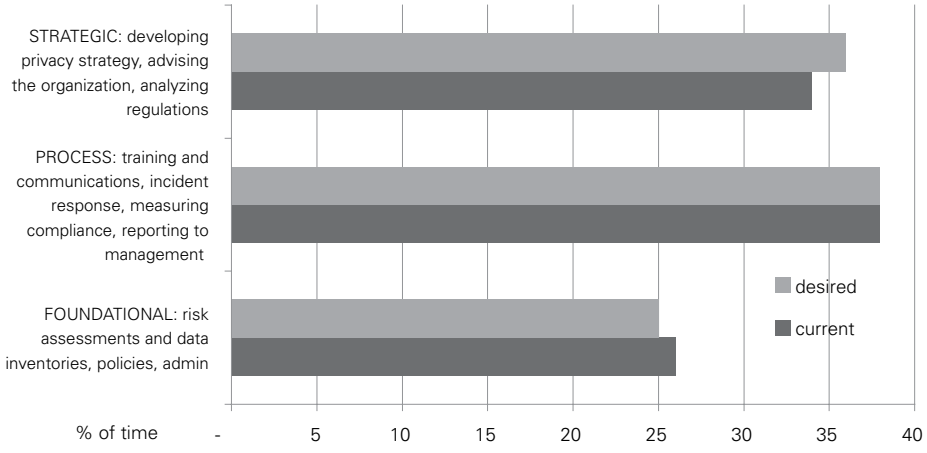
In the last 10 years, many privacy professionals have been focused on developing policies and procedures and responding to incidents. As a result, many of the privacy programs led by privacy veterans may be reaching maturity. A full 34 percent of the respondents to the IAPP's Privacy Professional's Role, Function and Salary Survey (2010) say their privacy programs are in the mature stage, and 49 percent say they are in the middle or late-middle stage.

**Privacy Professionals Rate Highly the Maturity of Their Programs**




When asked where they currently spend their time versus where they wish they could spend their time, respondents to the survey said they had found the right balance between foundational, process, and strategic tasks. This is an indicator that the privacy professional's daily tasks may be arriving at some predictability. It may also suggest that privacy professionals are self-directed, and have a good amount of control over establishing and prioritizing work items.

**Privacy Professionals Spend One-third of Their Time on Strategic Tasks and Desire Slightly Higher Share**




That said, the daily tasks of the privacy professional are not on the verge of becoming stale. "Most organizations today are in constant flux; changing products, business, employees," explains Kirk Herath, CIPP/G, chief privacy officer at Nationwide Insurance Companies. "Governing this will continue to mean updating policies and procedures and monitoring legacy programs."

"There will always be work in the program-build area as programs seek to improve, and as underlying laws and risks change," adds Zoe Strickland. "However, privacy programs will

indeed mature. That will allow the privacy leader to work strategically, beyond compliance, regarding the management of personal or business data."

Richard Purcell, former chief privacy officer at Microsoft and presently founder of the Corporate Privacy Group, sees much more work to be done. "An important question before us as we look forward to the next 10 years is this: 'How can we establish accountability and self-discipline while maintaining localized autonomy?'" Purcell says one answer may lie in, "how well we separate ourselves from the bad actors and free riders through stronger and more harmonized policy frameworks, compliance practices, and accountability standards."

Anecdotal evidence from privacy consultants operating across multiple sectors and geographies suggests that corporate privacy programs have been maturing over time, but at different paces in different regions. Canada has been a noteworthy leader. "I look to Canada frequently to see the future of where we're going," notes Michelle Dennedy, Oracle's vice president of business development for privacy and security.

A number of factors have spurred North American (and particularly American) organizations to dedicate more resources to privacy process improvement: most notably, PCI DSS enforcement, FTC enforcement, and data breach notification. Emerging enforcement and data breach notification in other OECD countries has prompted privacy process improvement there, too, but to a lesser degree. "The privacy process focus in Europe, driven in part by database registrations and compliance with certain other country-specific requirements, has prompted a different approach to resource allocation for privacy and data protection issues than in the United States," explains Dean Forbes, CIPP, senior director of the privacy office at Merck Corporation. "But that may change with additional focus on data breaches and related enforcement."

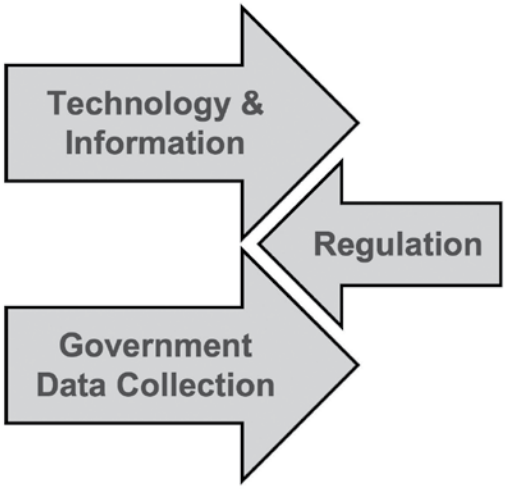
A lack of enforcement and resources at other organizations has left them in the earliest stages of privacy maturity. Maturity levels may also be varying geographically, potentially causing the agendas of privacy professionals to vary by region. Regardless of the sector, region, or position in the organization, following a transformative decade, today's privacy professional is poised to take advantage of an expanding horizon of opportunities.

# The Privacy Profession in 2020

Predicting specific outcomes, even near-term outcomes, with any level of accuracy is difficult. Given the known drivers that have shaped the profession's first decade and the current state of transition in which privacy roles appear to be, we offer some possible scenarios for the privacy role circa 2020. The trajectories of the original drivers of change offer some plausible outlines to consider.

## *Technology and Information*

One of the clear directions of technology in the past 10 years as it pertains to personal data has been more—more types of data collected from more people in more ways, and shared with more entities. The emergence of cloud computing—essentially a new computing paradigm in which data is stored off-premises and by a range of third parties—sets the pace for the next decade. Short of a wholesale social movement to opt out of information technology and "go dark," the conveniences and commercial benefits of more data collection and sharing seem to point in the direction of more. People will not "go dark," we estimate, because the utility of sharing information will continue to well exceed the risks of doing so. If the collection and sharing of personal data will increase over the next 10 years, will we approach an age of near-perfect information about ourselves and one another? If so, what will that mean for the privacy profession?




Nuala O'Connor Kelley, CIPP/G, chief privacy officer at General Electric and current IAPP president, and Oracle's Michelle Dennedy together draw a picture of daily life for tomorrow's privacy professional as it may appear in the not-so-distant future…

I*magine waking up in the morning, not because of an alarm clock, but because your bioalarm identified the peak time within your REM cycles to awaken you fully refreshed. You jump on the treadmill and it sends your exercise performance and bio-readings over the Internet to your personal health record (PHR). You grab some orange juice from the refrigerator, which records the amount taken via an RFID reader. It also sends that information to your PHR and updates your weekly grocery list, which is stored on your handheld device. The monitor in the kitchen displays all the social network updates and news stories—translated from foreign news organizations around the world—that it has learned you are most interested in. It has also prioritized all your incoming e-mails, texts, and voicemails from the previous eight hours based on your past message management. At the top is a meeting invite from your doctor, who would like you to come in to receive your DNA-personalized nutritional supplements and anti-carcinogen nanobots, and also talk about the cholesterol alerts he's been getting from your PHR. You hop in your electric car, which recharged at two o'clock that morning at the direction of the smart grid. You drive, obeying the posted speed limit, knowing that your insurance company will drop your rate if you do so. As you pass by your dry cleaner, your car's speakers sound an alert to let you know that your suit is ready. It's only nine in the morning, but you've already generated a terabyte of data in your personal account in the cloud.*

While such a scenario may incite a certain degree of consternation, if not alarm, in the eyes of privacy and consumer protection advocates, it remains a very possible extension of capabilities that technologies and systems offer today. Quite simply, if people do embed these types of innovations into their daily lives, a new role may materialize: the privacy engineer.

Companies that hope to market their innovations to a public more informed about their privacy risks will need to hire engineers who are also privacy experts. Their task will be to "bake in" privacy to their product designs.

The accumulation of sensitive personal data on the scale illustrated in the scenario above may also give rise to a new market niche: the personal privacy planner. This person could help erase past mistakes, monitor the public persona, and check on the security of the personal data account. If this development occurs, the privacy profession in 10 years may well expand out of organizational compliance into direct-to-consumer assistance.

In 2010, "there will be more technology in the hands of consumers," predicts Zoe Strickland. "This will range from simple RFID codes on products for easy returns, to complex and integrated applications offered through mobile devices." At the same time, Strickland adds, companies and other entities will have even more sophisticated back-end technologies to aggregate and analyze data from disparate sources. "Technology will absolutely remain a key driver for privacy."

Brian O'Connor, chief security and privacy officer for Eastman Kodak Company counters that this may only amount to a "numbing crush of boring information. At some point," he says, "there may be so much information out there that a data thief has a hard time finding anything usable."

Where the first chapters in privacy were defined largely by privacy notices, breach notifications, and international data transfers, Jim Koenig, practice leader of privacy and identity theft at PricewaterhouseCoopers, feels that the next era will be defined by corporate organizations and increased marketing sophistication as well as developments in health information technology. "Privacy will be profoundly shaped by companies desires to share information for business intelligence and derive revenue from direct and interactive marketing, the increasing inclusion of specific security controls in privacy laws, and the changes and investment in healthcare information used and the advent of electronic health records." he says.

Certainly, the privacy professional plays a key role in managing the data privacy issues inherent in any future scenario. The question for the next decade will be 'How many of the remaining 75 percent of the world not now online will become Internet users?' And how many people will participate in online social networks and media, or other connected technology? These questions raise another: What role will the privacy profession play in the globally networked civil society? Will the profession passively observe the phenomenon? Or will it take an active role in building trust in the Internet ecosystem? The path the profession chooses could well determine whether privacy will be viewed as something bad that happens to you, or an enabler of new horizons.

## *The Future of Regulation*

As long as citizens and consumers remain concerned about their personal information and legislators see an issue to be addressed, new privacy laws will be enacted. Looking out to the year 2020, what part of the privacy arena that is currently unregulated will catch the attention of legislators?

"Employee privacy in the United States," notes Agnes Bundy Scanlan, CIPP, chief regulatory officer of TD Bank North America and former president of the IAPP.

"Corporate video monitoring in the U.S.," says Brian O'Connor. "This is already hard to do in Canada and Europe."

The "Internet of things" may continue to come under regulatory scrutiny, speculates Sandy Hughes, referring to smart devices such

as sensors and RFID that communicates to and from humans and with one another to provide conveniences and efficiencies for consumers. "Right now the opportunities, economics, and technology are still developing, but that could speed up dramatically," she explained.

"Compliance-driven information security requirements will very likely increase in the coming decade," says IBM's Harriet Pearson.

The popularity of security breach notification has already gained traction in Canada, the United Kingdom, Germany, France, Australia, New Zealand, and Japan, and could well expand to all OECD countries. If breach notifications expose underlying weaknesses in corporate data practices, the laws could trigger a second wave of information-security regulation. Similarly, the success of the PCI Council in enforcing the PCI DSS in North America could result in enforcement of the standard in Europe, Asia, and beyond.

Canada's voluntary data breach notification guidelines, introduced in 2007, have been generally well received, because industry was integral to the process.

"We consulted broadly in the development of the guidelines, and we followed up with detailed interpretive documents," said Stoddart, the federal privacy commissioner. "We recognized that businesses are more likely to confess to serious data breaches if they have clarity on what is expected of them." Building on its experience in voluntary notification, Canada is now preparing to roll out a mandatory reporting regime.

The prominence of the European market and the requirements of the EU Data Protection Directive may well continue to persuade new countries to adopt national data protection laws. South Africa and Malaysia are already poised to do so and other APEC and Latin American countries might then find it more difficult to remain unregulated.

"Legislation will continue to increase," notes Brian O'Connor. "This will be a significant compliance issue, requiring privacy professionals to drive corporate programs."

As more countries regulate privacy, and if privacy is regulated across more sectors and technologies, will world privacy regulations begin to converge? Opinions vary.

Zoe Strickland sees convergence. "As rules converge, they will be principle-driven and technology neutral," she explains.

Jennifer Stoddart, now in the final months of her seven-year term as Canada's federal privacy commissioner is encouraged by the many initiatives underway that are seeking common ground among regulators. "A single, enforceable global standard for privacy won't materialize overnight, if ever," she says. But we are seeing a very determined push—in Europe, the Asia-Pacific region, within the OECD, and even in the U.S.—toward a more consistent and collaborative approach to the protection of personal information."

Stoddart notes that important global corporations have embraced these initiatives and are active in the dialogue. "They understand that a set of well-understood regulations, common to major jurisdictions, would bring a measure of legal certainty," she says. "That would promote both data privacy and robust global data flows."

Kirk Herath and Brian O'Connor, on the other hand, see further Balkanization of privacy laws into conflicting local and regional variances. But Jeff Green, chief privacy officer at Royal Bank of Canada, takes a middle ground. "I don't hold out a lot of hope for perfectly harmonized global regulations," he said, "but I think we'll continue to see a convergence of the key requirements found in the patchwork of laws and regulations already out there."

Sandy Hughes takes a similar stand. "I see more convergence of privacy frameworks, but continued local regulations. Ideally, if a company follows the framework it should get a 'free pass' for some of the local requirements in countries who recognize the framework."

What does this mean for the privacy professional of 2020? More laws in more places mean an extended role for legal experts both inside and outside of corporations, governments, nonprofits, and universities. It also means new positions within government agencies to enforce the new laws.

A landscape of conflicting privacy laws could leave the privacy profession mired in a protracted period of untangling the conflicts and adding less value to organizations and society. A Balkanized regulatory landscape could leave organizations viewing their privacy professionals as necessary tacticians, but not strategists invited to the planning table. To avoid this perception, "today's CPO needs to think broadly beyond legal terms and more about information risk and social impact," says Peter Cullen of Microsoft. Michelle Dennedy of Oracle Corporation believes it's incumbent on privacy officers to take the initiative. "It's up to us to be more strategic and less reactionary," she says.

The increasing importance of a proactive approach to privacy is a message frequently delivered by Ontarios Information and Privacy Commissioner Ann Cavoukian. "Fifteen years ago, taking a strong regulatory approach was the preferred course of action—but no longer. "Over the years, I have argued that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must come from making privacy the default within technology, business practices and networked infrastructure."

Richard Purcell thinks corporations can forestall more regulation through more comprehensive approaches to information governance. "At the end of this decade of growth in the professionalization of privacy and data protection," he explained, "there have been a number of leading companies such as Microsoft, HP, IBM, GE, Intel, Oracle, and Schering-Plough that have established enterprise-wide programs to manage personal information in strategically smart and responsible ways." He added that these approaches "have helped to diminish the appetite and perceived need for legislative and regulatory interventions."

If organizations continue on a more fragmented approach toward information governance, however, Purcell sees more regulation in the future. "That tolerance for independent judgment and decision (within autonomous operating units) may have the unintended consequences of data breaches and regulatory non-compliance that invite external control."

Nonetheless, ongoing regulation could have the indirect positive effect of propelling the upward maturity of privacy programs across all regions. Law firms, consultancies, and technology vendors serving privacy professionals in this scenario would face a market of increasing but still varied levels of privacy maturity. In order to remain competitive, they would need to offer high-end products and services to the North American, European, and some Asian markets, and foundational products and services to emerging markets.

At the same time, a rising awareness among small- and medium-sized businesses of the need for privacy compliance would generate new markets for delivering privacy products and services in a mass-produced, low-cost manner. As privacy compliance needs spread to new geographies and the vast market of small- and medium-sized businesses, today's privacy professionals will be best poised to compete for these new career opportunities.

## Governmental Data Collection

A more speculative future lies ahead for government agencies' exploration of new information technologies and the potential citizen response. Two scenarios could unfold, with differing impacts on the privacy profession. The table below portrays how we chose these two scenarios from among four potential intersections between government data collection and public response:

| | | |
|---|---|---|
| **Increased Government Data Collection** | Scenario 1: Most likely | Scenario 2: Next most likely |
| **Decreased Government Data Collection** | Unlikely | Less likely |
| | **Backlash** (strong public reaction) | **Acceptance** (minimal public reaction) |

The actions of many governments around the world suggest more not less collection of personal data as time goes on. Examples of Initiatives already in progress include: the implementation of new national ID cards, expansion of health information networks, and more intensive collection of air passengers' data. With this variable constant, a differing public reaction to these trends might alter the course of the privacy profession.

### *Scenario One: Backlash*

In this scenario, government agencies and related parties continue the initiatives noted above to advance information technologies toward the fulfillment of their missions. But they take it a step further. In order to achieve healthcare cost reductions for example, agencies use access to patient data to identify at-risk individuals whose health could be improved by an early medical intervention. To achieve energy conservation and greenhouse gas-reduction goals, agencies monitor households' consumption levels and intervene when households exceed allowable limits. A new round of terror strikes could heighten government monitoring of commercial transactions. Tax agencies use advanced computing power to greatly increase the ratio of audited tax returns, and political candidates use advanced databases to engage in microtargeting of individual voters. Taken as a whole, in this scenario the individual citizen perceives a dramatic loss in freedom and lives each day with a growing sense that he is under siege.

What if civil societies subjected to these types of advancements in government data collection marshaled a strong reaction? A couple of outcomes could affect the privacy profession. First, demand for greater accountability and restriction of agency data practices could result in a surge of demand for privacy professionals inside agencies as well as on oversight boards. According to Bundy Scanlan, "Any tightening of homeland security measures that involve more intrusive use of personal data could lead to more calls for government privacy protections."

Second, citizens could seek to take matters into their own hands and shield their data from the government. Their fears could increase demand for privacy enhancing technologies.

### *Scenario Two: Acceptance*

In this scenario, government agencies continue the initiatives noted above, but do not pursue the individual targeting and monitoring outlined in Scenario 1. They collect more data, but do so in a way that is moderated by transparency and privacy best practices.

A greater likelihood is for citizens in this scenario to accept the benefits of their governments more efficiently accomplishing their missions, as weighed against only an incremental change in the quantity and types of their data that would need to be disclosed. With only a minimal public reaction to these changes, privacy compliance becomes a routine part of government administration, and government data collection fades as a driver of change for the profession.

# The Agile Privacy Professional: A Call to Action

If regulation, information technology, and government data collection continue to shape the profession, how can today's privacy professional take full advantage of the emerging opportunities? According to the experts, more agility is a must. The agile privacy professional, amid a period of ongoing transformation, will be able to clearly identify new opportunities, move to these, and manage them responsibly.

What defines the agile privacy professional? And what can today's privacy professional start doing now in order to successfully achieve agility in the future? The IAPP sees five strategies for action: (1) Redefine the privacy role; (2) Rotate through departments/business units; (3) Develop multi-cultural literacy; (4) Understand legal and technical disciplines; and, (5) Instill direction and leadership. Any one, if not all, of these strategies will enable today's privacy professional with greater agility in confronting the privacy challenges of the next 10 years.

## *Redefine the Privacy Role*

As organizations struggle to determine where to place privacy in the organization and with what responsibility to endow it, opportunities will emerge for agile professionals to provide answers. Experts interviewed for this research believe that the role of the privacy professional will grow beyond regulatory compliance into the information risk arena and, finally, into information governance and information optimization. In this scenario, the privacy discipline becomes a subset of the broader practice of minimizing the cost of information and maximizing its value. Above the chief privacy officer, chief information security officer, and records-management director will be an information optimization officer. Agile privacy professionals will socialize these concepts and seek sponsors and advocates.

"The percent of usable information among all of the noise that we're collecting is going down," says Michelle Dennedy. "Tomorrow's privacy professional will need to help articulate the value of information and then what would be a reasonable cost to protect it."

"I think privacy becomes information governance," echoes Bundy Scanlan.

Many feel that privacy programs and enforcements will evolve to focus more on data usage versus data protection. Jim Koenig of PricewaterhouseCoopers sees integrated frameworks emerging versus the more siloed, law-by-law regulatory approaches often seen today. The health information industry offers an example. "Healthcare companies, given the change in information uses and investments from ARRA/HITECH (the American Recovery and Reinvestment Act of 2009 and the HITECH Act of 2009), will help to set best practices versus financial institutions and retailers who are historically known for this," says Koenig.

Commissioner Ann Cavoukian, believes that there is a real opportunity for privacy professionals to adopt a new role of "privacy ambassador", within their organization. "… privacy professionals can advance the goal of proactively embedding privacy into their organizations' programs. And if privacy is proactively designed into technology, business practices, and infrastructure right from the outset, then the maximum degree of privacy protection can be ensured."

## Rotate Through Departments/Business Units

Today's privacy professional is adept at meeting compliance requirements and crafting policy, but the agile privacy professional of the next decade will rotate through business units and field operations where higher level decisions about information management are being made and implemented. Privacy professionals who embed themselves where value is created in an organization will expand their network and influence the role their organizations play in building trust in the global information ecosystem and with stakeholders. Those who don't will risk being among the last to know about critical changes to business strategy and information uses.

"Business experience is probably the most important success factor for tomorrow's privacy professional," says Sandy Hughes. "You can always learn the privacy requirements afterward. The best way to obtain this business experience as a privacy professional is to conduct an inventory of where and when and how personal data is collected and used." "It's important to signal your willingness to take on broadening experiences," adds Harriet Pearson. "The fact that I've had assignments in legal, human resources and public affairs has enhanced the perspective that I bring to my responsibilities."

"Anti money laundering and healthcare expertise" will be increasingly valuable skill sets for privacy professionals to obtain, adds Bundy Scanlan.

## Develop Multicultural Literacy

As privacy regulations take root in a greater number of jurisdictions around the world and as the value chains of organizations further internationalize, privacy professionals—particularly those based in the more culturally homogenous North America—may face a crossroads. The privacy professional of today may be inclined to completely delegate questions of local concern to local subject-matter experts and local privacy champions. Western leadership training often teaches the value of delegation, after all. But an agile privacy professional will see opportunity in understanding how variances in culture create variances in information risk and optimization. After acquiring this understanding, the agile professional will be able to communicate strategy, policies, and solutions across cultural boundaries.

"I see four success factors for tomorrow's privacy professionals," notes Nuala O'Connor Kelly. "One, making the case for privacy in positive, measurable terms. Two, obtaining cross-functional talent beyond privacy. Three, obtaining enough knowledge about technology and data systems to ask probing questions. Four, gaining international experience and cross-cultural literacy. This will only grow over time."

"You may not need to speak the local language, particularly if you collaborate with colleagues in local markets whom you may help train to be knowledgeable in and accountable for privacy and security issues as part of their jobs," says Merck's Dean Forbes. "But you will need to listen, work to understand the cultures of these colleagues, assess reasonably foreseeable risks, and prioritize and provide direction accordingly to cross-functional global and local teams to address such risks in relevant areas of their business operations."

## Understand Legal and Technical Disciplines

While there is little debate as to whether privacy professionals ought to have a basic grasp of legal and technical concepts around data privacy and security, experts' opinions diverged on whether tomorrow's privacy professional would by necessity need a legal or technical degree. The central role of regulatory and IT drivers shaping the privacy profession almost ensures an ongoing need for privacy professionals to be conversant in not one, but both of these disciplines. Some may indeed become mid-career attorneys or mid-career masters of information systems. The most agile privacy professionals may also recognize the need to pursue literacy in finance and economics in order to quantify the value of information.

"One of the interesting things about the privacy profession is how many disciplines can provide useful background," says Zoe Strickland. "Legal or IT experience is common. Other desirable backgrounds, depending on the goals of the organization, are marketing, customer service, compliance, and communications." "Knowing more is always better than knowing less," says Kirk Herath. "Privacy is inherently legal and, in my humble opinion, a law degree is extremely helpful in this space, as is at least a good understanding of technology."

"We need two types of privacy professionals," proposes Michelle Dennedy. "One, the great lawyer who is a tactical, focused specialist. Two, the broad-thinking, stragetic person who integrates technology, law, marketing, and sociology."

Bojana Bellamy counters, "I believe the real privacy professional does both. I think this is somebody with a legal degree or background who has transcended a pure legal-advisory role and has become a trusted business advisor, as well as a complaints ombudsman, technologist, strategist, and government-relations person, a diplomat."

## Instill Direction and Leadership

Many things change, but some remain the same. Amidst continuing change, organizations will need charismatic strategists who can lead, persuade, persevere and provide stability. And with a forecast of ongoing regulation, the effective privacy leader will be a public speaker who works a vast personal network of legislators, industry groups, and standards bodies to articulate a vision and position.

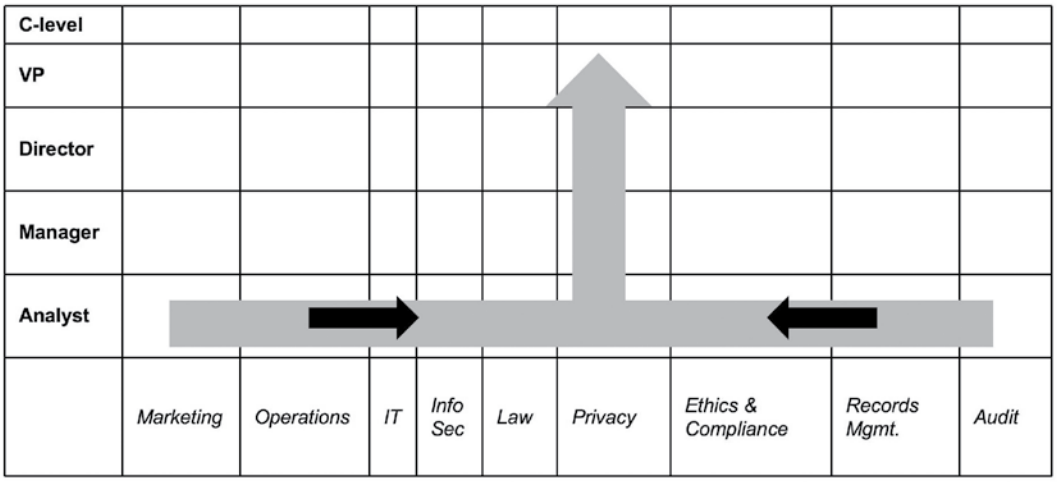
"Strong leadership abilities will be the biggest success factor for privacy professionals in the future," notes RBC's Jeff Green. "To be successful, they must be able to influence across all lines of business and the operational and functional areas that support them to drive a consistent approach to information governance."

# Agile Privacy Career Paths

Career development tracks for the agile privacy professional will likely follow one of several discrete paths. As privacy questions bleed into new parts of organizations, sectors, and geographies, the privacy professional of the next 10 years might well see themselves choosing one the following options.

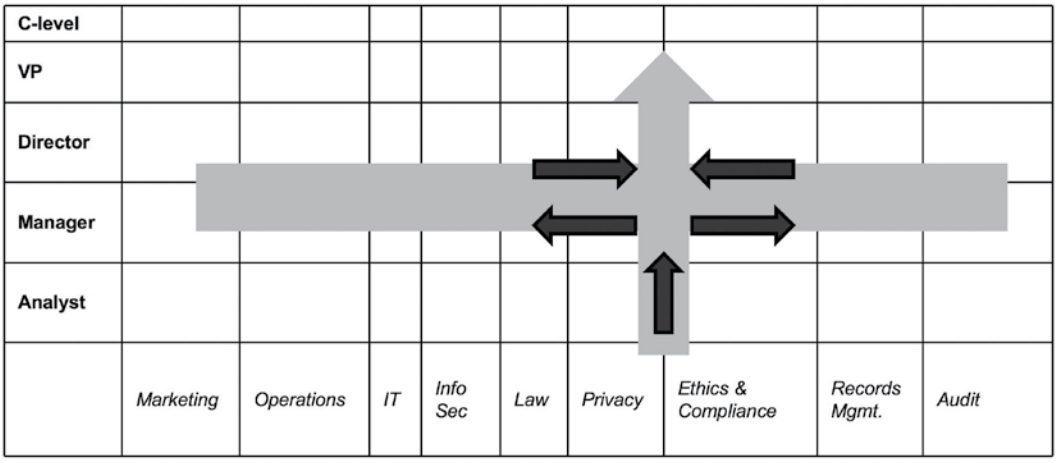
## *Path 1: Start anywhere, and rise through privacy*

In this scenario, the privacy professional follows a traditional ascent up through a privacy program. Getting a start anywhere in an organization, this person gravitates toward the privacy department and becomes a master in the privacy discipline. Depending upon the sector, size, and geographic reach of the organization, an entire career could be spent building and maturing a privacy program.




## *Path 2: Create rotational experiences that remain centered on privacy*

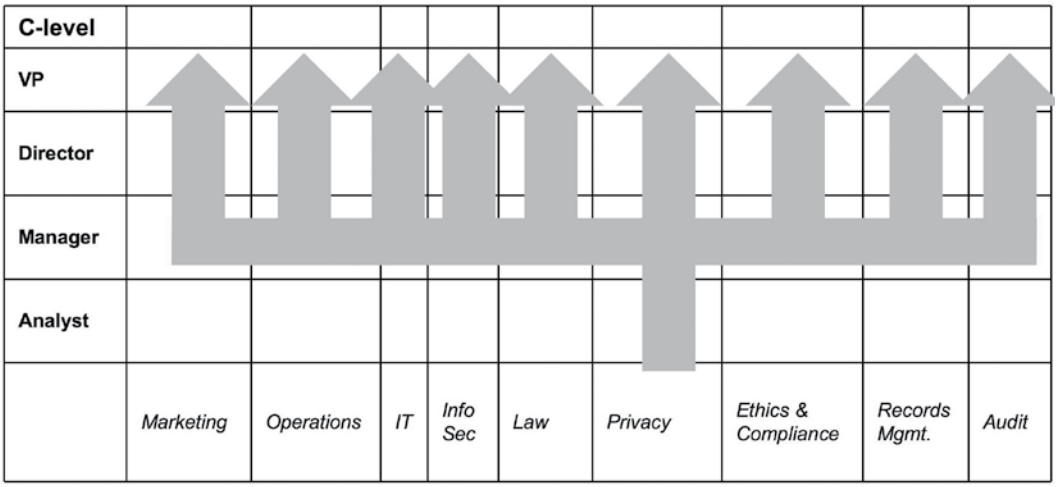
In this scenario, a privacy professional seeks one or more opportunities to spend time in other departments or business units before coming back to the privacy program. In larger privacy programs where there is competition for the top privacy job, these types of rotational experiences may prove to be the differentiators in demonstrating greater leadership potential.



"Data-intensive businesses may need a more complex privacy organization with career paths," says Brian O'Connor. "Other businesses that only collect routine personal data for basic marketing and finance functions will gravitate toward smaller privacy functions, often integrated into the IT or Legal organizations."

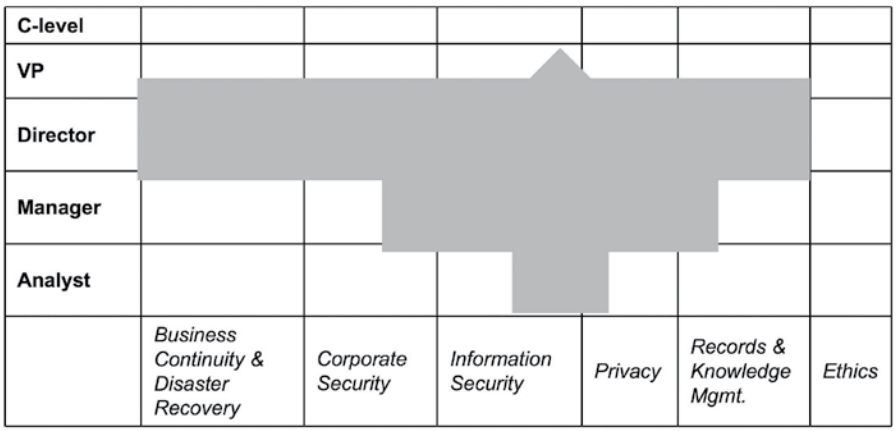
## *Path 3: Start in privacy, move to anywhere*

On this path, a privacy professional is sought after by other organizational functions that need to embed privacy into their DNA. Rather than being rotational experiences, this time outside the privacy program becomes a launching pad for an entirely new career where privacy becomes a differentiator for excelling in the new discipline.




## *Path 4: Grow the privacy function*

There has been much discussion in privacy circles about a convergence of information-related functions into an information-governance department. While some organizations will have a regulatory or other need to maintain a separation between the CPO and CISO functions in particular, other privacy professionals may have an opportunity to redefine their roles over time to more broadly encompass information risk and policy.



"I think we'll see more companies converging privacy, information security, and records management under a common framework of policies and procedures," comments RBC's Jeff Green.

"As organizations seek to manage the risk associated with managing data," said IBM's Harriet Pearson, "the worlds of the traditional IT security professional and the privacy professional will converge even more than we have already seen."

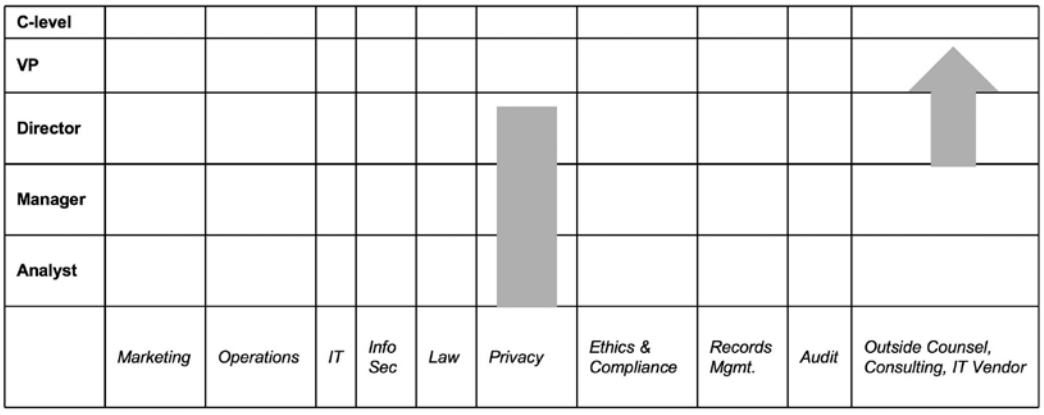
Walmart's Zoe Strickland offers a somewhat contrarian viewpoint in this regard: "I think we may actually see more divergence between the security and privacy functions. Many issues coming to the fore involve technology and uses of data that are separate from security. Security departments will likely stick to their core functions as those risks are not abating."

"The privacy professional needs a seat at the executive table," says Michelle Dennedy, "but security is going in the opposite direction, becoming more tactical."

"The unknown for me," says Brian O'Connor, "is whether surveillance technologies continue to develop and become so prevalent that companies will need to continue or expand the role of 'privacy advocate' separate from IT, Legal, and Compliance functions."

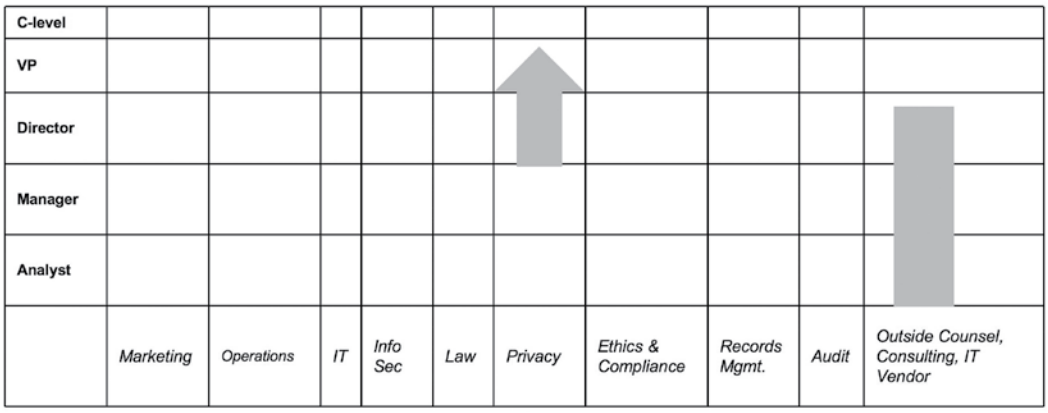
## *Path 5: Working inside out*

Some privacy professionals may seek to parlay the practical and unparalleled experience of working as a corporate privacy leader into an external path serving multiple organizations in a consulting capacity. Typically, this kind of an opportunity would not emerge until the privacy professional has reached a senior or leadership level that provides a sufficient basis of experience for imparting advice in many different scenarios.



## *Path 6: Working outside in*

Conversely, outside privacy practitioners may ultimately seek the relative predictability of a corporate executive job. With the diverse experience that an external position offers, the privacy consultant may be able to enter a corporate privacy path at a relatively high level.




The outside-in career path may become more prevalent if the CPO position becomes regulated or stipulated by more data protection laws. Bellamy notes that France, Germany, Netherlands, Sweden, Japan, and some U.S. agencies currently follow this approach. If more of these positions are created, new opportunities may open up for people inside and outside of the privacy profession who can garner the trust of regulators.

Adding the dimension of foreign assignments to any of these career paths—as is likely to be increasingly the case in the next decade—the career opportunities for driven privacy professionals will multiply.

## About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals, representing more than 6,500 members from businesses, governments and academic institutions across 50 countries.

The IAPP was founded in 2000 with a mission to define, promote and improve the privacy profession globally. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for many thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds the annual Privacy Summit, Privacy Academy and Practical Privacy Series conferences. These events are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.



## About the Author

Jay Cline, President of Minnesota Privacy Consultants, is a former chief privacy officer of Carlson Companies, IT management consultant at EDS, and international trade-law expert in the U.S. Government. Cline, a Certified Information Privacy Professional (CIPP), has held leadership positions in the International Association of Privacy Professionals, and is a privacy columnist for Computerworld and INSIDE 1to1: Privacy.

## About the Artist

The image on the cover of this whitepaper was commissioned by the IAPP to celebrate the tenth anniversary of the organization. Artist David Plunkert worked in a collage-style with an image that evokes the modern privacy professional. From within an organization a privacy professional reaches outward to bring order to disparate worlds of data. The connection to a global economy, technology, the Internet and the central role of privacy are all themes presented in the piece.

Plunkert is an award winning illustrator and graphic designer based in Baltimore, MD. A prolific artist, his work has appeared on the pages of *Esquire, Forbes, GQ, The New Yorker, Time, Reader's Digest* and *Rolling Stone* magazines, as well as in the *New York Times* and the *Wall Street Journal*. Plunkert has also worked extensively with publishers and recording artists. Among his credits are the covers for Natan Sharansky's "Case for Democracy" and Richard Thompson's "You? me? us?"

International Association of Privacy Professionals


170 Cider Hill Road | York, Maine 03909 USA | +1 207.351.1500 | www.privacyassociation.org

International Pharmaceutical
PRIVACY CONSORTIUM

1500 K Street NW • Suite 1100 • Washington DC 20005 USA
Telephone 202 230 5142 • Facsimile 202 842 8465 • Website www.pharmaprivacy.org

June 14, 2010

Mr. Gary Locke
Secretary
Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

**Re: Federal Register Notice of Inquiry Vol. 75, No. 78**

Dear Mr. Locke:

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies. The IPPC is committed to the promotion of sound policies for the protection of patient privacy and advancement of drug development and treatment. Information concerning IPPC membership and mission is described in Appendix A.[1]

We appreciate this opportunity to present our views on the impact of the current privacy framework on Internet commerce and innovation. More specifically, we intend to address how the current privacy framework, and changes thereto, would affect innovations in the health care sector and more generally public health.

In the next three sections we illustrate IPPC principles and activities that are intended to help provide important privacy and security protections in the context of our interactions with health care consumers. We consider these to be best practices that protect consumer privacy without restraining medical innovation. Implicit in these principles is our support for a use-based model for data privacy protection.[2] The IPPC believes that the way data is to be used should determine data privacy obligations. In the context of the pharmaceutical industry, this calls for a distinction to be made between uses of personal data for purposes of biomedical research and public health activities versus those for sales and marketing. The data protection principles we believe should apply in each of these contexts is outlined below.

## I. Research

A clear delineation must be made around the standards that apply to the collection and use of personal health information for marketing versus the collection and use of personal health information for scientific research and public health activities. Personal health data is essential for, *inter alia*, conducting research involving genetics and biomarkers,[3] seeking genetic patterns in the safety and effectiveness of drug therapies, determining the safety and effectiveness of new treatments, and locating appropriate

[1] For further information concerning the IPPC, please visit our website at www.pharmaprivacy.org. All Appendices referenced in this comment, and additional documents adopted by the IPPC, are publicly available on this website.
[2] The Business Forum for Consumer Privacy, "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," Dec. 7, 2009, available at http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf.
[3] A biomarker is a characteristic that is objectively measured and evaluated as an indicator of normal biologic processes, pathogenic processes, or pharmacologic responses to a therapeutic intervention.

participants for clinical research studies. Despite the clear importance of the ethical principles of respect for persons and autonomy, which serve as the basis for informed consent requirements, these principles are not absolutes and must be balanced with other ethical principles, such as beneficence. Beneficence requires that members of society recognize the longer term benefits and risks that may result from the improvement of knowledge and from the development of novel treatments.

Informed consent was originally conceived as a protection against physical harm to patients, permitting informed, competent patients to refuse unwanted medical interventions and to ensure patients were informed of the physical risks involved in medical research. However, informed consent has come to be used as protection against a broad range of nonphysical harms, such as breaches of privacy and confidentiality. The reliance on notice and choice as the basis for permitting analysis of patient information for pharmacoepidemiological research[4] or using biospecimen samples for biomarker and genomics research is becoming increasingly unworkable. Several alternative ethical frameworks to notice and choice have been proposed for balancing patient privacy interests and researchers' data needs. These include:

(i) Research subjects treated as donors (Subjects as Donors Model). In this Model, the law of property with respect to inter vivos gifts is applied to informational privacy. In essence, the idea is simply that where there is (1) present intent of a human subject to donate his biological materials or health information, (2) delivery of the sample or information in question by the subject to the researcher, and (3) acceptance of the gift by the researcher, the researcher becomes the 'owner' of the samples or information immediately and absolutely.[5]

(ii) Reciprocity as a guiding principle (Reciprocity Model). The reciprocity model seeks to address the situation where there is no consent for future research uses (whether specified or unspecified). Its proponents argue that by accepting the benefit of past medical research (which is inherent in the use of medical services), a patient agrees to allow the use of health information about him or her in future research for the common good.[6]

(iii) Informational restrictions narrowly tailored to address the specific risks associated with unauthorized use of that information (Harms-Based Model). Potential harms associated with the unauthorized use of personal health information include discrimination and stigmatization; and an erosion of the doctor-patient relationship, leading to compromises in health care. To address these risks, a harms-based model might call for the adoption of non-discrimination legislation and a requirement that entities with a legitimate need for health information secure the information against unauthorized access.

(iv) Adaptation of the fair information practice principles to accommodate the practical realties of scientific research by emphasizing research transparency over individual notice, choice, and access. Transparency could be achieved by permitting researchers to obtain one-time general consent for biobanking or genomics research, through the global publication of research results, and/or through the reporting of validated research results to data subjects who request such information.

---

[4] Pharmacoepidemiology is the study of the use and effects of drugs in populations.
[5] *cf. Wash. U. v. Catalona* (8th Cir. 2007).
[6] *See* Edison T. Liu, *The Importance of Research Using Personal Information for Scientific Discovery and the Reduction of Disease,* in Personal Information for Biomedical Research (Singapore Bioethics Advisory Committee, May 2007) at Annex A. *See also* B.M. Knoppers and R. Chadwick, *Human Genetic Research: Emerging Trends in Ethics*, 6 Nature Rev. Genetics (Jan.) at 75-79.

## II. Internet Commerce and Marketing

The IPPC supports the ability of consumers to play an active role in their healthcare by researching health conditions and treatments online, signing up to receive information and to take part in patient discussion groups, and tracking their health status using online tools. The benefits of such patient empowerment are described in the attached 2004 IPPC white paper *Dissemination of Prescription Drug Information Enhances Patient Healthcare* (see Appendix B). The IPPC has also developed in 2008 the attached *Privacy Guidelines for Marketing to U.S. Consumers* (see Appendix C) which we believe strike the appropriate balance between enabling the free-flow of information between consumers and health product manufacturers and preventing unwanted marketing uses and disclosures of personal information.

The IPPC believes that consumers should be provided with the choice to decide whether or not their personal health information will be used or disclosed for marketing purposes. Nevertheless, we are aware of anecdotal reports of consumer health information being used and/or disclosed for unexpected marketing purposes. This raises the dual questions of (i) whether notice and choice was ever provided; and (ii) if it was provided, whether it was done so in a clear and conspicuous manner such that the consumer was provided with meaningful choice. The IPPC suggests the following guidelines to help ensure that notice and choice is meaningfully provided:

- Layered privacy notices or other methods for highlighting marketing uses of health information should be considered.
- Express permission should be obtained before health information is used for marketing purposes for which notice and choice have not already been provided to the patient/consumer.
- If a third party provides remuneration in exchange for marketing communications to be made about that third party's products or services, each marketing communication should include an indication of this fact in addition to other notices of this fact that may have been previously provided.
- Patients/consumers should be provided with the ability to opt-out of receiving further marketing communications.
- Express permission should be obtained before personal health information is disclosed to an unrelated third party, including for that third party's marketing purposes.

The IPPC discourages the imposition of overly prescriptive requirements for what must be included in a consumer consent or the form of such consent. Many pharmaceutical company interactions with consumers occur by phone in response to inquiries and requests for information. We do not believe that consumers should be restricted from receiving information they request in settings where written permissions are not practical. Moreover, consumers should have the right to decide for themselves the scope of marketing permission they wish to grant, including whether to provide consent solely for a specific product or a range of products for a particular disease state.

In addition to providing consumers with the ability to opt-out of receiving further marketing communications, the IPPC supports providing consumers with the ability to find out how their personal health information was obtained by a pharmaceutical company. It should be understood, however, that it may not be possible for a company to pinpoint the source of a particular element of information as information may be aggregated from multiple sources.

The members of the IPPC follow reasonable procedures to ensure that personal information that is obtained from third parties is being provided to companies with the consumer's consent. However, aside from contractual requirements that the third party data provider obtained consent for the data sharing, there may be little a pharmaceutical company can do to verify what has been represented. Where representations have been made about the source of a consumer list and permissions associated

with that list, accountability for unauthorized uses and/or disclosures of the information should rest with the party making such representations, should they later prove false or misleading.

## III. Commitment to Privacy in U.S. Consumer Marketing: Myths and Facts

The IPPC is aware that there may be certain misperceptions about how pharmaceutical companies collect and use personal health information, and we have therefore developed the attached document entitled *Commitment to Privacy in U.S. Consumer Marketing: Here Are the Facts* (see Appendix D, adopted in 2008) to help correct these misunderstandings. This document is intended to make clear the following points:

- Pharmaceutical companies do not purchase identifiable patient health data (i.e., information relating to the medical conditions or treatments of named or otherwise identifiable patients) from pharmacies and health plans in order to market their products and services. As further described in the document, pharmaceutical companies may obtain anonymized, aggregated health data for scientific research purposes in order to design programs to improve patient health outcomes.

- Pharmaceutical companies do not have access to written and electronic health records in order to send consumers targeted marketing communications without their permission. As further described in the document, pharmaceutical companies may sponsor compliance and other treatment-related programs offered through pharmacies and health plans.

- Records from clinical research studies sponsored by pharmaceutical companies are not reused for marketing purposes.

- Spam email is not sent to consumers by pharmaceutical companies for the purpose of advertising prescription drugs.

## IV. Conclusion

The IPPC believes that the Department of Commerce could play an important role in coordinating data privacy initiatives that are underway within the Federal Trade Commission, the Department of Health and Human Services, and other branches and agencies of the federal government. We would welcome the opportunity to continue to engage in a public dialogue on the appropriate ethical principles that should govern the collection and use of health information for biomedical research and public health activities versus for sales and marketing.

We thank you for your consideration of our comments and would welcome the opportunity to discuss these issues with you. Please do not hesitate to contact us with any questions.

Sincerely,

International Pharmaceutical Privacy Consortium

# APPENDIX A: INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

## MEMBERS

The IPPC is an association of companies that face worldwide responsibility for the protection of personal health information and other types of personal data. Members of the IPPC include:

- Abbott Laboratories
- AstraZeneca
- Baxter International
- Bristol-Myers Squibb
- Elan Pharmaceuticals, Inc.
- Eli Lilly and Company
- GlaxoSmithKline
- Merck & Co., Inc.
- Novartis
- Pfizer Inc.
- Genentech (Roche)
- Sanofi-aventis
- Takeda Pharmaceuticals

## MISSION

The IPPC was formed in 2002 to promote responsible privacy and data protection practices by the research-based, global pharmaceutical industry. Maintaining data confidentiality and subject privacy are essential to clinical research, pharmacovigilance, and other activities of the pharmaceutical industry. The IPPC seeks to increase awareness of privacy and data protection issues and to engage government in a dialogue about the need for data to support cutting edge biomedical research and other public health activities. The IPPC pursues opportunities to collaborate with government and other stakeholders to develop data protection practices that enhance data subject privacy.

## GOALS

The IPPC goals are to:

- Engage government and stakeholders in the biomedical research and healthcare communities in a constructive dialogue on significant issues of privacy and data protection.
- Serve as a resource for sound analyses of privacy and data protection requirements and compliance tools tailored to the pharmaceutical industry.
- Serve as a forum for industry dialogue and promote responsible privacy and data protection practices.
- Promote consistent privacy and data protection standards that can be achieved on a worldwide basis.
- Remain on the leading edge of privacy and data protection.

## SCOPE OF ACTIVITIES

The IPPC advances understanding of existing and emerging data protection and security rules in Europe, the US, and other key countries. The Consortium engages regulators and policymakers in the following areas:

- Biomedical research
- Pharmacovigilance
- Sales and marketing
- Market research
- Human resources programs
- Other corporate programs

# APPENDIX B: DISSEMINATION OF PRESCRIPTION DRUG INFORMATION ENHANCES PATIENT HEALTHCARE

## I. Consumer-Directed Information

Healthcare outcomes are improved when patients are engaged in their treatment program. Informed consumers are more likely to recognize disease symptoms and to seek appropriate care. In turn, informed patients are more likely to adhere to physician-prescribed treatment regimens. Appropriate, proactive, and consistent use of prescription medications helps individuals to lead healthier lives, and can prevent or delay the need for more costly medical services and procedures. Pharmaceutical companies play an important role in our healthcare system not only by manufacturing prescription drugs and devices, but also by serving as an informational resource for interested patients and physicians.

### A. Background

The most important healthcare relationship is between patient and physician. While this relationship is vital to each patient's medical care, patients also obtain valuable health-related information from other sources. The wide availability of health information on the Internet and through other sources has empowered individuals to learn more about health conditions and treatments.[i]

While the majority of prescription drug promotional and educational activities is directed toward physicians[ii], pharmaceutical companies also provide a range of information to consumers. Consumer-directed information about medical conditions and new and existing prescription drugs and devices is provided in many different forms and media. On company web sites, consumers can access information, sign-up to receive newsletters, or request brochures and other product-related materials. Many companies operate call-centers, enabling patients to request materials over the phone. Pharmaceutical companies provide materials to physician offices, hospitals, clinics, and other medical centers for distribution to patients. Companies sponsor pharmacy programs designed to promote patient adherence to physician-prescribed treatments. Companies also work with health care providers and health plans to promote disease management.

Information provided by pharmaceutical companies on prescription drugs, unlike much other healthcare information (*e.g.*, medical information on the Internet, information on alternative medicines), is subject to intense regulatory scrutiny by the Food and Drug Administration (FDA). FDA protects public health by helping to ensure that pharmaceutical manufacturers provide truthful, balanced, and accurate health-related information to consumers and patients.[iii] In recent draft guidance on drug product advertisements, FDA noted that available data and information, including results of FDA's own research, have led the Agency to believe that consumer-directed promotion of prescription drugs can convey useful health information to patients.[iv]

### B. Benefits of Consumer-Directed Information

- ***Empowers Patients with Information***. Consumers who recognize disease symptoms and understand treatment options can more effectively seek appropriate care and make better-informed health decisions.[v] Heightened awareness of available therapies and the benefits, risks and side effects of these therapies, empowers patients to work with their physicians to make important decisions about their healthcare.

- ***Encourages Patients to Communicate with Physicians***. Pharmaceutical company communications about prescription drugs encourage patients to consult with their physicians about health conditions to determine what treatment options are available. FDA consumer surveys in 1999 and 2002 demonstrate that consumer-directed prescription drug information encouraged substantial numbers of patients to ask a doctor about a previously untreated medical condition or illness.[vi] Moreover, 93% of patients prompted by pharmaceutical advertising to discuss a drug with their doctor report that their doctor welcomed the question.[vii]

- ***Decreases Patient Inhibitions in Addressing Sensitive Conditions***. Consumer-directed information about available prescription therapies encourages patients to speak with physicians about their medical symptoms and treatment options. Patients who suffer from medical problems that may carry a social stigma or historically have been viewed as too personal to discuss with a physician are now, as a result of greater information, education, and understanding, more likely to discuss with their physicians their symptoms and possible treatments.[viii]

- ***Promotes Improved Medication Compliance***. Medication non-compliance is a significant public health concern – it has a negative impact on patients' health and significantly raises healthcare costs. Data from FDA show that about one-third of patients fail to take their medications as prescribed. Parental non-compliance with drug therapies prescribed for their children exceeds 50%, and non-compliance among elderly patients ranges from 26% to 59%.[ix] Industry-sponsored communications, such as refill reminders and other consumer-directed information, facilitate medication compliance.[x] Direct-to-consumer prescription drug advertisements prompt patients to take their medicine regularly and refill prescriptions as necessary.[xi]

## II. Physician-Directed Information

By providing scientific and educational information about prescription products, pharmaceutical sales representatives enhance the ability of healthcare providers to care for patients. Sales representatives meet with physicians to provide product information, answer questions regarding the use of their products, and deliver product samples. Ongoing research and development into safer and more effective medicines means that treatment standards are constantly evolving. It is important that healthcare professionals have the latest, most accurate information available regarding prescription medicines.

Prescription medicines play an ever-increasing role in patient healthcare, and it is critical that healthcare providers receive the latest information on the benefits and risks of those medicines. Traditionally, on-site visits by sales representatives have enabled physicians to get needed information and product samples with minimal disruption to patient care. In turn, direct interactions with physicians have enabled manufacturers to receive important product feedback.

As the external pressures of managed care place increasing demands on providers' time and focus, pharmaceutical companies have responded by delivering targeted information based on the needs and preferences of individual practitioners. Historical data on filled prescriptions (deidentified as to individual patients) helps pharmaceutical companies to understand the range of health conditions served by individual providers. This knowledge in turn enables companies to determine which product information is likely to be of most use to those providers. The ability to tailor information to individual provider needs is important not only to informing physicians of product advances and advantages, but also to alerting prescribers to newly discovered drug interactions and adverse events.

The delivery of high-quality healthcare depends upon the successful collaboration of multiple players. Pharmaceutical companies serve an important role by providing patients and physicians with necessary information.

---

[i] The Internet and advertising provide patients with increased access to health care information. For example, 24% of online information relates to healthcare and more than 50% of adults who access the Internet use it for health-related information. (Lyn Siegel, "DTC Advertising: Bane or Blessing?" *Pharmaceutical Executive*, October 2000).

[ii] Rosenthal M, Berndt E, Donohue J, Frank R, Epstein, A., "Promotion of Prescription Drugs to Consumers," *New England Journal of Medicine*, Vol. 346, No. 7, February 14, 2002.

[iii] Statement of Dr. Janet Woodcock, Director, CDER, FDA, before the Senate Special Committee on Aging, July 22, 2003, Hearing on Direct-to-Consumer Advertising of Prescription Drugs: What Are the Consequences?

[iv] Draft Guidance for Industry, "Brief Summary: Disclosing Risk Information in Consumer-Directed Print Advertisements," p. 7, January, 2004, http://www.fda.gov/cber/gdlns/consumad.pdf.

---

[v] For instance, in industry guidance FDA has commented: "FDA believes that disease awareness communications can provide important health information to consumers and health care practitioners, and can encourage consumers to seek, and health care practitioners to provide appropriate treatment. This is particularly important for under-diagnosed, under treated health conditions, such as depression, hyperlipidemia, hypertension, osteoporosis, and diabetes." Draft Guidance for Industry, "Help-Seeking" and Other Disease Awareness Communications by or on Behalf of Drug and Device Firms, p.1, January, 2004, http://www.fda.gov/cber/gdlns/helpcomm.pdf.

[vi] Statement of Dr. Janet Woodcock, Director, CDER, FDA, before the Senate Special Committee on Aging, July 22, 2003, Hearing on Direct-to-Consumer Advertising of Prescription Drugs: What Are the Consequences?; See also Direct to Consumer Advertising of Prescription Drugs: Preliminary Patient Survey Results at http://www.fda.gov/cder/ddmac/DTCnational2002a/; See also 2000 Scott Levin survey reporting that 56% of physicians agree that direct-to-consumer advertising brings in patients to seek treatment that would otherwise go untreated.

[vii] Direct to Consumer Advertising of Prescription Drugs: Preliminary Patient Survey Results at www.fda.gov/cder/ddmac/DTCnational2002a/sld001.htm.

[viii] David M. Cutler and Mark McClellan, "Is Technological Change in Medicine Worth It?" Health Affairs, Vol.20, No. 5, September/October 2001, noting the significant treatment expansion for persons with clinical depression.

[ix] 60 *Fed. Reg.* 44,182, 44,286 (Aug. 24, 1995). See also Sullivan, S.D., *et al*., "Noncompliance with Medication Regimes and Subsequent Hospitalization: A Literature Analysis and Cost of Hospitalization Estimate," Journal of Research in Pharmaceutical Economics, 1991, stating that 5.5% of all hospital admissions are due to non-compliance, resulting in $8.5 billion annually in unnecessary hospital-related expenditures, plus another $17-$25 billion in estimated indirect costs; See also Berg, *et al*., *The Annals of Pharmacotherapy*, 27 (9): S3-S22 (1993), finding that patients who do not adhere to drug therapy cost the U.S. health care system an additional $100 billion each year.

[x] *See, e.g.,* JS Benner (Brigham and Women's Hospital / Harvard Medical School), DA Ganz (Brigham and Women's Hospital / Harvard Medical School), et al. "Is It Cost-Effective to Improve Compliance with Lipid-Lowering Therapy?" (concluding that compliance-enhancing interventions appear to be an attractive way to recover some of the clinical benefits that are lost due to noncompliance with statins and that the most cost-effective intervention was to provide patient education and refill reminders via the mail and telephone); Ross T. Tsuyuki, Jeffrey A. Johnson, et al., "A Randomized Trial of the Effect of Community Pharmacist Intervention on Cholesterol Risk Management," *Arch. Intern. Med.* 162: 1149-75, 2002 (concluding that pharmacist intervention improved cholesterol management in high-risk patients).

[xi] 5th annual Survey: Consumer Reaction to DTC Advertising of Prescription Medicines, Emmaus, PA, Rodale, 2001-2002, reporting that 17% of consumers stated that direct to consumer advertising made it more likely (versus 2% less likely) that they would take their medicine regularly and 12% stated that these ads made them more likely to refill prescriptions.

# APPENDIX C: PRIVACY GUIDELINES FOR MARKETING TO U.S. CONSUMERS

This document sets forth voluntary privacy guidelines for marketing by pharmaceutical companies to U.S. consumers. These guidelines are aspirational in nature. Companies endorsing this document aim to follow these guidelines in their day-to-day business operations in connection with the collection, use, disclosure, and maintenance of written and electronic personal information that identifies an individual consumer and is retained by a company for marketing purposes. These companies also take steps to ensure that vendors who may communicate with consumers on their behalf comply with these guidelines or applicable privacy and data protection laws.

Policies or practices for addressing these guidelines vary by company. For information on an individual company's privacy practices, please refer to the company links at the end of this document.

## I. NOTICE

1. When personal information is collected directly from consumers, inform those consumers about:

   (a) the identity of the entity collecting the information;

   (b) the purposes for which the information is being collected;

   (c) the types of third parties to whom the information may be disclosed; and

   (d) where provided, the means by which consumers can access and amend personal information about themselves.

2. Where the means by which personal information is being collected is not obvious (e.g., passive or automatic collection of information through website tracking), include a notice of this fact in a privacy statement.

3. When personal information about a consumer that will be used to market to that consumer is received from a third party, obtain assurances from that third party that notice was provided to the consumer and that appropriate permissions were obtained to share the personal information with the pharmaceutical company.

## II. PERMITTED USES AND DISCLOSURES

1. Limit uses of personal information collected or received to:

   (a) those that are compatible with the purposes indicated in the notice given. Maintain processes to enable consumers to withdraw permission (opt-out) at any time and process such requests within a reasonable timeframe;

   (b) those that have been subsequently authorized by the consumer;

   (c) those that are necessary to comply with a legal or ethical obligation;

   (d) those that are necessary to ensure compliance with applicable laws and to detect and prevent inappropriate acts or practices, or to investigate, make or defend a legal claim; and

   (e) those that have been requested by governmental authorities.

2. Limit disclosures of personal information collected or received to:

   (a) others working for or on behalf of the company;

   (b) others with whom the company jointly markets products or services;

   (c) those that are compatible with the notice given at the time the information was collected;

   (d) those that are incidental to permissible uses of the information;

   (e) third parties to whom the consumer has authorized disclosure;

   (f) in the event of a sale or transfer of the business, successors and assignees;

   (g) those that are necessary to investigate, make or defend a legal claim; and

   (h) those that have been requested by governmental authorities or compelled by legal process.

## III. ACCESS AND AMENDMENT

When contacted by a consumer who has provided appropriate verification of his or her identity with a specific request related to personal information, work reasonably with that individual to address his or her specific concern.

Circumstances that may prevent a company from fully complying with an individual's request include those that would:

- affect the company's ability to comply with a legal or ethical obligation;
- affect the company's ability to detect and prevent inappropriate acts or practices, or to investigate, make or defend a legal claim;
- result in the disclosure of proprietary information; or
- result in the disclosure of personal information of other individuals.

## IV. SECURITY

1. Take reasonable precautions to protect personal information from loss and misuse, as well as unauthorized access, disclosure, alteration and destruction, commensurate with the sensitivity of the information processed.

2. Obtain assurances from vendors that they will protect personal information from loss and misuse, as well as unauthorized access, disclosure, alteration and destruction, commensurate with the sensitivity of the information processed, and that they will promptly notify the company of security incidents involving personal information.

3. Promptly investigate security incidents involving personal information and provide appropriate notice in accordance with applicable law.

## V. ENFORCEMENT

1. Employ appropriate measures to receive and, as appropriate, respond to privacy complaints and requests.

2. Adopt appropriate measures and take corrective actions against employees who are found to have violated company privacy policies. Take appropriate corrective actions against agents who have violated privacy policies or law.

## Endorsing Companies *(as of March 7, 2008)*

| | |
|---|---|
| Abbott Laboratories | Website Privacy Policy: http://www.abbott.com/global/url/content/en_US/0:0/general_content/General_Content_00029.htm |
| AstraZeneca Pharmaceuticals | Privacy Statement: http://www.azprivacystatement.com |
| Bristol-Myers Squibb | Internet Privacy Statement: http://www.bms.com/legal/data/privacy.html |
| Eli Lilly and Co. | Website Privacy Statement: http://www.lilly.com/privacy.html |
| Johnson & Johnson | Website Privacy Policy: http://www.jnj.com/privacy_policy/index.htm |
| Merck and Co., Inc. | Internet Privacy Policy and Privacy Notice for U.S. Patients, Consumers and Caregivers: http://www.merck.com/policy/commitment/home.html |
| Pfizer | Privacy Policy: http://www.pfizer.com/general/privacy_policy.jsp |
| Roche | Online Privacy Statement: http://www.rocheusa.com/privacylegal/privacy.asp |
| sanofi-aventis | Online Privacy Policy: http://legalnotice.sanofi-aventis.us/ |
| Schering-Plough Corp. | Online Privacy Notice: http://www.spfiles.com/policy/IWW0341.jsp?site=www.schering-plough.com&wm=privacyoffice@spcorp.com |
| Takeda Pharmaceuticals | Website Privacy Policy: http://www.tpna.com/privacy.asp |

International Pharmaceutical PRIVACY CONSORTIUM

March 2008

# APPENDIX D: COMMITMENT TO PRIVACY IN U.S. CONSUMER MARKETING: *HERE ARE THE FACTS*

The International Pharmaceutical Privacy Consortium is comprised of research-based pharmaceutical companies that are actively addressing privacy issues. Our ability to access and use personal information is critical to the work we do in researching and developing medicines and communicating with our customers. We have developed this document to better inform the U.S. public of our practices for respecting and protecting personal information in consumer marketing.

| | |
|---|---|
| ***Myth 1:*** | *Pharmaceutical companies purchase identifiable patient health data (i.e., information relating to the medical conditions or treatments of named or otherwise identifiable patients) from pharmacies and health plans in order to market their products and services.* |

**Fact:**

**Pharmaceutical companies DO NOT purchase identifiable patient health data from pharmacies or health plans. In fact, most pharmacies and health plans are prohibited by law from disclosing identifiable patient health information to any third parties for marketing without the explicit permission of the patient.**

***Anonymized, Aggregated Data***

**Pharmaceutical companies do purchase anonymized, aggregated health data for research purposes. Anonymized, aggregated data do not contain patient identifiers such as name, address, or other contact information; such data may include age, dates and geographic information. Anonymized, aggregated data are used, for example, to study the incidence, distribution and control of disease and to enable the development of programs that are designed to improve patient health outcomes.**

***Compliance and Adherence Programs***

**In addition, pharmaceutical companies may sponsor compliance and other treatment-related programs offered through pharmacies and health plans. For example, some pharmacies send refill reminders to customers when their prescription is due for refilling, and the program may be sponsored by a pharmaceutical company. The sponsoring company IS NOT provided with access to the customer records or any other identifying information about the customers to whom the refill reminders are sent unless the customer provides explicit permission. The sponsoring company often requires the program provider (i.e., the pharmacy or health plan) to provide its customers with the ability to decline these refill reminders (in some states, this is required by law).**

***Patient Assistance Programs***

**Pharmaceutical companies may receive identifiable patient health information from health plans to verify a person's eligibility for patient assistance programs or prescription discount programs. The information is usually transferred with the patient's explicit consent, and identifiable patient health information received under these circumstances is used solely for such programs.**

| | |
|---|---|
| ***Myth 2:*** | *Pharmaceutical companies have access to written and electronic health records in order to send consumers targeted marketing communications without their permission.* |

**Fact:**

**No, pharmaceutical companies do not have access to written and electronic health records in order to send consumers targeted marketing communications without their permission. Pharmaceutical companies send direct-to-consumer (DTC) marketing communications and offerings to individuals who have signed up and given their permission to receive such materials. DTC marketing and related programs are always *permission-based* (in certain states, this is required by law) and consumers usually have the ability to withdraw permission at any time. Consumers may provide permission via company web sites and call centers, business reply cards, or other avenues. In some cases, permission is obtained by a third party who then, in turn, provides the consumer's contact information to the pharmaceutical company.**

**Pharmaceutical companies do have an interest in obtaining anonymized, aggregated health data for scientific research purposes in order to design programs to improve patient health outcomes. For example, anonymized, aggregated data are a valuable source of information for studying the incidence and spread of disease or analyzing and comparing the cost-effectiveness of different drug therapies and the cost of hospitalization.**

| | |
|---|---|
| ***Myth 3:*** | *Records from clinical research studies sponsored by pharmaceutical companies are reused for marketing purposes.* |

**Fact:**

**No, such records are not reused for marketing purposes. In the course of a clinical study, medical records are generated or received by the physician or other medical professional under whose direction an investigational drug is given. This person is called an "investigator." Investigators maintain the medical records of study participants and report the study-related data back to the sponsor of the study. As sponsors of clinical studies, pharmaceutical companies receive data which has had the identities of participants replaced with unique codes, the keys to which are held by the investigators. Pharmaceutical companies do not receive those keys and do not receive the names or other contact information of study participants, except in very limited circumstances as described below.**

**First, a sponsor may be given the contact information of a study participant who has experienced an adverse event if further information is necessary for analysis of possible safety issues. Such contacts are a standard component of pharmacovigilance, the science of activities relating to the detection, assessment, understanding and prevention of adverse effects or any other drug-related problem. Employees of the sponsor who are responsible for conducting pharmacovigilance activities are bound by obligations of confidentiality covered by the company's employment contracts, policies or standard operating procedures.**

**Second, sponsors are given access to the medical records held by investigators to verify that the scientific data reported to the sponsor matches what is recorded in the investigator's copy of the records. Sponsor personnel involved in conducting such on-site quality inspections are required to maintain the confidentiality of patient identities and may not share this information for unrelated purposes.**

**Prior to enrolling a patient in a clinical study, investigators are required to explain what data will be collected, how it will be used, and to whom and for what purposes it will be disclosed. The patient's consent is documented in a written authorization.**

| | |
|---|---|
| ***Myth 4:*** | *Spam email is sent to consumers by pharmaceutical companies for the purpose of advertising prescription drugs.* |

**Fact:** **No, pharmaceutical companies do not send spam email. Pharmaceutical companies have no interest in sending customers unwanted email messages. In contrast, drug counterfeiters and illegal distributors often send spam email, in violation of federal law (*i.e.,* the CAN-SPAM Act). Some pharmaceutical companies might send unsolicited emails to consumers who have agreed to receive other emails from the company, but only in limited and unusual circumstances, such as to provide recall or safety information, and the communications would be expected to be in compliance with applicable laws.**

June 25, 2010

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 2023

Dear Colleagues:

I'm writing in response to the Notice of Inquiry re Information Privacy and Innovation in the Internet Economy. In particular, I'm writing to recommend that the Department of Commerce consider advocating for stricter laws governing the use of personal information combined with the provision of a Safe Harbor program. This is a regulatory strategy under which a federal statute explicitly recognizes differences in industry performance by treating safe harbor participants more favorably than non-participants. This approach builds upon the safe harbor program outlined in COPPA. Although COPPA's safe harbor program was well intended, it suffers from a low rate of adoption due to a lack of regulatory flexibility and failure to sufficiently differentiate statutory compliance from program participation.

Properly implemented, a robust safe harbor program could afford the ideal environment to foster innovations in privacy protection while allowing as much flexibility as possible for industry innovation. Critical to the success of a new Safe Harbor program would be differential treatment between firms that chose to participate and those that do not. The DOC should promote what is sometimes referred to as a "co-regulatory" approach, with the right balance of carrots and sticks to incentivize businesses to participate while providing them the space and means to influence the regulatory process. Safe harbor benefits would be limited to firms demonstrating superior performance and would not be available to other covered entities that merely meet the default statutory requirements. This co-regulatory approach is more fully described in my article, "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes" which is available online at http://ssrn.com/abstract=1510275.

Thank you.

Sincerely,

Ira Rubinstein

Senior Fellow, Information Law Institute, NYU School of Law

# Data Privacy Principles for Spurring Innovation

BY DANIEL CASTRO | JUNE 2010

*Policymakers should take a balanced approach to privacy that considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals at the expense of the collective good.*

Technological innovation, particularly in information technology (IT), is at the heart of America's growing economic prosperity. Crafting effective policies that boost innovation and encourage the widespread "digitization" of the economy is critical to ensuring robust economic growth and a higher standard of living. Perhaps the biggest barrier to more rapid progress toward a digitally enabled society is the fear by some people that this will entail a loss of privacy. Although IT is leading to vastly increased convenience, choice, and empowerment for individuals, some advocates see an IT-enabled world as a dystopia where our actions will be tracked by corporate or government leviathans. In this view, IT is stripping us of our privacy and exposing our intimate lives to anyone who wants to see them. As such, they argue that it is up to government not only to severely limit data collection and flows, but also to limit the very technology itself.[1]

Privacy concerns associated with IT must be taken seriously, but it is important to keep a sense of perspective. Historically, major new technologies have prompted what in hindsight were overblown privacy fears. To cite an example, some people objected to easy-to-use cameras, fearing that individuals' activities would no longer be "private' when walking down the street.[2] Or to cite another example, when transistors were first developed, there was a short-lived privacy scare that everyone would be able to be snooped on using small electronic "bugs." In fact, *Life Magazine* had a headline on it "Insidious Invasions of Privacy" and Congress even went so far as to hold hearings on the matter.[3] Of course, all this fuss was much ado about very little.

Society has always learned to manage the so-called threats in large part because of the fact that many—but certainly not all—of the concerns raised by privacy activists are hypothetical and speculative.[4] Given the large amount of information in digital format today, it is worth asking how much harm has

been done to date. Notwithstanding all the fear and gloom from privacy activists, there simply have not been widespread privacy violations caused by existing privacy laws and regulations. Moreover, the debate on privacy to date has been driven largely by privacy fundamentalists (i.e., those individuals who value personal privacy above all other values) that advocate protecting individual privacy above all else, no matter the costs or consequences. However, as with most issues, policymakers should take a balanced approach that considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals that come at the expense of the collective good.

Considered in this light, the answer to many technology-related privacy risks is not to ban IT applications entirely or to enact stringent regulations that limits beneficial uses of data, as some privacy advocates propose, but rather to ensure that the appropriate rules and practices governing privacy and civil liberties are in place and enforced. With this in mind, ITIF recommends that policymakers adhere to the following principles when crafting government regulations on data handling and use:

- Reduce roadblocks that impair the flow of data
- Foster consumer choice
- Protect individuals from harm (rather than try in vain to lock up all potentially harmful data)
- Implement strong protections for civil liberties

## REDUCE ROADBLOCKS THAT IMPAIR THE FLOW OF DATA

Countless examples abound of how sharing information provides many useful benefits to individuals and society from more informed consumers to a more politically engaged society. The private sector continues to find innovative ways to unlock the hidden value of data to create value for consumers and society. Social media tools in particular are an important example of useful data sharing. Consumers have enthusiastically embraced online tools for sharing information with social networking websites like Facebook reporting over 400 million active users worldwide. Political leaders use social networking tools to communicate directly with the public. For example, President Barack Obama has over 8.6 million fans on Facebook and former Governor Sarah Palin has over 1.6 million fans.[5] Consumers share photos on websites like Flickr, videos on sites like YouTube, and opinions and reviews on sites like Yelp. The Wikimedia Foundation hosts various information sharing projects such as Wikipedia, a user-created online encyclopedia, and Wikiversity, an online community for sharing free learning resources. Overall data sharing has created a more useful and interesting experience for Internet users.

Unfortunately, many privacy activists do not just want to set the privacy rules just for themselves, they want to set them for everyone else. Evidence of this can be seen in the recent debate about the privacy settings for Facebook where privacy fundamentalists did not just simply opt not to use the service, instead they advocated for laws to impose their standard of privacy on all users. For example, Danah Boyd a fellow at Harvard's Berkman Center for Internet and Society, claimed that Facebook is a utility and should be regulated like one.[6] Others, such as Chris Conley at the American Civil Liberties Union (ACLU) stated "People are not necessarily thinking about how long this information will stick around, or how it could be used and exploited by marketer."[7] This type of paternalistic view of Internet users is at the heart of arguments in favor of government regulation to protect consumers from themselves.

Such paternalism might be justified if it did not come with significant costs. Many of these proposed regulations either limit useful types of data sharing or impose unnecessary costs on consumers.[8] For example, restriction on sharing information with third parties would limit the ability of organizations to integrate their services with other providers. Organizations would find it more difficult to partner with outside entities to create a combined service. Mash-ups—remixing data across multiple external service providers—are one of the hallmarks of the Web 2.0. For example, Microsoft Hohm allows users to monitor, compare and share their home's energy usage. Google offers an application programming interface (API) which allows developers to create their own custom map. This has resulted in many interesting mash-ups. USA Today has used the API to map all of the home foreclosures in Denver since 2006, while websites such as WikiCrimes

provide mash-ups of user-submitted crime reports, and Virginia Tech's eCorridors application constructs maps of broadband coverage and speeds from user-submitted data. The more significant risk for most consumers is not a loss of privacy, but the loss of free Internet content and services as a result of overly restrictive privacy regulations.

Policymakers should recognize that consumer privacy should not come at the expense of beneficial uses of individual data. Both for-profit and non-profit organizations collect, share and use individual data routinely to provide important services. Organizations routinely purchase contact lists from companies like Hoover's to find sales prospects and media contacts. Websites like Trulia and Zillow use public databases to collect and share home prices and property tax information. Non-profits and politicians routinely purchase data for outreach and fundraising. Organizations promoting government openness use personal data to provide online tools to foster transparency and public accountability. For example, websites like OpenSecrets.org track money in politics and the website LegiStorm provides salary information on Congressional staffers. And of course many organizations have begun to use personal data for targeted advertising. Federal data privacy legislation should ensure that beneficial uses of data are not curtailed by overly-restrictive data sharing policies.

Another significant impediment to the free flow of data is privacy regulations that create unnecessary costs for the private sector which will be borne by consumers. Proposals for expanding privacy regulations rarely consider the impact such proposals have on consumers as a group. Rather, the focus is all about the individual. Policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can come at a real financial cost which hurts all consumers.

Examples of the impact of privacy regulations can be seen in health care.[9] The United States has made a commitment to using information technology to improve health care. In implementing health IT systems, nations must grapple with issues related to ensuring the privacy of patients' sensitive health and other personal information. If privacy laws at the state or federal level are too restrictive, they can impede the adoption of health IT and its use in clinical care. At the federal level, for example, the HIPAA Privacy Rule (45 CFR Parts 160 and 164), which provides the federal floor of privacy protection for health information in the United States while allowing more stringent state laws to continue in force, states that health care providers must "protect against any reasonably anticipated threats." This condition created much initial confusion for providers, who struggled to determine if the use of technology such as e-mail to communicate with a patient violated these terms (it does not).[10] Similarly, at the state level, a recent study of health IT adoption rates found that states with more restrictive privacy laws were less likely to have high rates of EHR usage.[11] Thus, a balance is needed in the United States that can both reassure patients that their privacy is being protected while not implementing restrictive measures that reduce data sharing and result in lower quality care.

The cost of complying with privacy regulations is one reason that any federal privacy regulations should include a preemption clause so that federal law would supersede any state regulations. To be effective, a federal framework for consumer data privacy should establish a single, nationwide standard for consumer privacy thereby reducing regulatory complexity for the private sector. If Congress does move forward with privacy legislation, it should ensure that any new regulations preempt state laws, otherwise online service providers will find themselves facing competing, and possibly contradictory, data use and handling requirements for consumers.

Health care also provides an example of how lack of government action can impede data sharing. As health IT is more widely adopted, the amount of health data that will be available to medical researchers will be increasing substantially. While past medical researchers had only a few limited data points recorded on paper on which to base their hypotheses, in the future researchers will have massive online databases containing terabytes of data for their analysis. Some of the major benefits from modernizing our health care system are expected to come from the improvements in medical research that it will enable. For example, medical researchers will be able to use rapid-learning health networks to determine the effectiveness of a particular treatment for a certain population or to discover harmful side-effects of a drug.[12] Unfortunately, the United States currently lacks the capability to share medical data for authorized research in a timely and efficient manner.[13] To address this problem, future efforts in the

United States to speed adoption of electronic health records systems should include functional requirements to allow the secondary-use of medical data for research. The goal should be to develop a national data-sharing infrastructure to support health informatics research, rather than to create isolated, project-specific research databases.

## FOSTER CONSUMER CHOICE

Societal values change over time and privacy is no different. Over the course of human history, privacy itself is a relatively new value, and varies from culture to culture (and person to person). Certainly the last decade has seen a sharp rise in individuals willing to share what was previously considered private information publicly on the Internet. For example, the website NetworthIQ allows individuals to share their personal financial information online and the microblogging website Twitter allow individuals to easily share personal information, including their location, publicly and in real-time.

In response to consumer demand, the private sector has created a variety of online services catering to consumers with different types of privacy wants. Currently, websites operate under a notice and choice regime, whereby consumers can review the privacy policies, if any, offered by an organization, and then decide whether to use the services offered. For example, if a new mobile application or online service does not provide a privacy notice on their website or states that the organization will share personal information with third-parties, consumers can decide that this does not meet their standards and not use the application or service. This allows for a broad array of consumer choice between services offering different levels of privacy.

Freedom of choice to reveal or conceal private information has led to many important innovations that benefit consumers. Many, if not most, individuals routinely choose to make a trade-off of private data in exchange for something of value. In grocery stores and retail stores, consumers use loyalty cards to allow merchants to track their purchases in exchange for discounts. The same is true online—users allow websites to provide them with free or discounted content or services in exchange for targeted advertising based on personal information. This business innovation has generated an entirely new class of ad-supported online businesses. Moreover, targeted ads—advertisements relevant to a particular user—generate more than two times the revenue of non-targeted ads and are, and will continue to be, an important source of revenue for the Internet ecosystem, particularly the so-called "long tail" of small websites supported by ad revenue.[14] In addition, policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.

Individuals who place a high value on their privacy also help drive innovation. Competition between service providers, whether it is for social networking or for medical data, encourages companies to provide users with simple and effective privacy controls and ensure high levels of security to protect data.[15] Competition also encourages the development of privacy-enhancing technologies (PETs). For example, in response to consumers concerns (mostly unfounded) about the ability of advertisers to track users across multiple websites through the use of cookies (small data files stored on a user's computer by a web browser to improve the web user's experience), every major web browser now includes many features to allow users control over their online privacy and the use of cookies. Other PETs, such as anonymous Internet proxies or anonymous peer-to-peer (P2P) clients, that allow individuals to use the Internet without directly revealing their IP address, similarly have come about because of user interest.

Market forces are an important mechanism for protecting user privacy. One of the most effective ways to ensure that consumers can continue to find online services that satisfy their privacy requirements is to encourage a competitive market that responds to consumer demand. For example, although Facebook is routinely criticized by privacy activists, the company has a long history of responding to consumer pressure including in May 2010 when it announced plans to roll out new privacy controls to users in response to consumer feedback.[16] Neither was this the first time that Facebook revised its policies or services in response to consumer opinion. In December 2009, Facebook altered its privacy settings so that certain information including friends list, gender, city, and profile photo, would be public information. In response to complaints from some users, Facebook modified its

interface to give users more control over the privacy of different types of information. Similarly, in 2006, Facebook revamped its policy regarding its "news feed" feature that updates users about their friends' activities after receiving negative user feedback.

Encouraging competition that gives consumer choices between service providers is more useful than government privacy regulations that try to impose a one-size-fits-all approach to privacy.

## PROTECT INDIVIDUALS FROM HARM (RATHER THAN TRY IN VAIN TO LOCK UP ALL POTENTIALLY HARMFUL DATA)

One key goal of government information policy should be to protect individuals from harm. Many tools, even if they provide important benefits, can be misused and consumers should be protected from misuse. Privacy activists often argue that government should concern itself with the mechanics of how the private sectors handles or uses data rather than the outcomes. However, additional privacy regulations cannot guarantee privacy or prevent accidental disclosures or data theft. Instead, protections should be in place to minimize or eliminate harm to consumers if private data becomes public.

Protecting individuals from harm is important because the impact of private data becoming public is more important for consumers than the mechanism by which it becomes public. For example, individuals concerned about employment discrimination because of their health conditions are better served by strong anti-discrimination regulations that prevent harmful uses of private data than by arbitrary restrictions and limitations on legitimate uses of this data. Often, consumers are already protected from the hypothetical harms envisioned by privacy activists by existing regulations. For example, privacy advocates recently expressed concern that lenders might deny loan applications based on information found on social networking websites even though these lenders would be in violation of the Fair Credit Reporting Act.[17] Similarly privacy concern are sometimes raised for health IT applications involving data sharing. These issues become even more complicated when data must flow internationally, such as when a health care worker is located in another country. For example, teleradiology can involve sharing personal medical data with health care workers not directly involved in a patient's care. However, such concerns are probably unnecessary as patients can hold the original source of the data (i.e. their health care provider) accountable for misuse of their data.

*Protecting individuals from harm is important because the impact of private data becoming public is more important for consumers than the mechanism by which it becomes public.*

Emphasizing the need for government to protect users from harm does not mean organizations are given a free pass to use consumer data without any restrictions. Importantly, organizations must adhere to their stated privacy policies. Protecting users from harm involves enforcing existing regulations. The Federal Trade Commission (FTC), for example, already has sufficient authority to protect consumers from unfair or deceptive trade practices. This means that companies, for example, cannot pull a "bait and switch" on consumers where they promise not to use data in a certain manner and then do so. Where possible, policymakers should first try to improve enforcement of existing policies rather than adding yet another layer of complexity to the existing patchwork of federal laws regulating consumer privacy, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act and the Fair Debt Collection Practices Act. Additional legislation would likely end up imposing more costs on consumers and limiting innovation and the development of new online services. Policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can, as it will here, come at a real financial cost.

## IMPLEMENT STRONG PROTECTIONS FOR CIVIL LIBERTIES

To be sure, as more and more information is created in a digital format, the ease of aggregating information and tying it to individuals has grown. However, in most nations, a series of rules and laws govern how government actors can use personal data, electronic or otherwise. In fact, many of the privacy fears are not about technology, but rather about government access to sensitive information. The fact that more information is in digital form does not change this in any way.

These questions routinely appear as new technologies are introduced that use private information from cloud computing to e-books to the smart grid. For example, the prospect of vehicle manufacturers installing dedicated short-range communication (DSRC) tags on every car, begs the thorny question of who will have access to the tags, what they can do with the information, and whether access will require consent from the driver or vehicle owner. Will government be able to use this information to police violations of speed limits, red lights, and stop signs? Will police have access to vehicle travel histories or real time access to vehicle locations for use in criminal investigations? These are important questions that must be addressed with new technology. Improper use of consumer data by government is a legitimate threat that might prevent more widespread use of technologies like cloud computing. As ITIF and others have argued previously, Congress should act to reform laws such as the Electronic Communications Privacy Act (ECPA) to ensure that citizens have a right to privacy for their electronic data whether it is stored at home on a PC or remotely in the cloud.[18]

Similarly, civil liberties groups have objected to many applications of data mining because of privacy concerns stemming from the risk of data misuse. Some of their concerns arise from the fact that the government's data-mining projects involve data collected from both the public and private sectors. An additional concern is that the proliferation of digital information will lead to privacy violations by the government. The suspension of the U.S. government's Total Information Awareness (TIA) data-mining initiative—eventually renamed the Terrorism Information Awareness Program—reflects the degree of privacy advocates' concern with government data-mining programs. The TIA program established by the Defense Advanced Research Projects Agency was discontinued early in the project's lifecycle, so the privacy concerns raised by civil liberties groups were primarily about potential risks rather than actual problems.[19]

Although data mining does not provide investigators a crystal ball, it still can provide insights and clues into investigations. And the benefits of data-mining programs have not yet been fully explored. As data-mining techniques improve, with better data sources, refined algorithms, and lower false-positive rates, societies must continue to find the appropriate balance between privacy and security. But government should not let legitimate uses of technology to improve public safety get sidelined because of potential abuses; instead it should find ways to use technology effectively while ensuring that civil liberties are protected (as it should be noted, the design of TIA was intended to do).

## CONCLUSION

As data on individuals or their actions increasingly is collected and stored electronically, it is important for policymakers to consider the effect this has on privacy. This Notice of Inquiry provides a welcome opportunity to explore the best ways of protecting individual privacy while avoiding constraints on business innovation and unintended negative impacts on consumers as a whole. Privacy is important, but it must be balanced against competing goals including usability, cost and future innovation. While many technologies can be misused, they should not be banned simply because they come with some risk. Privacy fundamentalists often overstate privacy concerns as a rationale for opposing certain innovations: we have seen this in everything from RFID to biometrics to electronic health records.[20] Moreover, restrictive privacy regulations for the private sector would likely result in less innovation, fewer free services for the average user, and higher costs for consumers. Instead, policymakers should embrace principles that support consumer privacy, but not at the expense of productivity and innovation.

## ENDNOTES


1. For example, see the debate about using smart ID cards.

2. For a modern day example of misplaced privacy fears, see Daniel Castro, "I Spy a Luddite: Why the Lawsuit over Google Street View is Absurd," Information Technology and Innovation Foundation, Washington, D.C., April 25, 2008, http://www.itif.org/files/WM-2008-03.pdf.

3. John Neary, "Electronic Snooping—Insidious Invasions of Privacy," *Life Magazine,* May 20, 1966. http://www.bugsweeps.com/info/life_article.html.

4. Robert D. Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," remarks at the 16th Annual Computer, Freedom and Privacy Conference, Washington, D.C., May 4, 2006, http://www.itif.org/files/rfid.pdf.

5. As of June 7, 2010. Source: Facebook.com.

6. Dana Boyd, "Facebook is a utility; utilities get regulated," May 15, 2010, http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.

7. Brad Stone, "For Web's New Wave, Sharing Details Is the Point," New York Times, April 22, 2010, http://www.nytimes.com/2010/04/23/technology/23share.html.

8. Daniel Castro, "ITIF Comments on Draft Privacy Legislation," Information Technology and Innovation Foundation, May 25, 2010, http://www.itif.org/files/2010-privacy-legislation-comments.pdf.

9. Daniel Castro, "Explaining International IT Application Leadership: Health IT," Information Technology & Innovation Foundation, September 22, 2009, http://www.itif.org/files/2009-leadership-healthit.pdf.

10. Laura Parker, "Medical-privacy law creates wide confusion," *USA Today*, October 16, 2003, http://www.usatoday.com/news/nation/2003-10-16-cover-medical-privacy_x.htm.

11. Amalia Miller and Catherine Tucker, "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," Management Science, 55 (July 10, 2009): 1077-1093.

12. Lynn M. Etheredge, "A Rapid-Learning Health System," Health Affairs, 26 (2007): w107-w118.

13. Daniel Castro, "The Role of Information Technology in Medical Research," 2009 Atlanta Conference on Science, Technology and Innovation Policy, October 2009, http://www.itif.org/files/2009-it-medical-research.pdf.

14. "Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads," Network Advertising Initiative, press release, March 24, 2010, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

15. Daniel Castro, "Improving Health Care: Why a Dose of IT May Be Just What the Doctor Ordered," Information Technology and Innovation Foundation, October 2007, http://www.itif.org/files/HealthIT.pdf.

16. Mark Zuckerberg, "Making Control Simple", Facebook.com, May 26, 2010, http://blog.facebook.com/blog.php?post=391922327130.

17. Catharine Smith, "Lenders Mine Facebook, Twitter For Info On Borrowers," June 4, 2010, http://www.huffingtonpost.com/2010/06/04/lenders-use-facebook-twit_n_600408.html.

18. "ITIF Calls for Updates to Privacy Laws," Information Technology and Innovation Foundation, March 30, 2010, press release, http://www.itif.org/pressrelease/itif-calls-updates-privacy-laws.

19. "Counterterrorism 2.0: Using IT to Connect the Dots," Information Technology and Innovation Foundation, February 23, 2010, http://www.itif.org/events/counterterrorism-20-using-it-connect-dots.

20. See Robert D. Atkinson, "RFID: There's Nothing To Fear Except Fear Itself," 16th Annual Computer, Freedom and Privacy Conference (Washington, DC: May 4, 2006), Robert D. Atkinson, "Confronting Biometric Detractors," 2006 Biometric Consortium Conference (Baltimore, MD: September 21, 2006), and Daniel Castro, "Improving Health Care: Why a Dose of IT May Be Just What the Doctor Ordered," (Washington, DC: ITIF, 2007).

## ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with Information Technology and Innovation Foundation. His research interests include technology policy, security, and privacy. Mr. Castro has a B.S. from the School of Foreign Service at Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

## ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (ITIF) is a Washington, DC-based think tank at the cutting edge of designing innovation policies and exploring how advances in technology will create new economic opportunities to improve the quality of life. Non-profit, and non-partisan, we offer pragmatic ideas that break free of economic philosophies born in eras long before the first punch card computer and well before the rise of modern China and pervasive globalization.

ITIF, founded in 2006, is dedicated to conceiving and promoting the new ways of thinking about technology-driven productivity, competitiveness, and globalization that the 21st century demands. Innovation goes far beyond the latest electronic gadget in your pocket – although these incredible devices are emblematic of innovation and life-changing technology. Innovation is about the development and widespread incorporation of new technologies in a wide array of activities. Innovation is also about a mindset that recognizes that information is today's most important capital and that developing new processes for capturing and sharing information are as central to the future as the steam engine and trans-Atlantic cable were for previous eras. This is an exciting time in human history. The future used to be something people had time to think about. Now it shows up every time we go online.

At ITIF, we believe innovation and information technology are at the heart of our capacity to tackle the world's biggest challenges, from climate change to health care to creating more widespread economic opportunity. We are confident innovation and information technology offer the pathway to a more prosperous and secure tomorrow for all citizens of the planet. We are committed to advancing policies that enhance our collectivecapacity to shape the future we want - beginning today.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. It develops new and creative policy proposals to advance innovation, analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.itif.org.
**ITIF | 1101 K St. N.W. | Suite 610 | Washington, DC 20005**

June 14, 2010

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Docket No. 100402174-0175-01

Dear Sir/Madam,

The Marketing Research Association (MRA) hereby submits these comments in response to the Department's Notice of Inquiry, "Information Privacy and Innovation in the Internet Economy"[1], in support of the survey and opinion research profession.

Respectfully,

LaToya Rembert-Lang
General Counsel
MRA

[1] 75 Fed. Reg. 21226 (April 23, 2010).

**Before the**
**United States Department of Commerce**
**Office of the Secretary**
**National Telecommunications and Information Administration**
**International Trade Administration**
**National Institute of Standards and Technology**

| | | |
|---|---|---|
| In the Matter of: | ) | |
| | ) | |
| Information Privacy and Innovation in | ) | |
| the Internet Economy | ) | **Docket No. 100402174-0175-01** |
| | ) | |
| | ) | |

# COMMENTS OF THE MARKETING RESEARCH ASSOCIATION (MRA)

LaToya D. Rembert-Lang
General Counsel
Marketing Research Association
1111 16th Street, NW Suite 120
Washington, DC 20036
(202) 775-5171

June 14, 2010

## TABLE OF CONTENTS

## INTRODUCTION AND SUMMARY

The Marketing Research Association (MRA) hereby submits comments in response to the Notice of Inquiry seeking comment on the impact of current privacy laws on the pace of innovation in the information economy. Specifically, MRA comments on the scope of current privacy laws and its implications for the survey and opinion research profession.

MRA, a non-profit national membership association, is the leading and largest association of the survey and opinion research profession. MRA promotes, advocates and protects the integrity of the research profession and strives to improve research participation and quality. The research profession is a multi-billion dollar worldwide industry, comprised of pollsters and government, public opinion, academic and goods and services researchers, whose companies and organizations range from large multinational corporations to small or even one-person businesses.

Survey and opinion research is the scientific process of gathering, measuring and analyzing public opinion and behavior.[2] On behalf of their clients -- including the government (the world's largest purchaser), media, political campaigns, and commercial and non-profit entities -- researchers design studies and collect and analyze data from a small but statistically-balanced sample of the public. Researchers seek to determine the public's opinion regarding products, services, issues, candidates and other topics. Such information is used to develop new products, improve services, and inform policy.

[2] MRA has developed the following definition of survey and opinion research, in consultation with the research profession: "Bona Fide Survey and Opinion Research" means the collection and analysis of data regarding opinions, needs, awareness, knowledge, views, experiences and behaviors of a population, through the development and administration of surveys, interviews, focus groups, polls, observation, or other research methodologies, in which no sales, promotional or marketing efforts are involved and through which there is no attempt to influence a participant's attitudes or behavior.

## III. THE DEPARTMENT SHOULD SUPPORT A PRIVACY STANDARD OF SELF-REGULATION

### A. The Survey and Opinion Research Profession Incorporates a Standard of Self-Regulation

Privacy is a key component of the survey and opinion research profession. The survey and opinion research profession is unlike most businesses that collect data in support of their businesses or in order to make their businesses work. The collection and analysis of data is the business of the survey and opinion research profession. Therefore, privacy is the cornerstone of the survey and opinion research profession.

Research information is not normally looked at by individual answers. Instead, each person's answers are combined with those of many others reported as a group to the client who requested the survey. Moreover, most research companies destroy individual data records at the end of the study, and names and contact information of participants are separated from the answers if additional tabulation of the results is conducted. Again, all of the personally identifiable records are usually destroyed after the study is completed or the validation check has been made, and all of a respondent's personally identifiable information is kept strictly confidential. Legitimate survey and opinion researchers never divulge the identity, personal information or individual answers of a research participant unless specifically granted permission to do so by the participant.

Due to the nature of the survey and opinion research process, confidentiality is the bedrock of the research and the resultant industry codes and guidelines, like the MRA Code of Marketing Research Standards[3]. Members of MRA are stringently bound by their ethical obligation to protect the privacy and confidentiality of research participants

[3] *MRA Expanded Code of Market Research*, available at http://www.mra-net.org/resources/documents/CodeMRStandards.pdf.

and their data and maintain thorough practices to obtain consent prior to sharing any personally identifiable information. MRA members uphold to the Federal Trade Commission's Fair Information Practice Principles[4] and have numerous best practices on the handling of personal information.

The Department should support the approaches taken by MRA and the survey and opinion research profession and recommend model guidelines that promote self-regulation of privacy and confidentiality. Standards should be implemented that support the notion of protecting the privacy and confidentiality of consumers, but also maintain that the specifics of protecting consumers should be determined according to the individual endeavors of each business in a self-regulated framework. The standards should particularly focus on the incorporation of codes and guidelines, formal complaint procedures, best practices and the application of the Fair Information Practice Principles.

## IV. THE DEPARTMENT SHOULD ENDORSE FEDERAL PRIVACY LAWS THAT PRE-EMPT STATE LAW

### A. A Segmented Privacy Law Framework Imposes Compliance Burdens on Survey and Opinion Research

The multitude of various federal and state privacy laws creates a fragmented privacy framework that makes compliance difficult for survey and opinion researchers. Current privacy laws create different obligations and challenges, and sometimes conflicting standards. The burden of compliance with multiple privacy laws with different obligations is a serious challenge for a profession whose business <u>is</u> data. The survey and opinion research profession is composed of a broad spectrum of various

[4] Federal Trade Commission, Fair Information Practice Principles, available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm. These principles include: Notice/Awareness, Choice/Consent, Access/Participation and Integrity/Security.

entities which are often small businesses and often engage in multi-state and international survey research activities. Due to the broad nature of privacy laws on the state and federal level, survey and opinion researchers are often forced to create different research models based on the location where the research is conducted. As a result, there is a time burden imposed on completing a research study and an extensive cost burden for maintaining standards for compliance practices and procedures for every law and regulation.

The Department should endorse federal privacy laws that pre-empt the numerous privacy laws on the state level. The federal privacy framework should be based on the overarching needs of protecting the privacy and personal information of consumers that has been often incorporated in state laws, but develop a means whereby conflicting standards are overruled in a comprehensive federal privacy law that promotes a uniform standard for privacy enforcement.

### B. The Department Should Not Endorse a Federal Privacy Law Framework Based on the European Union

Although the Department should endorse the creation of federal privacy laws, the framework should not follow the model of the European Union.[5]. The framework should be based on the needs of businesses and consumers within the United States and their respective perceptions of and needs for privacy. Privacy should balance the needs of consumers with the ability to share information in order to conduct business.

The Department, however, should establish a privacy law framework that harmonizes international laws, particularly with respect to the EU Data Directive. This

[5] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31 *et seq.*).

framework should reflect the desires of businesses dealing in the EU environment, but also incorporate practices that allow the free flow of information to continue. The framework should support the notion of safeguarding personal information, yet safeguarding should be based on the level of sensitivity of the information.

## CONCLUSION

The survey and opinion research professional supports the endeavors of the Department in creating a model privacy law framework. For the reasons illuminated in this comment, MRA respectfully requests that any proposed legislation or regulatory activity be reflective to balance the needs of consumers and businesses as any direct law or regulation will have serious implications for the survey and opinion research profession. Thank you for providing the survey and opinion research profession the opportunity to share our perspectives in this matter. We look forward to working with the Department to create a privacy law framework that incorporates the business needs of the survey and opinion research profession.

Respectfully Submitted,

LaToya D. Rembert-Lang
MRA
1111 16th Street, Suite 120
Washington, D.C. 20036
(202) 775-5171

June 10, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams,

## I. **Introduction**:

Microsoft Corporation appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration's (NTIA) Notice of Inquiry (NOI), on "Information Privacy and Innovation in the Internet Economy," as part of the Department's Internet Policy Task Force mission to identify leading public policy and operational challenges in the Internet environment.

In addition to this submission, Microsoft is also a signatory to the Centre for Information Policy Leadership (CIPL) submission. Microsoft supports the Centre's thought leadership on these issues. But, we also wanted the opportunity to provide some additional company insights to a number of the probing questions raised in the NOI. Microsoft commends the Department's efforts in conducting this inquiry and believes now is the right time for the United States to address these critical issues.

We note that the questions posed by the NOI were extremely expansive. In this submission, Microsoft will not attempt to answer all of these questions but instead hopes to provide some insight into what we consider to be some of the key questions posed by the Inquiry in Q&A format.

## II. Future US Federal Policy Framework:

**Q. Does the existing privacy framework provide sufficient guidance to the private sector to enable organizations to satisfy these laws and regulations?**

*A. We believe that now is the right time to revisit the current policy framework, both in terms of "privacy policy" but also in terms of more expansive, "information policy" as outlined in the CIPL submission. In late 2005, Microsoft, and other companies, called for a set of baseline requirements through comprehensive privacy legislation that are not specific to any one technology, industry or business model. We asserted then – as we do now – that to achieve this, baseline legislation would need to be flexible, technology neutral and can build upon the current framework of technology tools, sound*

*business practices, self-regulation and enforcement. Getting the balance right will also require a close partnership between industry, government, advocates, and consumers*. *This NOI process is a positive step for this collective input and dialogue.* It is also important to examine these issues in the context of an increasing global focus on privacy.

**Q. Are there modifications to U.S. privacy laws, regulations and self-regulatory systems that would better support innovation, fundamental privacy principles and evolving consumer expectations? If so, what areas require increased attention, either in the form of new laws, regulations or self-regulatory practices?**

A. *When Microsoft and other companies called for baseline privacy protections five years ago, we suggested some very basic but fundamental guidelines be put into place. This included federal pre-emption, baseline privacy protections that applied both online and offline, increased transparency and user control over collection, use and disclosure of data and minimum security requirements. But, as the information economy has rapidly evolved, so too has our thinking around the fundamentals of information policy.*

*Such a framework would necessarily build on the important protections already in place and should be framed by a clear set of information policy principles. These principles should serve as clear guidelines – rather than regulations – that define organizational accountability and align with other international privacy standards and norms. We believe the development of such principles needs to include broad stakeholder engagement and be outcomes-based, to help clarify application of privacy regulations. Taking an outcomes-based approach would help the private sector understand accountability, would isolate many of the risks associated with data, and it would give guidance to law enforcement agencies as they prioritize their efforts. To that end, enforcement should focus on harms, with the nexus on the use of the data. This is because it is increasingly difficult to track data back to the original collector. It therefore enhances consumer protection to make the use of data the nexus for enforcement rather than the collection. Finally, we believe that the current regime of functional enforcement organized – which looks at how data is used, or abused within specific industries – should remain the same.*

*These reasons for supporting sensible federal privacy legislation in 2005 are equally compelling in 2010. Earlier this year, we called on Congress to take a critical look at the specific security and law enforcement issues raised by cloud computing, for both consumers and enterprises. Recognizing that these issues have to be examined thoughtfully, we welcome the opportunity to work with Congress, the Administration and other stakeholders to determine the most appropriate vehicle for promoting trust and protecting user data to advance commerce and the growth of cloud computing.*

*While Microsoft sees an increasingly important role for basic privacy guidelines to be laid down, we have also asserted that we do not believe that legislation is a complete solution. Legislation must work in conjunction with industry self-regulation and best practices, technology solutions, and consumer education. As noted above, there are some areas, particularly with respect to emerging technologies or business models where self-regulation will ultimately be the preferred model at the outset. Search and online advertising are examples of this and we commend the FTC for establishing self-regulatory*

*guidelines for online advertising, as one pertinent example. Because both models create legitimate concerns about what user information is collected and for what purposes it is used, in July 2007, Microsoft introduced an enhanced set of privacy principles related to search and online advertising to ensure a greater level of transparency for consumers. Additionally, Microsoft actively engages with data protection authorities around the world to ensure that our practices meet high standards for protecting privacy.*

**Q. An addendum to question 2 – Cloud Computing Advancement Act (CCAA) and ECPA**

*For the cloud to deliver on its promise, we believe the USG needs to take responsible action to foster users' confidence that their privacy interests will be preserved and their data will remain secure in the cloud. One possible avenue we would advocate the Department and Congress consider is the introduction and eventual passage of the, "Cloud Computing Advancement Act," which would include several key elements:*

- ***Strengthen privacy*** *by ensuring that users are not forced to give up their reasonable expectations of privacy when they move data to the cloud. Among other things, Congress should update the Electronic Communications Privacy Act of 1986 and related laws to account for how people use cloud technologies today and how they will use them in the future.*

- ***Enhance security*** *by increasing law enforcement resources and strengthening criminal and civil enforcement mechanisms against malicious hacking of cloud services. As a first step, Congress should amend the Computer Fraud and Abuse Act (CFAA) to make it easier for law enforcement and cloud providers to combat unauthorized access to data stored in the cloud. Congress also should provide law enforcement with the funding it needs to pursue cybercriminals.*

- ***Help users make informed choices*** *by promoting transparency around cloud providers' security practices.*

*We believe that such consideration in necessary because ECPA, in particular, has been overtaken by technological change, and it no longer strikes the right balance between consumers' privacy interests and the government's legitimate need to access user information when it comes to new developments like cloud computing. For these reasons, Microsoft supports the efforts to modernize ECPA that are being led by the Center for Democracy and Technology (CDT) and has recently joined the Digital Due Process coalition to address these issues. We believe such reform is vital to bring the statute up-to-date and into alignment with current technological realities and that this should involve extensive stakeholder input.*

*We also believe these reforms of ECPA would complement prior calls for omnibus federal privacy guidelines. Comprehensive legislation would ensure that consumers understand and have control over the data collected about them both online and offline. In combination, omnibus federal privacy legislation, responsible reforms to modernize ECPA, and industry leadership and best practices can help create an environment that addresses users' legitimate concerns over the privacy implications of cloud computing and engenders user confidence in the cloud.*

*Finally, the Administration can help **promote user confidence in the cloud** by working with other governments to agree on common approaches to jurisdiction over cloud services and data stored in the cloud—an issue that is of particular concern where cloud services transcend national borders.*

**Q. Those who urge a use-based model for commercial data privacy should detail how they would go about defining data protection obligations based on the type of data uses and the potential harm associated with each use. Describe how a use-based privacy system would work?**

A. *The premise of the "use and obligations" model is that the decision to **use** information creates legal **obligations** on the organization that uses the information. At a practical level, such a system may classify uses based on standard use categories. These categories might include: (A) fulfillment; (B) internal business processes; (C) marketing and selling of products and service; (D) fraud prevention and authentication; (E) research; and (F) public purposes. Irrespective of where data was collected or by whom, the obligations related to the use categories must be honored.*

**Q. What is the relationship between use-based privacy rules and proposed accountability systems?**

A. *The concepts are interrelated and complimentary as the obligations placed on various information uses requires organizational accountability. Under the accountability model, organizations of every size that collect or use information should assess and understand the risks that they create for others and mitigate those risks appropriately. Furthermore, promises made to individuals – including those related to complying with national laws must be honored regardless of the use, no matter where data is processed or by whom. Fundamentally, this means organizations must be transparent and answerable for their strategies to identify and mitigate risks.*

## III. State Legislation

**Q. What, if any, hurdles do businesses face in complying with different state laws concerning privacy and data protection?**

*One of the reasons Microsoft has supported the adoption of an omnibus federal privacy law is because the increasingly complex patchwork of state and federal laws resulted in an overlapping, inconsistent and incomplete approach to protecting privacy. We believe that this is both inadequate and confusing from the perspective of consumers, and unnecessarily burdensome for organizations. Additionally, widely publicized privacy lapses indicated that not all companies were adopting responsible practices for protecting the data they maintain. And these failures were leading to concerns among consumers about privacy and identify theft that threatened to erode public trust in the Internet and dampen online commerce. To illustrate the extent of this challenge, 45 U.S. states, the District of Columbia, Puerto Rico, and the Virgin Islands have each enacted their own legislation requiring notification of security breaches involving sensitive personal information. Especially for organizations committed to the proper management and use of personal information, compliance with this many different data breach regimes can prove both difficult and expensive.*

## IV. International Privacy Laws and Regulations

**Q. What, if any, hurdles do businesses face in complying with different foreign laws concerning privacy and data protection? Q. Do foreign laws that contain content-based restrictions impede global trade or foreign investment?**

*See response about conflicting state laws above. Multiply this by the number of local data breach notification laws coming into effect in other parts of the globe, and compliance in this single realm becomes a regulatory quagmire.*

*That said, this legal patchwork has been a facet of the global privacy environment and companies like Microsoft, who have done business internationally for some time have had to come up with mechanisms to comply without interfering with business operations or trans-border data flows.*

*The foundation of Microsoft's approach to privacy and improved data protection is a commitment to empowering people to help control the collection, use and distribution of their personal information. One way we have implemented this is by instituting clear privacy principles and a corporate privacy policy, which together govern the collection and use of all customer and partner information, provide our employees with a clear and simple framework to help ensure privacy compliance companywide. We made sure that these principles represented the "highest common denominator" in terms of privacy protections so that every Microsoft customer, regardless of geography, would enjoy the same high level of privacy protection whether a law was implemented in their country or not. These principles also closely align with globally accepted fair information privacy principles enshrined in the OECD and APEC Privacy Frameworks. And, we believe that both companies and policymakers need to focus on where the commonalities of information policy and privacy principles exist to forge a greater level of global harmonization then focusing on differences or "adequacy standards" and the like.*

*Of course, there are other mechanisms that can be used to help facilitate such trans-border data flows such as through "safe harbor agreements" and "binding corporate rules" but these too have certain limitations.*

*In light of the ascendance of cloud computing and exponential growth in global data flows, we believe that we need to view these issues and policy solutions from a very different perspective.*

*To explain, we now have a fundamental tension at play. Information flows are global but privacy is local – privacy and security laws are also local. We need to question what "local" mean in this distributed global environment. Is it where the consumer resides? Where the data is stored? Where the business is registered? Or, perhaps even the jurisdictions this data may be routed through?*

*The "local" aspect is at fundamental tension with the complexities of information flows today, and by extension, at tension with the various players - for example, a policymaker in one economy is likely conditioned to think and prioritize "locally" despite the "global" reality of information flows. Trying to apply laws to data extraterritorially or manage trans-border data flows through corporate binding rules or contracts may prove to be even more challenging – if not impossible - as modern data flows become more continuous and multipoint.*

*Given these challenges, we believe a privacy governance model based on **accountability** which requires that businesses take ownership and responsibility for the management of information – regardless of where it resides or is processed – is an important consideration. This is important because industry would like predictability and consistency and to clearly understand it's "accountability" responsibility. It is also important for policymakers and regulators everywhere to think and act both locally and globally – and this is also a tension. This can be done by ensuring that domestic legislation is consistent with well accepted international norms; that we should be considering a range of international and regional efforts such as the APEC and OECD efforts or perhaps even the COE's Data Protection Convention or emerging global standards efforts. It may be complicated and difficult, but we believe it is the only way forward.*

**JURISDICTIONAL CONFLICTS AND COMPETING LEGAL OBLIGATIONS**

Q. **Do organizations face jurisdictional disputes as a result of domestic or foreign privacy laws? What, if any, conflicting legal obligations do companies face as a result of data privacy laws? How do companies address jurisdictional conflicts and any resulting conflicting legal and regulatory obligations? Does cloud computing, or other methods of globally distributing and managing data, raise specific issues with respect to jurisdiction of which Commerce and regulators should be aware? Have jurisdictional conflicts had any impact on U.S. consumers?**

*Today, foreign governments seek access to data or other evidence located in another jurisdiction through international legal instruments, such as Mutual Legal Assistance Treaties, and through established judicial procedures such as Letters Rogatory. For providers like Microsoft, we currently store all personal data of our U.S. customers in datacenters that are located in the United States. At the same time, Microsoft is building datacenters outside the United States, and the ability to transfer data across datacenters is critical to the efficiency and reliability of cloud computing in the long term. Cloud computing does not diminish or expand a foreign government's ability to seek access to customer data through these instruments.*

*The complications in the cloud computing context arise because a provider may have datacenters located in multiple countries, and providers need to be able to transfer data between datacenters freely in order to maximize the efficiencies and other benefits of cloud computing. Another complicating factor is that different countries can have divergent and, at times, conflicting approaches with respect to whether and how the government should access data stored by online service providers abroad. This uncertain state of the law — along with the highly fact-specific nature of whether a government entity has jurisdiction over data — precludes any blanket statements as to exactly when foreign governments can compel production of data held by online service providers.*

*Any long-term solution to the problem of conflicting jurisdictional claims and inconsistent legal obligations over data stored in the cloud must involve all stakeholders and specifically include leadership from governments. The most effective solution would be the development of a multilateral framework, such as a treaty, to address jurisdictional claims and requirements in a coherent fashion. Short of a multilateral solution, governments should continue to pursue bilateral consultations and consensus*

*building on procedures for resolving data access and privacy issues in ways that avoid placing cloud providers under conflicting legal obligations or erode user trust in the cloud. Such bilateral cooperation might also pave the way for a longer-term, more formal solution. In the shorter term, governments should seek ways to enhance existing Mutual Legal Assistance Treaties (MLATs) to improve the speed and effectiveness of assistance between them.*

*Until that happens, multinational companies may be operating in very murky waters where jurisdictional issues are likely to increasingly arise. We believe that those countries those countries that work with other governments, including the United States, to develop coherent, consistent obligations are places where cloud service providers are going to feel comfortable storing data and making other investments in providing cloud services to consumers and businesses. Those are the countries that will realize the benefits of cloud computing the most quickly and the most meaningfully.*

**SECTORAL PRIVACY LAWS AN FEDERAL GUIDELINES**

**Q. How does the current sectoral approach to privacy regulation affect consumer experiences, business practices or the development of new business models?**

*It adds to the complexity of compliance for many organizations, confusion among consumers and it potentially results in certain gaps in the law for emerging sectors or business models. As recommended above, baseline privacy protections that apply across sectors that are not specific to any one technology, business model or sector is preferred.*

**Q. How does the sectoral approach affect individual privacy expectations? What practices and principles do these sectoral approaches have in common, how do they differ?**

*This very much depends on the consumer as well as the sensitivity of the data in question. Fundamentally, individuals have rights related to the collection and management of information that pertains to them. Those rights are contextual based on the types of data collected and used, how the data are us used, and who is using the data. Those rights may include consent, access to information, and the ability to correct or request deletion or masking. These rights should be consistent across sectors.*

**NEW PRIVACY ENHANCING TECHNOLOGIES AND INFORMATION MANAGEMENT PRACTICES**

**Please describe any other ongoing efforts to develop privacy-enhancing technologies or processes of which the Commerce Department should be aware. Is any government action needed to encourage the marketplace in this direction?**

*Our software products are designed to empower individuals to block unwanted communications, protect themselves from potentially dangerous online content, and control the details of their online activities. Specifically, the InPrivate Browsing and InPrivate Filtering options in Internet Explorer 8 give individuals greater control over details about their online activities. InPrivate Browsing helps prevent users' browsing history, temporary Internet files, form data, cookies, and usernames and passwords from being retained by the browser, thereby leaving virtually no evidence of their browsing or search history.*

*InPrivate Filtering helps individuals control the elements—such as maps, ads, scripts, or images—that third-party Web sites can potentially use to track their browsing activity.*

*A few other examples include the SmartScreen Filter, part of Internet Explorer 8 and Microsoft's e-mail platforms, which helps identify and block intrusive communications as well as dangerous online content by notifying people when they try to visit a Web site or download software that has been reported as unsafe. Another example includes IE 8 We also offer Microsoft Security Essentials, a free download that protects against viruses, spyware, and other malicious software.*

*Another area that is increasingly important in this context is identity management. To get the complexities of online identity management right, we need to balance privacy and security. Microsoft believes that we have an innovative cryptographic technology called U-Prove that balances both imperatives. U- Prove enables solutions that can ensure users reveal no more than the minimum amount of necessary information needed by a given service or applications. It can also eliminate unnecessary or unwanted linking and tracing capabilities. In March, Microsoft announced the first step toward making U-Prove available for free to anyone interested. Essentially, we donated the IP and have opened the technical foundation to the community to explore so people can test the technology organically given we believe so strongly in its importance and benefits. We did this because we believe that for an identity metasystem to take hold, the associated political, economic, legal and technical forces need to be better aligned for the ecosystem to thrive.*
*In terms of privacy enhancing processes, Microsoft has instituted robust internal standards guided by the principles of: Privacy by default, privacy by design and privacy by deployment. We have developed a process called the Microsoft Standard for Privacy Development (MPSD) and we make this standard publicly available for other organizations to use to develop and guide their own product development and gating processes.*

*While we do not believe that specific privacy enhancing technologies or processes should be mandated by law, incentives and encouragement to do so should be encouraged through flexible guidelines and standards. It bears mentioning that the concept of "privacy by design" has taken hold in a number of jurisdictions around the globe, including Canada and Europe and should be considered in the context of any legislative or regulatory guidelines being contemplated in the U.S.*

**SMALL AND MEDIUM-SIZE ENTITIES**

**Q. How do existing privacy laws impact SMEs and startup companies? Please describe any unique compliance burdens placed on smaller companies as a result of existing privacy laws.**

*Compliance with existing laws and the building of requisite privacy processes require a certain level of investment and organizational maturity that some SMEs may not have the luxury of possessing. For SMEs conducting business inter-state or internationally, the complexity and costs will likely multiply.*

**Q. Are there commercial or collective tools available to address such issues? How might privacy protections be better achieved in the SME environment?**

*There may be some third party tools that are available. Microsoft, for instance, has published its Microsoft Privacy Standard for Development (MPSD) precisely for this reason – so that other companies could have the benefit of our experience and apply these processes and standards as they see fit. A number of SMEs also use third party trust agents, such as TrustE for both guidance and validation that they are striving to be privacy-centric organizations.*

**Q. Have smaller companies been unable to engage in certain types of business activities as a result of existing privacy laws?**

While we cannot say for certain, we would guess that some existing and soon to be enacted laws present challenges to smaller companies. For example, while they have not been implemented yet, t*he new EU model clauses require extensive flow through of contract terms to sub-processors, as well as tracking of sub-processors, which represents a significant administrative burden. The new model clauses go into effect May 15. We're working on keeping better track of our vendors as required, but for smaller companies this could be quite difficult.*

**ROLE FOR COMMERCE GOVERNANCE**

**How can the Commerce Department help address issues raised by this Notice of Inquiry?**

*The Commerce Department can help address the issues raised in the NOI by stimulating the discussion, assimilating feedback from interested stakeholders and presenting the ideas to Congress. Additionally, DOC can help guide discussions and leadership with policymaking bodies and multi-lateral organizations like the OECD and APEC to ensure greater levels of consistency and harmonization across borders, help drive solutions and/or adjudicate around jurisdictional and cloud issues and provide privacy leadership for the US abroad.*

**CONCLUSION**

Microsoft appreciates the opportunity to contribute to the Department of Commerce's work to encourage the appropriate balance between privacy and innovation in the information economy. We look forward to continuing our engagement with the Department on these important policy issues and please do not hesitate to contact us should you need further information or clarification of these comments. Please direct any questions to Peter Cullen at pcullen@microsoft.com or Julie Inman Grant at juliei@microsoft.com.

# GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES*

MIRIAM WUGMEISTER,** KARIN RETZER,*** CYNTHIA RICH****
MORRISON & FOERSTER LLP

## I. INTRODUCTION

Technology has radically changed the manner in which information flows around the world. Global transfers of information are now a common and essential component of our daily lives. Sharing information allows businesses to provide consumers with enhanced services such as 24-hour customer hotlines as well as a greater choice of products and services at lower prices. At the same time, businesses are able to manage their operations in a more cost effective and efficient manner. Countries, in turn, benefit from increased global business investment and activity. All in all, consumers, businesses and governments receive enormous benefits from global data transfers.

Nevertheless, such transfers are becoming more difficult and costly from a business perspective as more countries adopt privacy laws that, among other things, regulate and limit cross-border transfers of personal information, including transfers to headquarters, affiliates, branch offices or subsidiaries. Typically these laws either explicitly prohibit transfers to other countries unless certain conditions are met or impose regulatory obligations on the organizations transferring the personal information. Many of these laws are enacted in response to growing public concern about the potential and actual misuse of personal information in an increasingly networked economy.

Privacy laws, however, vary dramatically from country to country. Some countries have enacted comprehensive laws while others have

---



** Miriam Wugmeister is a Partner at the law firm of Morrison & Foerster LLP. She heads the Firm's Global Privacy and Data Security Practice and is resident in the New York office of Morrison & Foerster. She can be reached at mwugmeister@mofo.com.

*** Karin Retzer is an Of Counsel at the law firm of Morrison & Foerster LLP. She leads the Firm's European Privacy and Data Security Practice and is resident in the Brussels office of Morrison & Foerster. She can be reached at kretzer@mofo.com.

**** Cynthia Rich is a Senior Policy Analyst at the law firm of Morrison & Foerster LLP. She is a key member of the Firm's Privacy and Data Security Practice and is resident in the Washington DC office of Morrison & Foerster. She can be reached at crich@mofo.com.

little or no rules in place. For those countries that do have laws in place, the standard of protection provided for in the law, its interpretation and the level of enforcement can vary significantly.

At the same time, the cross-border limitations are adversely affecting both the quality and choice of products and services that can be offered to consumers on a global basis. Consumers and employees (herein referred to as "individuals") as well as businesses are equally ill served by this patchwork arrangement of cross-border privacy protections.

As a result, greater attention is being paid to the development and use of global or enterprise-wide privacy rules ("Corporate Privacy Rules") as a way to correct the problems associated with this patchwork of cross-border privacy rules. Under Corporate Privacy Rules, businesses would establish their own set of rules for the transmission of personal information via the Internet. These rules would incorporate internationally accepted principles of fair information practices. If all affiliates are subject to the Corporate Privacy Rules, then a business could freely move information within the entire group, e.g., between headquarters, subsidiaries, branch offices and any affiliated entities.

The concept of Corporate Privacy Rules is based on the notion of accountability—that is, the organization as a whole assumes responsibility for protecting the data. Corporate Privacy Rules are not a new concept; rather, they are an extension of an approach that has worked successfully in other areas for many years (e.g., enterprise-wide policies in the field of financial reporting and determination of conflicts of interest). The challenge, however, will be to secure the necessary international acceptance and cooperation that will enable businesses to implement Corporate Privacy Rules as a global, rather than a national or regional, solution for cross-border data transfers.

Two of the major stumbling blocks to the widespread acceptance and use of Corporate Privacy Rules are concerns about the manner in which such rules can be enforced under existing laws and methods to secure the necessary cooperation among the respective enforcement authorities in the event of cross-border disputes or breaches. These stumbling blocks, however, are not insurmountable, contrary to what some in the data protection community might think. As we will explain, there are other laws such as those that pertain to unfair commercial practices which can be used to enforce Corporate Privacy Rules. Moreover, while cross-border cooperation is not easy to accomplish, it is not unprecedented. There are many areas in which government agencies around the world are already collaborating. These existing arrangements could serve as a source or model for cooperation in the privacy area.

Before addressing the issues of enforcement and cross-border cooperation, this article will provide an overview of the international privacy legislative landscape and the difficulties that arise on a practical level from both a consumer and business perspective. It will then assess the current options available for cross-border transfers, identify the advantages and disadvantages of same, and then discuss how Corporate Privacy Rules can be used to overcome the current difficulties.

## II. Privacy Laws—an Overview

### A. *Privacy Landscape*

More than sixty countries around the world have laws that regulate the collection, use and disclosure of personal information.[1] Typically these laws cover any personal information pertaining to individual customers, business contacts, consumers, employees and in some cases legal entities. By and large, these laws require that the collection of personal information or establishment of databases containing personal information be publicly disclosed and that these activities be registered with the government or with an independent data protection authority ("DPA"). They also require that individuals whose personal information is maintained by an organization be given notice of, and in certain circumstances the right to consent (or to withhold consent) to, the collection, use and transfer of their personal information, as well as the right to access and correct the information held about them. In addition, organizations must protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Growing concerns about data security have resulted in some countries prescribing detailed technical and organizational security measures.

The laws of some of these nations also require the permission of a DPA to "export" or transfer personal information. These DPAs may refuse permission if the data protection laws of the receiving country are not considered to be as strong as those of the home country. Failure to adhere to these rules may result in civil and/or criminal penalties for the organization concerned.

Countries or jurisdictions that now have privacy statutes include:

1. "Personal information" as used in this Article denotes any information about an identified or identifiable individual.

- **Asia**: Australia,[2] Japan,[3] Hong Kong,[4] Macau,[5] New Zealand,[6] South Korea[7] and Taiwan;[8]
- **Europe**: the 27 European Union (EU) Member States,[9] Albania,[10]

---

2. Privacy Act 1988 (amended 2006), *available as amended at* http://www.privacy.gov.au/publications/privacy88130706.pdf.

3. Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *available in unofficial English translation at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

4. Personal Data (Privacy) Ordinance, (1995) Cap. 486. (H.K.), *available at* http://www.pcpd.org.hk/english/ordinance/down.html.

5. Lei da Protecção de Dados Pessoais [Personal Data Protection Law], Lei No. 8/2005, No. 34 Boletim Oficial da Região Administriva Especial de Macau I Serie 868 (2005) (Mac.), *available at* http://images.io.gov.mo/bo/i/2005/34/lei-8-2005.pdf.

6. Privacy Act, 1993 S.N.Z. No. 28, *available at* http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes.

7. Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (amended 2005), *available in unofficial English translation at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

8. The Computer-Processed Personal Data Protection Law (1995), *available in unofficial English translation at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf.

9. The twenty-seven EU Member States and their respective data protection acts are: *Austria*—Bundesgesetz über den Schutz personenbezogener Daten [Datenschutzgesetz 2000-DSG 2000] [Federal Act Concerning the Protection of Personal Information] Bundesgesetzblatt Teil I [BGBl I] No. 165/1999 (amended 2001) (Austria), *available at* http://www.dsk.gv.at/dsg2000e.pdf; *Belgium*—La Loi Relative à la Protection des Données à Caractère Personnel [Privacy Protection in Relation to the Processing of Personal Data] (1992) (amended 1999), *available at* http://www.privacycommission.be/textes_normatifs/loi_wet_8_12_92%20.pdf *and in unofficial English translation at* http://www.law.kuleuven.ac.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf; *Bulgaria*—Personal Data Protection Act 2002, State Gazette No. 1/4.01.2002 (amended 2006), *available in unofficial English translation at* http://www.aip-bg.org/pdf/pdpa.pdf; *Cyprus*—The Processing of Personal Information (Protection of Individuals), Law 138 (I) (2001) (amended 2003), *available in English translation at* http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument; *Czech Republic*—[Personal Data Protection Act], zákon č. 101/2000, *available in unofficial English translation at* http://www.uoou.cz/index.php?l=en&m=left&mid=01:01:01&u1=&u2=&t=; *Denmark*—Act on Processing of Personal Data, Act No. 429 (2000), *unofficial English translation available at* http://www.datatilsynet.dk/attachments/20001061548/ENGELSK%20LOV.doc; *Estonia*—Isikuandmete Kaitse Seadus [Personal Data Protection Act] (2003), Riigi Teataja [RT I] 2003, 26, 158 (amended 2004), *available at* https://www.riigiteataja.ee/ert/act.jsp?id=264800 *and in unofficial English translation at* http://www.legaltext.ee/text/en/X70030.htm; *Finland*—Personuppgiftslag [Personal Data Act], 523/1999 (amended 2000), *available at* http://www.abo.fi/dc/admin/reglerlagar/L-personuppgifter.pdf *and in unofficial English translation at* http://www.tietosuoja.fi/uploads/hopxtvf.HTM; *France*—Law No. 78-17 of Jan. 6, 1978 [Data Processing, Data Files and Individual Liberties], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 7, 1978 (amended 2004), *available in official English translation at* http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf; *Germany*—Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990 BGBl. I 1990 at 2954, *available at* http://www.bfdi.bund.de/cln_030/nn_

Bosnia and Herzegovina,[11] Croatia,[12] Iceland,[13] Liechtenstein,[14]

---

946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct, templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf; *Greece*—Nomos (1997:2472) [Protection of Individuals with Regard to the Processing of Personal Data] (amended [year]), *available at* http://www.dpa.gr/law2472.htm, *English translation available at* http://www.dpa.gr/Documents/Eng/2472engl_all.doc; *Hungary*—1992. évi LXIII. Törvény a személyes adatok védelméröl és a közérdekü adatok nyilvánosságáról [Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest], Magyar közlöny [MK.] 1992 no. 116, *available at* http://abiweb.obh.hu/dpc/index.htm; *Ireland*—Data Protection (Amendment) Act 2003 (Act No. 6/2003), *available at* http://www.dataprotection.ie/documents/legal/act2003.pdf; *Italy*—Codice in materia di protezione dei dati personali [Italian Personal Data Protection Code], Decreto Legislativo di 30 Jun 2003 [Legislative Decree of June 30, 2003], Gazz. Uff. July 29, 2003, n. 196, *unofficial English translation available at* http://www.privacy.it/privacycodeen.html; *Latvia*—Fizisko personu datu aizsardzības likums [Personal Data Protection Law of 2000], Vēstnesis 123/124 06.04.2000, *available in unofficial English translation at* http://www.dvi.gov.lv/eng/legislation/pdp/; *Lithuania*—Asmens duomenų teisinės apsaugos istatymas [Law on Legal Protection of Personal Data] (2003) 2003 m. sausio 21 d. Nr. IX-1296 (amending the Law of the Republic of Lithuania on Legal Protection of Personal Data), *available at* http://www.ada.lt/images/cms/File/pers.data.prot.law.pdf; *Luxembourg*—Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Law on the Protection of Persons with Regard to the Processing of Personal Information] (2002), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A-nº 91 p. 1836, *available at* http://www.legilux.public.lu/leg/a/archives/2002/0911308/0911308.pdf#page=2; *Malta*—Att dwar il-Protezzjoni u l-Privatezza tad-Data [Data Protection Act], 2001 Cap. 440. 1 (as amended), *available in unofficial English translation at* http://www.dataprotection.gov.mt/dbfile.aspx/DPA.pdf; *Netherlands*—Wet bescherming persoonsgegevens [Personal Data Protection Act] Stb. 2000, 302, *available in unofficial English translation at* http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple; *Poland*—Dziennik ustaw Rzeczypospolitej Polskiej [Act on the Protection of Personal Data] (1997) no. 133, item 833 (amended 2002), *available at* http://www.giodo.gov.pl/data/filemanager_en/61.pdf; *Portugal*—Lei da Protecção de Dados Pessoais [Law to Protect Personal Data] (1998), Diário da república 67/98, *available in unofficial English translation at* http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM; *Romania*—Law No. 677/2001 for the Protection of Persons Concerning the Processing of Personal Data and Free Circulation of Such Data, Monitorul Oficial 2001 no. 790, *available in unofficial English translation at* http://www.dataprotection.ro/images/PDF/Law677_en.pdf; *Slovakia*—Zbierka zákonov [Protection of Personal Data] č. 428/2002, Čiastka 167, strana 4403 (as amended), *available at* http://www.zbierka.sk/get.asp?rr=02&zz=02-z428, *unofficial English translation available at* http://www.dataprotection.gov.sk/buxusnew/docs/act_428.pdf; *Slovenia*—Zakon o varstvu osebnih podatkov [ZVOP-1] [Personal Data Protection Act] (2004), Uradni list Republike Slovenije [Official Gazette of the Republic of Slovenia], No. 86/2004 (partially annulled and corrected by the Information Commissioner Act, Uradni list Republike Slovenije, No. 113/2005), *unofficial English translation available at* http://www.ip-rs.si/index.php?id=162; *Spain*—Protección de Datos de Carácter Personal [Protection of Personal Information] B.O.E. 1999, 298 (amended 2003), *available at* http://civil.udg.es/normacivil/estatal/persona/PF/Lo15-99.htm, *unofficial English translation available at* https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf; *Sweden*—Personuppgiftslag [Personal Data Act] (Svensk författningssamling [SFS] 1998:204) (Swed.), *available in unofficial English translation at* http://www.sweden.gov.se/content/1/c6/01/

Macedonia,[15] Norway,[16] Russian Federation,[17] and Switzerland;[18]
- **Middle East/Africa**: Israel,[19] Mauritius,[20] Tunisia[21] and the U.A.E. (DIFC);[22] and

55/42/b451922d.pdf; *The United Kingdom*—Data Protection Act, 1998, c. 29 (amended 2000), *available at* http://www.opsi.gov.uk/acts/acts1998/19980029.htm.

10. Ligji 8517 of July 22, 1999 [On the Protection of Personal Data], Fletorja zyrtare Republikës të Shqipërisë, No. 23, Sep. 4, 1999, 839 (Alb.), *unofficial English translation available at* http://www.hidaa.gov.al/english/pub/l_8517.htm.

11. Law on the Protection of Personal Data, Official Gazette of Bosnia and Herzegovina 32/01, *unofficial English translation available at* http://www.privacyinternational.org/countries/bosnia/bosnia-dpa.html.

12. Law of June 12, 2003 [Act on Personal Data Protection], Narodne novine; sluzbeni list Republike Hrvatske 2003 no. 103, item 1364 (Croat.), *English translation available at* http://www.azop.hr/DOWNLOAD/2005/02/16/Croatian_Act_on_Personal_Data_Protection.pdf.

13. Act No. 77/2000 [Act on the Protection of Privacy as Regards the Processing of Personal Data] (as amended) (Ice.), *unofficial English translation available at* http://www.personuvernd.is/information-in-english/greinar//nr/438.

14. Datenschutzgesetz (DSG) [Data Protection Act], Liechtensteinisches Landesgesetzblatt [LGBI] 2002 no. 55 (Liech.), *available at* http://www.gesetze.li/get_pdf.jsp?PDF=2002055.pdf.

15. Law 12/94, Law on Personal Data Protection, Official Journal of Rep. of Macedonia 12/94, *available at* http://www.libertas-institut.com/de/MK/nationallaws/Law_on_personal_data_protection.pdf.

16. Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data, *English translation available at* http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf.

17. Federal law 152-FZ [Personal Data], Roz. gaz., Jul. 29, 2006, 4131, *available at* http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, *unofficial English translation available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1625/Privacy_Russia_White_Paper.pdf.

18. Loi fédérale sur la protection des données [LPD] [Federal Act on Data Protection], Recueil officiel des lois fédérales, June 19, 1992, RO 235.1, *available at* http://www.admin.ch/ch/f/rs/2/235.1.fr.pdf, *unofficial English translation available at* http://www.edoeb.admin.ch/org/00828/index.html?lang=en.

19. The Protection of Privacy Law (Amendment) 5745-1985, 1011 LSI 128 (1981-82) (Isr.).

20. Act 13 of 2004 [Data Protection Act], *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc.

21. Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004 (Tunis.), *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html.

22. Data Protection Law 2007, DIFC Law No. 1 of 2007, *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

• **North/South America**: Argentina,[23] Canada,[24] Chile,[25] Paraguay,[26] Peru,[27] the United States,[28] and Uruguay.[29]

Moreover, many other countries are debating or considering privacy legislation, including Barbados, Bolivia, Brazil, China, Costa Rica, Ecuador, India, Jordan, Lebanon, Malaysia, Mexico, Morocco, Pakistan, Panama, Singapore, South Africa, Sri Lanka, Tanzania, Thailand, Trinidad and Tobago, Turkey, the Ukraine, and Venezuela.

### B. *Local Compliance Obligations*

#### Europe

The twenty-seven Member States of the European Union (EU) have adopted comprehensive privacy laws based on the 1995 Data Protection Directive[30] (the "EU Directive"). The laws of the members of the European Economic Area (EEA), i.e., Iceland, Liechtenstein, and Norway, provide for very similar requirements, and the laws of neighboring countries such as Albania, Andorra, Bosnia and Herzegovina, Croatia, Macedonia, and Switzerland largely reflect the EU Directive. The Russian Federation has also recently adopted legislation that is similar to the EU Directive.

Personal information is very broadly defined as "any relating to an identified or identifiable natural person."[31] An identifiable person is

---

23. Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html.

24. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

25. Law 19628 [Protection of Personal Data], Diario Oficial, Aug. 28, 1999 (as amended) (Chile), *available at* http://www.sernac.cl/leyes/compendio/Leyes/Ley_19.628_sobre_Proteccion_de_la_Vida_Privada_y_Datos_Personales.pdf.

26. Ley 1969 [Private Information], Registro oficial de la República del Paraguay, Jan. 19, 2001 (as amended), *available at* http://www.informconf.com.py/informconf/site/downloads/Ley_1682.pdf.

27. Law No. 27489, Centrales Privadas de Información de Riesgo (CEPIRS) (Peru), *available at* https://www.agpd.es/upload/C.5)%20Ley%20peruana%20de%20protecci%F3n%20de%20datos.pdf.

28. 15 U.S.C. §§ 6801–6809 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-91, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

29. Ley 17,838 [Protection of Personal Information in Commercial Sources and Recognizing the Right of Habeas Data Action], D.O. 1, Oct/004, No. 26599 (Uru.), *available at* http://www.parlamento.gub.uy/Leyes/Ley17838.htm.

30. Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31.

31. *Id.* at 138, art. 2(a).

one who can be identified, directly or indirectly, taking account of all means that are likely to be reasonably used either by the controller or by any other person to identify the said person.[32]

According to the EU Directive, personal information can only be processed when one of the following exceptions is met: consent from the individual; contractual necessity (that is, data may be used if necessary for the performance of the contract with the individual); compliance with (local) legal obligations; or the legitimate interests of the entity collecting the personal information outweigh the privacy interests of the individual.

### Asia, Americas, Middle East, and Africa

Unlike in Europe, the data privacy laws elsewhere around the world vary more widely from country to country, particularly with respect to the processing of certain types of personal information and database registration.

For example, Hong Kong, Japan, and New Zealand regulate the processing of personal information in all sectors; Australia regulates all sectors of the economy but exempts much of employee data from requirements of its Act; Taiwan and, to some extent, Korea regulate only selected sectors of the economy.[33]

In the Americas, only a few countries have adopted omnibus data protection laws. Argentina has adopted legislation that is similar to the EU Directive, but it only regulates the collection, use, and disclosure of personal information contained in databases that are shared.[34] Chile regulates the processing and use of personal information by the public and private sectors, and has specific provisions that pertain to the use of financial, commercial and banking data, as well as the use of informa-

---

32. *Id.* at 133, rec. 26.

33. *See* Personal Data (Privacy) Ordinance, (1995) Cap. 486. (H.K.), *available at* http://www.pcpd.org.hk/english/ordinance/down.html; Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *unofficial English translation available at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf; Privacy Act, 1993 S.N.Z. No. 28, *available at* http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes; Privacy Act 1988, 1988 (as amended), *available at* http://www.privacy.gov.au/publications/privacy88130706.pdf; Computer-Processed Personal Data Protection Law (1995), *unofficial English translation available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf; Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (as amended), *unofficial English translation available at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

34. Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html.

tion by government agencies.[35] Canada regulates the collection, use, and disclosure of personal information by all private sector businesses in the course of their commercial activities, except in provinces that have enacted legislation deemed to be substantially similar to federal law.[36] Canada's federal law does not generally apply to employee information unless the business is in the telecommunications, broadcasting, inter-provincial or international transportation, aviation, banking, or nuclear energy sectors.[37]

In Africa, only Tunisia and Mauritius have adopted comprehensive privacy laws. While the Tunisian law follows the EU Directive, it imposes even stricter requirements for processing information and in particular for cross-border transfers.[38] In Mauritius, both notice and opt-in consent are required to collect, use, and transfer personal information unless the information is required for the performance of the contract.[39]

The Middle East, Israel, and the United Arab Emirates (DIFC) require DPA authorization, contractual safeguards and/or opt-in consent to process and transfer personal information outside the respective countries.[40]

### C. *Rules for Cross-Border Data Transfers*

Most if not all of the countries that have enacted privacy laws have rules that regulate the transfer of personal information. Transfer covers any sharing, transmission or disclosure of, providing access to, or otherwise making available, information to third parties. Third parties include corporate affiliates as well as government authorities. Some countries do impose specific restrictions on cross-border trans-

35. Law 19628 [Protection of Personal Data], Diario Oficial, Aug. 28, 1999 (as amended) (Chile), *available at* http://www.sernac.cl/leyes/compendio/Leyes/Ley_19.628_sobre_Proteccion_de_la_Vida_Privada_y_Datos_Personales.pdf.

36. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

37. *Id.*

38. Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004, at ch. 2-4, *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html.

39. Act 13 of 2004 [Data Protection Act] § 22, *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc.

40. *See* The Protection of Privacy Law (Amendment), 5745-1985, 1011 LSI 128 (1981-82) (Isr.); Data Protection Law 2007, DIFC Law No. 1 of 2007 (U.A.E.), *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

fers; alternatively, others require the organization collecting the information to impose certain requirements on the recipient entity, such as contractual undertakings.

## Countries That Restrict Cross-Border Data Transfers

### *European Union*

The transfer of personal information to countries outside the EEA is prohibited unless the receiving countries provide an "adequate" level of protection, as determined by the European Commission or national DPAs, or the transfer satisfies one of the exceptions contained in the law. Any business operating in the EU that fails to meet these conditions may incur substantial legal liability. To date, the European Commission has deemed adequate the laws of Argentina,[41] Canada,[42] Guernsey,[43] the Isle of Man,[44] and Switzerland,[45] as well as the U.S. Safe Harbor Framework.[46]

The laws of the EU and its Member States also provide several exceptions that allow for international transfers of personal information where there has been no determination of adequacy for the receiving jurisdiction. These exceptions include situations where: (i) the individual has given his or her unambiguous consent; (ii) the transfer is necessary for the performance of the contract with the individual, or concluded in the interest of the individual; or (iii) the transfer is necessary for the defense of a legal claim.[47] EU privacy regulators do, however, interpret these exceptions narrowly.

---

41. *See* Commission Decision No. 1731/2003 of 30 June 2003, art. 1, 2003 O.J. (L 168) 5 (EC), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf.

42. *See* Commission Decision No. 2/2002 of 20 Dec. 2001, art. 1, 2002 O.J. (L 2) 13 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_002/l_00220020104en00130016.pdf.

43. *See* Commission Decision No. 821/2003 of 21 Nov. 2003, art. 1, 2003 O.J. (L 308) 27 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_308/l_30820031125en00270028.pdf.

44. *See* Commission Decision No. 411/2004 of 28 Apr. 2004, art. 1, 2004 O.J. (L 152) 48 (EC) (as corrected by Corrigendum to Commission Decision No. 411/2004, 2004 O.J. (L 208) 47), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0411R(01):EN:HTML.

45. *See* Commission Decision No. 518/2000 of 26 July 2000, art. 1, 2000 O.J. (L 215) 1 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00010003.pdf.

46. *See* Commission Decision No. 520/2000 of 26 July 2000, art. 1, 2000 O.J. (L 215) 7 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00070047.pdf.

47. Council Directive 95/46, art. 26, 1995 O.J. (L 281) 31 (EU), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

Alternatively, a business may transfer personal information to a recipient country that does not provide adequate protection if it ensures that "adequate safeguards" are in place when the information is to be transferred. Traditionally, this entails the establishment of contracts between the entity sending the data (the "exporter") and the receiving entity (the "importer"). Approval of most Member State DPAs is required if individually negotiated contacts ("ad hoc contracts") are used. Contracts that incorporate certain standard contractual clauses approved by the European Commission ("Standard Clauses")[48] do not require DPA approval.

When Standard Clauses were introduced, it was hoped that because they provided one form of contract useable in all EU Member States and required no approval by individual DPAs, they would create workable and substantially more streamlined international data transfers. Unfortunately, it appears that the drawbacks of Standard Clauses may outweigh their advantages. Besides entailing burdensome compliance requirements, Standard Clauses require that all individuals to whom the information relates be made third party beneficiaries of the agreement between the exporter and the importer, providing individuals with a direct cause of action and imposing liabilities on both the exporter and the importer. Further, an importer may generally only provide the information to third parties if those third parties are either subject to an adequacy finding, executed the Standard Clauses, or consent is obtained from each and every individual whose information will be transferred. Only in environments where the data flow is stable and fairly limited would such limitations be practical.

In addition, both ad hoc contracts and Standard Clauses can be very difficult to administer. Data flows do not follow neat or well-established paths, but travel along multiple paths through a multitude of channels, through e-mail exchange, access to databases, and intranets. Global organizations have complex organizational structures that can change frequently. Unless regularly revised—at considerable expense—

48. *See* Commission Decision No. 497/2001 of 15 June 2001, 2001 O.J. (L 181) 19 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_181/l_18120010704en00190031.pdf. The European Commission has also adopted standard contractual clauses for the transfer of personal information to third countries from a data controller to a data processor. *See* Commission Decision No. 16/2002 of 27 December 2001, 2002 O.J. (L 6) 52 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_006/l_00620020110en00520062.pdf. In 2004, the European Commission amended its 2001 Decision and added a new set of standard contractual clauses. *See* Commission Decision No. 915/2004 of 27 Dec. 2004, 2004 O.J. (L 385) 74, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf.

contracts will not be able to reflect the changes in usage of information in organizations, as required under the contract regime.

*Argentina, Australia, Mauritius, Tunisia and the United Arab Emirates (U.A.E.)*[49]

Like the EU, Argentina also prohibits transfers to countries without "adequate" data protection, but because Argentina has not issued any adequacy findings, organizations must rely on contracts or the consents of individuals. Similarly, Mauritius, Tunisia, and the U.A.E. restrict transfers to countries that do not provide "adequate protection" and require opt-in consent and/or a DPA permit or authorization. In addition, Australia permits organizations to transfer personal information to a recipient in a foreign country only if it is subject to a "substantially similar" privacy regime; however, organizations must determine for themselves what constitutes "substantially similar."

Countries that Impose Accountability Obligations

*Canada & Japan*[50]

In contrast, the laws in Canada and Japan do not distinguish between cross-border and domestic transfers to third parties. They apply the same rules to all third parties, regardless of their location. Third parties include affiliates, subsidiaries and parent organizations. In brief, these laws require organizations to remain accountable for protecting personal information transferred to third parties. This means, in the case of Canada, that organizations that hold personal information and transfer it to third parties must include a privacy protection clause in

49. *See* Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html; Privacy Act, 1988 (as amended) (Austl.), *available at* http://www.privacy.gov.au/publications/privacy88130706.pdf; Act 13 of 2004 [Data Protection Act], *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc (Mauritius); Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004 (Tunis.), *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html; Data Protection Law 2007, DIFC Law No. 1 of 2007 (U.A.E.), *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

50. *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf; Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *unofficial English translation available at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

contracts to guarantee that the third party provides the same level of protection as does the organization that originally collected the personal information. In Japan, organizations must establish contracts with service providers and other third parties that contain specific data security provisions.

### Countries that Impose Consent or Other Requirements

*Korea & Taiwan*[51]

Cross-border agreements to transfer personal information to third parties outside of Korea and Taiwan are not required; however, Korea does require opt-in consent to transfer personal information, while Taiwan requires that entities subject to the privacy law obtain a license to process and transfer personal information abroad. At present, the Taiwanese law is limited to certain private entities such as financial, securities, insurance, mass media, and telecommunications companies but there is a new privacy law pending before the Taiwanese legislature, which, if enacted, would cover companies in all industry sectors. Korea also has more than one draft privacy law pending but the leading proposal does not specify the rules for cross-border transfers; instead, it directs the government to develop a policy in the future to address this issue.

## III. Assessing the Current Options for Cross-Border Transfers

Most businesses that wish to transfer personal information currently use one of three options: obtain the consent of the individual concerned; establish a contract between the entities exchanging the information; or if transferring from the EU, limit data flows to jurisdictions where there is an "adequacy" finding such as the U.S. Safe Harbor regime.[52]

---

51. *See* Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (as amended) (Korea), *unofficial English translation available at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html [herinafter PICNU]; The Computer-Processed Personal Data Protection Law (1995) (as amended) (Taiwan), *unofficial English translation available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf.

52. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 56,534 (Sept. 19, 2000); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (Jul. 24, 2000). *See also* Safe Harbor, http://www.export.gov/safeharbor/doc_safeharbor_index.asp (last visited May 13, 2007).

In some situations, however, organizations may be unable to rely on the use of the three options above to make their international data transfers legal. For example, many banks function internationally through branches rather than through separate legal entities; therefore, contracts generally cannot be used when the same legal entity would be on both sides of the contract. Likewise, only organizations subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are currently eligible to join the Safe Harbor, thereby excluding participation by financial services institutions and telecommunications common carriers that are subject to the jurisdiction of other regulatory agencies. In addition, the Safe Harbor principles may only be used for data transfers from the EU to the United States, so their applicability is limited. Moreover, in certain jurisdictions, and in most EU Member States, consent is strongly disfavored particularly when it involves the transfer of employee data because there is a view that consent cannot be given "freely" within the context of the employment relationship or in exchange for goods or services.[53] Also, if consent is required and a customer does not consent, then the organization may not be able to centralize its procurement functions to centrally ship the goods to all of its customers.

Despite the fact that each privacy law provides some means for transferring information, the divergent laws of the sixty or more countries make it virtually impossible for businesses to select a single safeguard to protect the data as they transfer data from one country to another. That is certainly the case in the EU,[54] where businesses must analyze and satisfy twenty-seven different standards for transferring information outside the EU, thus defeating the harmonizing intent of the EU Directive.[55] The European Commission acknowledged this difficulty in its first report on the implementation of the EU Directive, and stated: "more work is needed on the simplification of the condi-

53. Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 Oct. 1995, Art. 29 Working Party Doc. WP 114 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

54. The EU Directive sets a floor for the Member States' legislation, and in some instances it may also set a ceiling. It does not, however, prohibit divergences among Member State laws. *See* Parliament and Council Directive No. 95/46 of 24 Oct. 1995, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

55. The only uniform method of complying across the EU is with standard clauses/model contracts. If a global organization, however, is elected to utilize model contracts to transfer data among affiliates, it is perfectly possible that it would have to enter into hundreds of contracts which would be administratively burdensome and complex.

tions for international transfers."[56] Thus, there is no standard means to comply with the cross-border transfer obligations even among the twenty-seven EU Member States, let alone among the sixty-plus countries with data protection laws that restrict cross-border transfers.

### A. *Consent*

As mentioned above, organizations can legitimize the transfer of personal information from one country to another by obtaining the consent of the individual to transfer his or her personal information. In most EU Member States, for example, consent to transfer personal information to a country that has not been deemed adequate by the EU would need to be affirmative (opt-in) consent. Similarly, affirmative consent is usually required in countries such as Argentina, Korea, Mauritius, and the U.A.E. (DIFC). In other countries such as Australia and Canada, opt-out consent may be sufficient. Regardless of the form of consent required, almost all jurisdictions require that such consent be informed and as such, notice would need to be provided.

At first glance, consent appears likely to be an organization's simplest option for legitimizing its data processing practices as it could be drafted to cover all uses of the data. Authorizations also can be made relatively consistent across all countries, thereby enabling organizations to use a uniform, worldwide approach to data transfers.

This method, however, poses significant issues for an organization, particularly in the employment context. Whether "consent" may be freely given in the context of an employment relationship has been the subject of much debate among the EU Member States. Several EU Member States maintain the view that an existing employee cannot freely give consent. Moreover, the Working Party 29, the assembly of all twenty-seven EU DPAs, takes the view that:

> where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal information, it is misleading if the employer seeks to legitimize this processing through consent. Reliance on consent should therefore be confined to cases where the worker has a genuine

56. *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 19, COM (2003) 265 final (Feb. 24, 2004), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

> free choice and is subsequently able to withdraw the consent without detriment.[57]

Similarly, the U.K. Information Commissioner recently issued revised guidance on international data transfers confirming that valid consent means that the data subject must have a real opportunity to withhold their consent without suffering any penalty.[58] Accordingly, in the EU Member States that take this position, an employer who relies on consent to legitimize data processing in the employee context may face significant risks and should consider other (additional) possibilities for transferring information.

Also, consent may provide at best only a short-lived solution for businesses because employees or customers may withdraw their consent at any time.

The advantages and disadvantages of a consent-based approach to cross-border data transfers can be summarized as follows:

*Pros:*

- *Choice:* Use of consent, particularly opt-in consent, is the most direct and, in some instances, the least risky means of legitimizing cross-border data transfers of personal information as the entities sending and receiving the data assume only the obligations delineated in the notice that forms the basis of the consent.
- *Consistency:* Consent can be relatively consistent across all countries.
- *Liability:* The receiving entity does not have to take on any liability for its information processing practices.
- *Audit:* Consent does not expose the entities receiving information to audit by the data protection authorities of the exporting country.
- *Compliance Burdens:* Consent is required in many instances to satisfy local compliance obligations. In Argentina, the EU Member States, Korea, Mauritius, Tunisia and the U.A.E., for example, any processing of "sensitive" data (i.e., specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex

57. Opinion 8/2001 on the Processing of Personal Information in the Employment Context of 13 Sept., 2001, at 23, Article 29 Working Party Doc. WP 48 (2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

58. Info. Comm'r's Office, Data Protection Guidelines: International Transfers of Information General Advice on how to Comply with the Eighth Data Protection Principle, at 9, a*vailable at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/general_advice_on_how_to_comply_with_8th_data_protection_principle.pdf.

life of the individual) usually requires consent. Also, in certain countries there are additional categories of sensitive information such as performance appraisals, criminal background checks and credit checks. Thus, adding a consent to transfer the data across borders can be relatively easy.

*Cons:*

- *Time and Expense:* Obtaining opt-in consent from all individuals (customers, employees, independent contractors and employees of vendors) is time consuming and costly. Obtaining consent to reflect changes in business needs may prove difficult.
- *Validity of Consent:* Several EU DPAs and in particular the Working Party have expressed doubt that truly voluntary consent can ever be given by employees and serve as a basis for international transfers.
- *Individual Choice*. Some individuals may refuse to provide consent and there can be no penalty associated with such a decision. Individuals are also permitted to withdraw their consent at any time. While this ability to repudiate consent strengthens the argument that individuals have genuine free choice, it might weaken the effectiveness of consent.
- *Form Requirements:* Some countries including Argentina, Germany, Korea, Mauritius, Tunisia and the U.A.E. require consent to be given in writing.
- *Adequacy Statement:* If an organization in the EU wants to transfer personal information to a country that has data protection that has not been deemed "adequate" by the EU, it is required to include a sentence in the notice to individuals that their information will be transferred to a country that may not ensure "adequate" privacy, which may discourage some individuals from providing consent.

### B. *Contracts*

Use of contracts between the entity transmitting information and the recipient is another legitimate means by which to transfer personal information from one jurisdiction to another. In the EU, the European Commission has approved different sets of model contracts ("Standard Clauses").[59] When Standard Clauses were introduced it was hoped that

59. The Commission Decision No. 497/2001 of 15 June 2001, 2001 O.J. (L 181) 19, on standard contractual clauses for the transfer of personal information to third countries, under Directive 95/46/EC (2001/497/EC), incorporates the standard terms suggested by the European Commission for transfers to so-called controllers; Commission Decision No. 915/2004 of 27 December 2004, 2004 O.J. (L 385) 74, amended Decision 2001/497/EC as regards the introduc-

because they provided one form of contract useable in all EU Member States without further scrutiny by DPAs, they would allow for workable and substantially more streamlined international data transfers. Unfortunately, however, it appears that the drawbacks of Standard Clauses may outweigh their advantages.[60] Contracts that derogate from Standard Clauses require approval from most EU DPAs, which is a costly and lengthy process.

In Japan, there is no pre-approved model contract, but the Guidelines published by the Financial Services Administration contain detailed guidance relating to the provisions that should be contained in a contract with a service provider (either in Japan or in any other country).[61] Similarly, in Korea, there are no pre-approved clauses but entities and their agents are required to take necessary security measures, including technical and administrative measures to protect personal information and procedures to handle complaints and disputes.[62] In Argentina and the U.A.E., the laws explicitly, in the case of the former, and implicitly in the case of the latter, provide for the use of contracts as a way to legally transfer data outside the country but clauses have yet to be developed by the DPA.[63]

The main disadvantages of contracts are that they are administratively burdensome and only work in environments where the informa-

---

tion of an alternative set of standard contractual clauses for the transfer of personal information to third countries; and on 27 December 2001, the European Commission adopted Commission Decision (EC) No. 16/2002 of 27 December 2001, 2002 O.J. (L 6) 52, on standard contractual clauses for the transfer of personal information to processors established in third countries, under Directive 95/46/EC.

60. Besides entailing burdensome compliance requirements, the Standard Clauses require that individuals to whom the information relates are to be made third-party beneficiaries of the agreement, providing individuals with a direct cause of action and impose liabilities on both the exporter and the importer. *See* Commission Decision No. 915/2004 of 27 December 2004, 2004 O.J. (L 385) 74, 79. Further, an entity importing EU data may generally only provide the information to third parties if those third parties are subject to an adequacy finding, execute model contract clauses or consent is obtained by each and every individual. *Id.* at 78-79.

61. [Japanese Financial Services Administration General Guidelines on the Protection of Personal Information in the Financial Services Area], *available at* http://www.fsa.go.jp/common/law/kj-hogo/01.pdf; [Japanese Financial Services Administration Guidelines on the Security Measures for the Protection of Personal Information in the Financial Services Sector], *available at* http://www.fsa.go.jp/common/law/kj-hogo/04.pdf.

62. *See* PICNU, *supra* note 51.

63. *See* Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html; Data Protection Law 2007, DIFC Law No. 1 of 2007, *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

tion flow is stable and fairly limited. However, for most businesses, information flows do not follow neat or well-established paths, but travel along multiple paths through a multitude of channels, through e-mail exchange, access to databases, and intranets. Global organizations have complex organizational structures that can change frequently. Unless regularly revised—at considerable expense—contracts will not be able to reflect the changes in usage of information in organizations, as required under the contract regime.

The advantages and disadvantages of a contractual approach to cross-border data transfers can be summarized as follows:

*Pros:*

- *Legal Certainty.* In the EU, contracts have been used for almost 20 years. Regulators are familiar with them, and therefore contracts, and the Standard Clauses, can provide a great deal of legal certainty.
- *Individual Consent Not Required.* The organization can put contracts in place without seeking consent from each relevant individual.
- *Tailored Solution.* Contracts can reflect the data that is being moved and the activities that are being carried out in relation to that data.
- *Involvement of the DPAs.* Contracts do not require approval from DPAs in most countries other than the EU Member States. In the EU, in theory, Standard Clauses do not require prior authorization by individual DPAs either. (In practice, however, almost half of the EU DPAs do require businesses to file using the Standard Clauses "as an administrative formality" and obtain authorization for data transfers.)

*Cons:*

- *Administrative Difficulties:* Contracts can be difficult to administer as they are static documents and must be updated as organizational, technical and other changes are implemented and then reauthorized either by new signatures or new unilateral undertakings. If an organization relies on the use of ad hoc contracts, it will need to continue to track data received from the Member States by country of origin to ensure that the data is handled in compliance with the appropriate Member State data protection requirements.
- *Involvement of DPAs:* In the EU, any contract derogating from the Standard Clauses requires approval, which generally takes a minimum of one to two months and may take longer if the DPA has questions about the transfer or the requisite forms were not completed properly in the first instance. Subsequent additional approvals also may be required if changes are made in the processing or type of personal information collected.
- While prior approvals are not required for Standard Clauses,

almost half of the EU Member States (i.e., Denmark and the Netherlands) require that such contracts be registered prior to the contract being relied on as a cross-border mechanism. Although the DPAs are technically precluded from requesting changes to the terms of the Standard Clauses, a DPA can request amendments and additions to the appendices.

- *Non-EU Jurisdictions.* Standard Clauses will not necessarily meet all of the cross-border requirements in non-EU jurisdictions, such as Japan, Australia and Argentina; at the same time, an organization may have to provide protections greater than those required in non-EU jurisdictions.

### C. *Adequacy Decisions*

Another option for transferring data is to rely on an adequacy decision. As mentioned earlier, the EU has issued a limited number of adequacy decisions, including one in 1998 for the U.S. Safe Harbor Privacy Principles ("Safe Harbor"), which provides an alternative basis for data transfers to the United States.

For a U.S. organization to be eligible for the Safe Harbor, it must be subject to the jurisdiction of a "government body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices. . .in case of noncompliance with the [Safe Harbor] Principles."[64] At present, only the FTC (under section 5 of the Federal Trade Commission Act ("FTC Act")) and the DOT (under 49 U.S.C. § 41712, which covers air carriers)[65] are recognized by the European Commission as satisfying this requirement. Therefore, only organizations subject to the jurisdiction of either of those two agencies are eligible to join the Safe Harbor.[66] Thus, financial institutions, telecommunications, and several other regulated entities are not able to utilize the Safe Harbor.

The Safe Harbor provides *one* privacy regime for all EU personal information that is transferred to the United States. It eliminates the

64. Commission Decision No. 518/2000 of 26 July 2000, art. 1(2)(b), 2000 O.J. (L 215) 1 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00010003.pdf.

65. The EU wanted to ensure that a government body (state or federal) would provide Safe Harbor enforcement in the event that self-regulatory mechanisms did not operate appropriately. To date, only the FTC and DOT have agreed to enforce the Safe Harbor.

66. Financial services institutions that are subject to the jurisdiction of the banking regulatory agencies and telecommunications common carriers (which are subject to the jurisdiction of the Federal Communications Commission) are not eligible for the Safe Harbor at this time.

need for prior approvals or makes them automatic. As a result, the Safe Harbor can provide a streamlined approach for data transfers from the EU and can make those transfers less expensive and less onerous. In addition, the Safe Harbor requirements are interpreted in accordance with U.S. law, which imputes a reasonableness standard to the Safe Harbor's terms. The Safe Harbor, however, only applies to transfers of data from the EU to the U.S. and, thus, it is not a global solution. The same is true for the other adequacy decisions issued by the EU. The rest of the world is left out.

*Pros:*

- *Consistency*. Reliance on an adequacy decision would harmonize transfers of personal information between adequate countries, subjecting such information to a common privacy regime.
- *Compliance Burden*. Transfers to countries or entities that are subject to an adequacy decision eliminate the need for prior approvals from EU DPAs or make such approval automatic.
- *Familiarity*. With respect to the Safe Harbor, the Safe Harbor more clearly reflects the U.S. approach to privacy and to some extent the moderate requirements of the EU Directive.
- *Public Relations*. Referring to the Safe Harbor or transferring to a country with adequate data protection can have a positive PR effect.

*Cons:*

- *Limited Applicability*. Adequacy decisions are only applicable to individual countries or, in the case of the Safe Harbor, to organizations that certify to the Safe Harbor. Therefore, these authorizations may only be used for transfers between the EU and the country subject to the particular authorization. Also, in the case of the Safe Harbor, it is not available to financial institutions or providers or telecommunications services.
- *Involvement of the DPAs*. For the Safe Harbor to cover an organization's employment data, the organization must agree to cooperate with the EU DPAs as the complaint resolution mechanism.
- *Compliance Burden*. For the Safe Harbor, organizations have to recertify to the Safe Harbor every year.

## IV. Problems with the Current Compliance Alternatives

Unfortunately, the existing patchwork of cross-border rules has done little to provide real protection for individuals' personal information. At the same time, these cross-border rules, by virtue of the fact that they are making such transfers more difficult and costly, are adversely affecting the quality and choice of products and services that can be offered to consumers on a global basis.

### A. *Illusory Protection for Individuals*

Individuals and, in particular, consumers, are ill served in the networked economy because their personal information is not protected in a uniform and consistent manner. If a problem arises, such as, for example, they are a victim of identity theft or their personal information is shared with third parties against their wishes, the consumer must determine who is at fault, what laws apply, what his or her rights are with respect to the standard of protection in that jurisdiction, and who needs to be contacted to have the problem resolved. The answer to these questions may be complex given the multi-jurisdictional nature of data flows and the potential applicability of one or more sets of national rules. Even after these questions are answered, consumers may not be able to resolve the problem depending on how well law is enforced in a given country (or countries). Differences in language may further complicate the matter. At the same time, consumers depend on the international flow of information because it gives them access to a wider array of information as well as goods and services at lower prices, and enables them to receive customer service twenty-four hours per day.

The following are some examples that illustrate the illusive nature of the privacy protections afforded to consumers by the current international regime.

#### No effective recourse mechanism

*A U.S. consumer purchases a product over the Internet from a German company that is an affiliate of a U.S. company. The German company fails to properly secure the personal information of the individual and the U.S. consumer becomes the subject of identity theft. What recourse does the U.S. consumer have against the German company?*

The FTC has no jurisdiction over a German company doing business in Germany.[67] The U.S. affiliate has no legal authority to compel the German affiliate to take any particular activities. The U.S. consumer (if he or she can speak German) could call and file a complaint with the German DPA, but it is unlikely that the German DPA will take any action based on an issued raised by a U.S. consumer. Thus the U.S. consumer effectively has no recourse.

---

67. The FTC's enforcement authority is limited to those organizations covered by Section 5 of the FTC Act. *See* 15 U.S.C. §§ 41-58 (2000).

### Privacy breach occurs but no privacy law is violated

*A U.S. consumer is on vacation in Europe. The consumer asks the hotel where he is staying to make reservations for him at two other associated hotels in Asia and Latin America. At the consumer's request (*e.g.*, with his consent), the European hotel transfers personal information about the consumer to the other hotels such as his name, address, and meal preferences, which reveal his religion and credit card information. The hotel in Asia, located in a country that has a privacy law that contains very limited security obligations, fails to properly protect the information and the consumer becomes a victim of identity theft. In addition, the hotel in Latin America, located in a country that has no privacy laws in place, may sell its customer information to data brokers and the information is then used for other purposes. Who is at fault for these privacy violations? What rights and recourse does the consumer have?*

In this scenario, the consumer has no rights or guarantees that his personal information will be protected because he consented to the transfer. The European hotel did not violate European privacy laws because it transferred the information with the consent of the individual. It is not legally responsible for any misuse of that information by other hotels in its international chain. The Asian hotel is also not liable for any damages because it has minimal security safeguards in place that technically satisfy the local requirements (although they may fall far short of security requirements in jurisdictions with more rigorous standards). The hotel in Latin America is not liable because it is located in a country that has no privacy laws and therefore is also not limited to how it may use the data. Thus, the consumer has no recourse.

### Unable to determine who is at fault

*A U.S. consumer uses a credit card to purchase a computer product from a U.S. company. The customer's personal information will need to be shared with two different affiliates within the company: one for warranty purposes and the other for customer service purposes. These affiliates are located outside the U.S. The company's U.S. privacy policy discloses that customer information will be shared with affiliates of the organization for those purposes and the U.S. company will safeguard the personal information that it processes in the U.S. It refers the customer to the privacy policies of its affiliates for information about how those entities protect customer information. A hacker then breaks into the company's global computer system and steals customer information. Which entity is at fault? What rights and recourse does the consumer have?*

It may be extremely difficult, even with superb computer forensics, to determine at precisely which point in the global network a hacker found entry. If it cannot be determined where in the system the

hacking occurred, or if the hacker was from a completely different country and the information was collected in transmission between two affiliated entities, then it will be impossible to assign fault or responsibility for the security breach. Given that none of the affiliates will be responsible, each can avoid liability and the consumer is left completely unprotected and with no viable recourse mechanism.

Delayed or cumbersome access to customer service

*A U.S. consumer purchases a computer from a U.S. company and has trouble setting it up. Over a one-week period, the consumer has to call the company's customer service support hotline at three different times of the day. Calls to the hotline between 9:00 a.m. and 9:00 p.m. EST are handled by the U.S. company, between 9:00 p.m. and 3:00 a.m. EST by its Japanese affiliate, and between 3:00 a.m. and 9:00 a.m. EST by its Irish affiliate.*[68]

*In order to provide this service and comply with the various national privacy laws, the company must either require the customer to repeat the same information about his problem (and provide service warranty information) every time he calls customer service or, to avoid such repetition, put into place four different contracts that will enable information to be shared among the affiliates. If the company opts for the latter approach, then the Irish affiliate must enter into a contract with the Japanese affiliate to transfer the data to it; the Irish affiliate must also enter into a contract with the U.S. affiliate or the U.S. affiliate must certify to the Safe Harbor. The Japanese entity must also enter into contracts with the Irish and the U.S. affiliates.*

*Even with such contracts in place, the customer service representatives will still need to provide the customer with two verbal privacy notices before they can begin to address his problem. For example, the customer calls at 6:00 a.m. EST time and the Irish affiliate receives the call. In order to access the customer's purchase information to find out, for example, whether the customer purchased a service contract, the Irish customer service representative must provide a verbal privacy notice to the individual, describing the types of information collected, the purposes of the collection, with whom the information will be shared, the security measures taken to protect the information, the methods of keeping the data accurate, and the process by which the personal information can be corrected. The Irish customer service representative then collects additional information from the U.S. customer (*i.e.*, the nature of the problem, information about the printer*

68. As it is prohibitively expensive and extremely difficult to find qualified individuals to staff a customer service department in the United States twenty-four hours per day, the U.S. company has opted to set up customer service centers in other parts of the world so that they can retain qualified individuals and provide twenty-four-hour customer service.

*that is being attached to the computer and the individual's phone number for a call back). The next day, the customer has an additional problem at 11:00 p.m. EST and the call is answered by the Japanese affiliate. The Japanese customer service representative will need all of the information that has been collected to-date and may collect additional personal information. But, before the Japanese customer service representative can access the account information, he or she must provide a verbal privacy notice similar to that provided by the Irish representative. The customer then calls a third time at 11:00 a.m. EST and speaks with a U.S. customer services representative. Depending on the U.S. company's privacy policy, the customer could conceivably hear a third privacy notice.*

The customer will be extremely frustrated that he must hear the privacy notice each time and will likely be equally frustrated that he must provide his relevant data each time a customer service phone call is placed. For the company, the costs associated with establishing this type of customer service system is enormous. For example, an organization with offices in 15 EU Member States, Japan, the U.S., and Canada that wants to have a centralized customer data base to provide global customer services to its clients, would be required to enter into 108 separate contracts among the corporate affiliates and to have 18 different privacy notices. The cost of compliance is so administratively burdensome and so expensive that it may be easier simply to not provide twenty-four-hour customer service.

### Diminished services and choice

*A U.S. consumer wants to travel to Argentina and calls a U.S. travel agency. The U.S. consumer is not interested in the travel agency's group travel packages and instead wants a customized itinerary for independent travel through Argentina. Because the U.S. travel agency does not have all of the information requested by the consumer, it wishes to provide the consumer with the name and address of a travel agent from its affiliated travel agency in Argentina. What has to happen for the business contact information to be provided to the U.S. consumer?*

In order for the U.S. travel agent to provide the business contact information of the Argentinean travel agent to the customer, the affiliated Argentinean travel agency would be required to give a notice to the individual Argentinean travel agent informing him or her that personal information is going to be collected and sent to the U.S. so that a referral can be made, that U.S. travel agents will have access to the information and that the information may be provided to customers in the U.S. In addition, it is likely that the individual travel agent in Argentina will have to consent to the provisions in the notice. Thus, the

U.S. and Argentinean travel agencies would need to keep track of and ensure that each relevant travel agent in Argentina receives a notice and consents to the collection, use and disclosure of his or her business contact information. In addition, if any one of the Argentinean travel agents withdrew his or her consent, the U.S. travel agent would have to be informed and the information relating to that travel agent would have to be removed from the database maintained by the U.S. travel agency. As a result, the U.S. and Argentinean travel agencies might decide that it was too difficult to manage the notices and consents. Under those circumstances, the U.S. travel agent could tell the consumer that no other information was available or provide the main telephone number and address of the Argentinean agency without providing the name of an individual travel agent. The travel agency may then lose the potential business if the consumer looks for another travel agency that can help locally. Alternatively, if the consumer decides to call the Argentinean agency directly, it might take several calls to identify the appropriate agent who can assist, an experience that will likely frustrate and annoy the consumer and undermine the overall business relationship with that consumer.

### B. *Regulatory Burden for Organizations*

Businesses are also ill served by this patchwork regime. Businesses are eager to offer consumers a wide array of goods and services at competitive prices and provide customer service 24 hours per day. To do that, they need to manage their global operations in the most cost effective way possible which generally means that they will centralize certain functions throughout the entire organization (e.g., one affiliate may be responsible for processing all of the organization's human resources data, another would maintain the marketing/sales database, and a third affiliate may be responsible for managing the vendor database). As a result, the organization will need to transfer both non-personal information, such as inventory data, as well as personal information, such as customer, vendor and employee data, to their operations around the world. While such transfers are necessary to manage the business in an efficient manner, they also permit the organization to offer, for example, customer service to consumers twenty-four hours per day, by relying on customer service representatives from different time zones to "come online" at different times to assist customers who may be located halfway around the world. To be effective and convenient for the customer, these customer service representatives must have access to the organization's databases containing customer information such as the customer's credit, purchase and repair records.

They also need access to the organization's employee data so they can, for example, direct any required follow-up service to the correct office or dispatch the appropriate repair technician.

While organizations are striving to meet consumer demands for convenience and lower prices for goods and services, they are facing an increasingly complex burden to comply with both local and cross-border privacy rules in more than sixty different jurisdictions around the world.[69] In particular, as discussed below, cross-border rules are having the following impact on business operations.

### Greater administrative burden

Managing the contracts among affiliated entities or obtaining workers' consents imposes an enormous administrative burden on companies. Any given organization may need to manage hundreds or thousands of contracts depending on how many affiliates the organization has at the time. In addition, anytime there is an organizational change among the parties to the contract (e.g., a different affiliate is assigned responsibility for processing human resources data for a given affiliate or possibly on an enterprise-wide basis), new contracts will need to be negotiated. Or, if the organization relies on consents, then it must permit the individual to withdraw consent at anytime and keep track of those preferences.

### Increased jurisdictional conflicts

Reliance on contracts may increase the chances for jurisdictional conflicts of law, particularly with the advent of the Internet. To run a global business and to transfer information to affiliated entities to achieve coherent customer services, organizations that rely on contracts must enter into contracts with each affiliated entity. Many countries require that the law of the country from which the data is being

69. In addition to the cross-border compliance obligations previously discussed, there are extensive local compliance obligations. For example, all of these privacy laws impose notice obligations that require organizations to provide information to individuals about what personal information is being collected, the purposes for which it will be used, and the identity and location of the organization collecting and using the information. Each country generally has a different set of required elements that must be contained in the notices. In addition, some countries require organizations to update such notices on an annual basis while others require new notices whenever there is a slight change in the data being collected or its intended purpose or use (e.g., the organization changes from one service provider to another that may be located in a different country). Consequently, for large global organizations, thousands of new notices must be generated.

exported must be the law that controls the contract and the jurisdiction in which disputes must be heard. Thus, data that is transferred from Japan to France must be governed by Japanese law and data that is transferred from France to Japan must be governed by French law. In theory, to ensure compliance with all of the legal obligations, the data of each organization should be segregated based on the country of origin. In addition, with the advent of the Internet, if data is entered into a global database in Bangladesh and is instantly available in the fifty offices in which the organization has offices, it is not clear which contract or which countries' laws would be applicable. Consequently, if a breach involves multiple jurisdictions or it is not clear where the breach occurred in the network, it will be complicated to untangle the jurisdictional and choice of forum issues and would likely delay resolution of the issue.

### Decreased business flexibility

The current system reduces business flexibility and inhibits businesses from managing their operations in an effective and efficient manner, which, in turn, impacts the range and price of products and services offered to consumers. In particular, the existing arrangement discourages or impedes enterprise-wide initiatives in such areas as training, succession planning, expense management, security, payroll, and provision of stock options. Given the complexity and administrative burden of obtaining workers' consents to transfer their personal information, some organizations opt to implement such programs locally which makes it difficult to ensure the same level of standards are followed at the local level as well as achieve the same economies of scale that could be achieved if the program were operated on an enterprise-wide basis. With respect to expense management, for example, if organizations were able to track and manage expenses on an enterprise-wide basis, they might be better positioned to negotiate larger discounts with suppliers and control their costs more effectively.

In addition to these administrative challenges, organizations must also grapple with conflicting cross-border transfer requirements in areas such as security that can make it difficult or impossible for them to develop systems best suited to their needs. For example, differences in security requirements could deter an organization from developing a harmonized and centralized security system on an enterprise-wide basis which, depending on the structure of its business, might provide better security protection than security systems at the affiliate level, each with different standards of security protection.

Workers are also disadvantaged by these restrictions on cross-border

transfers, particularly with respect to succession planning and stock options. If personal information is not transferred, then workers may lose out on valuable company benefits or promotional opportunities.

## V. The Emerging Global Solution: Corporate Privacy Rules

Given the problems inherent in the existing approaches to cross-border data transfers, the concept of Corporate Privacy Rules is emerging as a new and better approach to managing global data transfers. Under Corporate Privacy Rules, an organization would apply just one set of rules to govern data transfers among all jurisdictions. Both the parent and its affiliates are bound to protect the information according to those rules. The organization would then be able to move data as required among participating jurisdictions pursuant to these rules. The organization would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual jurisdictions.

If a breach occurs, the affected individual will be able to file a complaint locally in his or her native language—regardless of where the breach occurred or which affiliate was responsible for the breach—and have the complaint addressed in an appropriate manner by the company with whom he or she has a relationship. In short, a breach by one affiliate would be treated the same as a breach by any other, so individuals would be provided with consistent and enforceable rights, even in jurisdictions with no privacy laws in place.

To understand how such rules would work in practice, consider the following scenario:

*An individual located in Europe provides personal information directly to an affiliate located in Asia or indirectly through its local European affiliate. The Asian affiliate mishandles the information (violating the organization's Corporate Privacy Rules).*

Rather than force the individual to resolve the problem directly with the Asian affiliate and have to contend with different time zones as well as linguistic and cultural differences, the individual would be able to contact his or her local affiliate to file a complaint. The local (European) affiliate would be responsible for resolving the problem within the organization and would serve as the local interface with the individual. How the organization chooses to resolve the problem internally (e.g., determine which entity is financially or legally responsible) would be for the organization to decide.

If the individual is unable to resolve the problem with the local

entity, the individual would then be directed to an independent dispute resolution body authorized by the organization to hear and resolve complaints. If the issue was not resolved to his or her satisfaction, the individual would still be able to pursue legal claims against the organization or file a complaint with the authorities in the jurisdiction in which its Corporate Privacy Rules were approved or certified. As discussed *infra*, there should be a logical connection between the designated jurisdiction and the organization's operations (e.g., the jurisdiction selected might be the jurisdiction in which it has its center of activity or in which it is headquartered).

### A. *Benefits Of This Approach?*

#### Individuals

Corporate Privacy Rules offer significant benefits to individuals. They offer an effective method of protecting personal information no matter where the data is located throughout the world. Corporate Privacy Rules can ensure consumers' personal information is accorded a uniform level of protection, eliminate the need to determine the legal regime applicable to data processing activities in multiple countries, particularly with respect to on-line transactions, provide a local recourse mechanism, and simplify and reduce the cost of data privacy compliance for cross-border transfers, thereby encouraging greater compliance.

In the context of the consumer examples cited in Section IV *supra*, the benefits of Corporate Privacy Rules to individuals become apparent:

#### 1. *Corporate Privacy Rules Can Provide the Consumer with More Effective Recourse Mechanisms*

In the example involving a U.S. consumer and a German company, the U.S. consumer would be able to call the offices of the U.S. entity and file a complaint locally (and in English) if the parent has Corporate Privacy Rules in place. Consequently, the U.S. consumer would have recourse that it would not otherwise have if it had to deal directly with the German company. Moreover, the FTC would be able to exercise its jurisdiction through the U.S. entity if the German company failed to address the complaint.

#### 2. *Corporate Privacy Rules Provide Consumers with Consistent and Enforceable Rights Even in Jurisdictions with No Privacy Laws in Place*

In the hotel example, the hotels located in countries with less

stringent or no privacy laws would be required to abide by the same privacy rules of all the other hotels in the chain. As a result, the U.S. consumer's privacy rights will not change from one jurisdiction to another and the consumer has the assurance that his or her personal information will be protected in a consistent manner by all of the hotels in the organizational group. In the event that there is a breach or unauthorized use of the consumer's personal information, the consumer will be able to file a complaint with any of the hotels in the chain and have the complaint addressed in an appropriate manner.

3. *Corporate Privacy Rules Eliminate the Need to Determine Which Entity is at Fault*

In the example involving the purchase of a computer product, the organization as a whole is responsible for protecting the data regardless of which affiliate processes the data. A breach by one affiliate is treated the same as a breach by any other affiliate. The consumer's rights and recourse are protected no matter where the breach occurs.

4. *Corporate Privacy Rules Facilitate Twenty-Four-Hour Customer Service*

Corporate Privacy Rules would enable organizations to provide seamless twenty-four-hour customer service. Consumers would not need to receive multiple privacy notices. Their customer history files would be accessible to any customer service representative in any location, thereby eliminating the need to have the customer repeat his or her problem with the product. By eliminating the privacy compliance costs associated with global data transfers, more companies might implement twenty-four-hour customer service hotlines.

Businesses

From a business perspective, Corporate Privacy Rules are attractive because they would enable organizations to implement uniform privacy policies and practices on a regional or global basis without the administrative, legal, and organizational complexities of contracts. Moreover, these rules can be tailored to the needs of a particular business or industry sector, taking account of particular challenges and sensitivities, the corporate culture, processes, and the organizational structure. In addition, Corporate Privacy Rules could further encourage best practices and, in particular, the training and education of the workforce regarding privacy rules and expectations. Companies would be able to institute a single organization-wide program rather than

replicate the program in multiple local markets. Corporate Privacy Rules could also translate abstract obligations into a "real life" context without any legalese, and thus help the workforce understand and implement their respective obligations.

Implementing Corporate Privacy Rules is simply an extension of an approach that has worked successfully in other areas. It is not a new concept. For years, businesses have developed and enforced enterprise-wide policies in a variety of areas (e.g., in the field of financial reporting, determination of codes of conduct, and conflicts of interest). For these reasons, we believe that Corporate Privacy Rules could offer a new approach for consumers and organizations that will promote a more comprehensive culture of privacy.

### B. *Moving Toward the Development of Corporate Privacy Rules*

Currently, there are two separate initiatives underway in different regions of the world that are developing new ways to facilitate cross-border data transfers:

#### EU Approach

In the EU, Corporate Privacy Rules take the form of binding corporate rules ("BCRs"). The main current features of BCRs are outlined by the Working Party 29 in papers issued in 2003 and 2005.[70] As envisioned by the Working Party 29, organizations would be required to comply with the strictest EU national regimes in order to use BCRs. The organization would be required to select and contact a "lead authority" and then present its draft BCRs in English as well as the language of the lead authority, together with sufficiently detailed information on the organization's structure, data flows, etc.

The lead authority would generally be the DPA in the jurisdiction where the organization is headquartered in the EU, or where the person with overall responsibility for the definition and implementation of the data processing is located or the jurisdiction from which most data are transferred or from which most processes are controlled.

---

70. *See* Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", Article 29 Working Party Doc. WP 107 (Apr. 14, 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm. *See also* Transfers of Personal Information to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Article 19 Working Party Doc. WP 74, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf.

This authority would work with the other regulators in other relevant Member States. One Member State would not, however, have the ability to approve the rules without consultation with other Member States. Because the proposed mechanism for regulatory approval is purely voluntary, national authorities may refuse to co-operate either generally or with respect to the approval of a particular set of rules.

In January 2006, the U.K. Information Commissioner approved the first set of BCRs for the transfer of personal information by the General Electric Company to countries outside the EEA without an adequate data protection regime in place.[71] Nonetheless, a large number of EU Member States remain either lukewarm or hostile to BCRs because of concerns relating to the enforceability of BCRs.

Given the discussion above, it is apparent that important obstacles still remain to the widespread adoption of BCRs within Europe. In particular, the lack of a streamlined mechanism for obtaining regulatory approval of BCRs and the fact that these authorities can request changes to the BCRs reduces the likelihood that a single set of rules can be implemented. If an organization must comply with the strictest obligations in each Member State in which it operates, any "balancing" mechanisms that currently exist within national legislation may be lost. For example, different national regimes often have different focuses, e.g., strict surveillance may be compensated for by less strict internal audit requirements or broad statutory exemptions under which data may be processed may be complemented by a very narrow interpretation of what constitutes valid consent. Forcing organizations to adhere to a combination of the strictest regimes may deter them from adopting BCRs.

Further, many Member States have adopted differing views on the binding nature of BCRs and in some Member States, such as Spain, there is no provision in the law for recognizing binding corporate rules. To achieve widespread practical usage, EU data protection authorities will need to harmonize their individual approaches to BCRs.

Ideally, each Member State should recognize and give full effect to a set of BCRs approved by another Member State DPA (which could be the authority of the country in which the data controller has its "centre of activities"). To accomplish this, the Member State authorities would need to agree to recognize the regulatory authority of the country

71. *See* Info. Comm'r's Office, Binding Corporate Rules Authorisation (2005), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/binding_corporate_rules_authorisation%20_final.pdf.

where a transaction takes place, as well as the country from which a product, a person, or a service originates. This, in turn, embodies the principle that if a service can be provided lawfully in one jurisdiction, it can be provided freely in any other participating jurisdiction, without having to comply with the regulations of the other jurisdictions.

In this respect, it is important to bear in mind the common denominator of BCRs—to ensure that the data is adequately protected. The goal is not to afford protection equivalent to every Member State's privacy regime. The EU Directive does not require that BCRs provide more protection than that offered by other adequacy mechanisms established in the EU Directive; rather, it only requires that BCRs provide adequate protection.

### APEC Approach

In November 2004, the Asia Pacific Economic Cooperation ("APEC") Member Economies[72] approved a regional privacy framework that would permit the use of Corporate Privacy Rules to transfer personal information easily throughout the region.[73] This APEC Framework is also intended to promote a consistent approach to information privacy protection across APEC Member Economies, while avoiding the creation of unnecessary barriers to information flow. Creation of the APEC Framework also contributes to broader APEC e-commerce objectives to increase cross-border trade and growth in e-commerce in the region. In addition, APEC Ministers endorsed a Future Work Agenda on International Implementation of the APEC Privacy Framework, which includes instructing APEC members to continue efforts to develop a regional approach to privacy that will support global business models, such as privacy codes.[74]

The APEC Framework, which consists of a set of privacy principles ("Privacy Principles") and implementation guidance, seeks to achieve

---

72. The APEC Member Economies are Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Viet Nam.

73. *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), http://www.apecsec.org.sg/apec/apec_groups/som_special_task_groups/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

74. *See* Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group, *Future Work Agenda: Privacy Subgroup*, 2004/SOMIII/ECSG/024 (Sept. 29-30, 2004), *available at* http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2004.html.

four main goals:

- To develop appropriate privacy protection for personal information;
- To prevent the creation of unnecessary barriers to information flow;
- To enable multinational businesses to implement a uniform approach to the collection, use and processing of data; and
- To facilitate both domestic and international efforts to promote and enforce information privacy protection.

The APEC Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It highlights the reasonable expectations of consumers that businesses will recognize their privacy interests in a way that is consistent with the Privacy Principles outlined in the APEC Framework.

In general, the nine Privacy Principles are closely aligned with those found in the 1980 OECD Privacy Guidelines[75] and cover notice, choice, collection limitation, use of personal information, data integrity, security safeguards, access and correction, and accountability. The accountability principle, however, goes further than the OECD accountability principle by stating explicitly that when transferring information, whether domestically or internationally, organizations that control the collection, holding, processing or use of personal information should be accountable for ensuring that the recipient organization will protect the information consistently with the Privacy Principles when not required to obtain consent. The goal of the accountability principle is to enable organizations to develop and implement uniform approaches within their organizations for global access to and use of personal information.

Work on the implementation phase is underway. In particular, Member Economies have agreed to:

- Develop a multilateral mechanism for promptly, systematically and efficiently sharing information among APEC Member Economies;
- Develop cooperative arrangements among privacy investigation and enforcement agencies of Member Economies; and

75. *See* Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

- Endeavor to support the development and recognition of organizations' cross-border privacy codes across the APEC region.[76]

The next round of APEC privacy meetings were held in late January 2007 in Australia. During those meetings, Member Economies were expected to continue their efforts to support the development and recognition of Corporate Privacy Rules and continue to work on ways to implement the APEC principles in the Member Economies.

### C. *Where Do We Go From Here?*

At present, it is unclear if and how the initiatives in the EU and APEC can come together to achieve a global solution to international data transfer issues. One thing is clear, however: regional solutions alone will not be sufficient to resolve this issue. For Corporate Privacy Rules to become a reality, governments will need to recognize their value and make them a priority. While the initiatives in the EU and in APEC are laudable, regional solutions do not address the need for free information flow while protecting privacy, let alone the reluctance of some EU DPAs to commit to a pan-European solution.

A solution will require creative thinking about how to implement transfers in their respective jurisdictions as well as a strong commitment to work closely with other governments to devise an approval process that will be acceptable to all. In many, if not all of the jurisdictions, the proactive involvement of data protection, privacy authorities, consumer protection agencies and other relevant agencies will be required.

The key to any solution is that, apart from being truly global, it must also provide a method of implementing one set of rules throughout the world. As demonstrated above, the cost—both from a business and a consumer perspective—of divergent cross-border solutions is too high. What is needed is a method of adopting and being bound by one set of rules that can be uniform across the globe and is deemed sufficient in every jurisdiction. In the following sections, we lay out a possible roadmap for implementing and enforcing Corporate Privacy Rules.

## VI. Corporate Privacy Rules: Implementation Overview

Any business that intends to implement Corporate Privacy Rules

76. *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework International Implementation ("Part B") Final—Version VII*, 2005/SOM3/ECSG/020 (Sept. 8-9. 2005), *available at* http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.html.

would have to develop a set of rules to incorporate internationally accepted principles of fair information practices, such as the APEC Privacy Principles. The Corporate Privacy Rules would be evaluated and "certified" to ensure full compliance with these principles. For example, the Corporate Privacy Rules should be evaluated to ensure that they prescribe disciplinary sanctions for employees who violate the rules, allow for training on the Corporate Privacy Rules, and appointment of a Chief Privacy Officer and/or local privacy officers to further promote internal compliance. As will be further examined below, the certification could take the form of attestations/self-declaration or review by designated public or private entities to determine if the Corporate Privacy Rules comply with the internationally accepted set of principles.[77]

After completion of the certification procedure, the business would issue a public declaration of its adherence to the Corporate Privacy Rules or submit the rules to an appropriate DPA that would render the Corporate Privacy Rules enforceable, and a promise by the business to follow the policies established. The public declaration would be by the entire "corporate family"[78] or any affiliated entities that wished to share data. A complaint handling procedure would be developed to detail the manner in which complaints should be addressed.

The business would also need to undertake a comprehensive self-audit of its information processing practices in order to ensure that the practices are in accord with the stipulations in the Corporate Privacy Rules. Each business would then be obligated to regularly review its practices to ensure compliance with the requirements of the Corporate Privacy Rules.

Once these steps have been completed, the Corporate Privacy Rules would be regarded by all of the participating jurisdictions as satisfying the cross-border data transfer requirements of each jurisdiction without the need for further authorization or regulation. The business would then be able to move information as required to meet its needs among participating jurisdictions pursuant to its Corporate Privacy Rules. The business would still be responsible for complying with the local data protection requirements (e.g., database registration, notice

77. Whether the business in fact lives up to the promises made in its Corporate Privacy Rules would not be a matter to be determined at the certification stage. Rather, that would be determined by self-audit or through a third party audit procedure if a complaint is received and is not resolved through the internal complaint procedure.

78. The mechanism to ensure that Corporate Privacy Rules are binding upon all members of the corporate group will depend on the jurisdiction.

and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual jurisdictions.

### A. *Certification Process for Corporate Privacy Rules*

There are several different models possible for certifying Corporate Privacy Rules. While each jurisdiction should have the ability to select the certification model best suited for its own jurisdiction, the model used across participating jurisdictions would need to be consistent and uniform to ensure credible and predictable enforcement.

1. **A business could self-certify that its Corporate Privacy Rules comply with a set of internationally accepted privacy principles.**

The self-certification would involve an internal assessment of the Corporate Privacy Rules to ensure that the rules are in accord with the APEC Framework or other internationally accepted principles of fair information practices. The business would be required to self-certify compliance with these principles.

2. **A business could submit its Corporate Privacy Rules to a designated private or public entity for approval.**[79]

If a designated private or public entity reviews the Corporate Privacy Rules to ensure that they comply with the Privacy Principles or other internationally accepted principles of fair information practices, its compliance review might involve verification that there is an online privacy policy posted that covers the Privacy Principles or other internationally accepted principles of fair information practices and the designation of a dispute resolution mechanism.

A hybrid approach may include the development of an approval or verification process by public sector entities, which would be carried out by authorized private sector entities. Such a process could include guidance in the form of checklists or other documents that set forth essential code aspects or factors to satisfy the verification process. While there is a desire to obtain consistent outcomes in the verification process, some flexibility must be maintained to allow for variances in business models, customer bases, sectors and legal frameworks.

---

79. If a nonprofit organization carried out these functions, the regulatory body would need to give priority to referrals of non-compliance with guidelines that govern private organizations. If these private organizations fail to carry out their responsibilities (e.g., they approve Codes without undertaking the proper due diligence), their conduct would be actionable, in the case of the United States, under the FTC's unfair and deceptive trade practices authority or enforcement authority of other regulatory bodies.

### B. *Public Declaration*

There are also different ways in which businesses might make public declarations that would then be enforceable together with a promise to follow the policies in its public declaration. For example, consider the following options:

1. **A business would make a public declaration that it will protect personal information that it transfers from one jurisdiction to another in accordance with its approved Corporate Privacy Rules.**

The declaration could be included in the organization's privacy policy or some other public statement that is posted on its website (or in the case of workers, on its intranet). The organization would need to designate or indicate the jurisdiction in which it is certifying its set of Corporate Privacy Rules. There should be a logical connection between the designated economy and the business's operations (e.g., the jurisdiction selected might be the jurisdiction in which it has its center of activity or in which it is headquartered).

2. **A business would make a public declaration that it will protect personal information that it transfers from one jurisdiction to another in accordance with its Corporate Privacy Rules by registering its commitment with a designated private or public entity.**

The declarations/registrations would be submitted by the business to a private or public body and would then be available online for public inspection.

Once a business makes a public declaration, then its Corporate Privacy Rules would be regarded by all of the other participating jurisdictions as satisfying the "cross-border" data transfer requirements of each participating jurisdiction without the need for further authorization or regulation. The business could then move data as needed among participating jurisdictions pursuant to its Corporate Privacy Rules. The business would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual economies.

### C. *Complaint Handling*

Those businesses that elect to participate in a Corporate Privacy Rules process would provide information about their complaint handling procedure in either their privacy policy or other documents that

are made available to the individual concerned. This information would detail the manner in which and to whom complaints should be addressed, the existence of any third party dispute resolution mechanisms, and the regulatory authority or agency that would receive complaints from individuals once all other dispute resolution mechanisms have been tried.

Complaints about any handling of personal information would be addressed, first, through the business's internal complaint handling process. If the complaint cannot be resolved internally, then the business is strongly encouraged to have an independent dispute resolution mechanism in place that can be used.

Possible third party dispute resolution programs in the U.S. include those run by businesses such as BBBOnline, TRUSTe, AICPA WebTrust and the Direct Marketing Association. In addition, outside arbitration and mediation service such as JAMS or the American Arbitration Association could also be used. In countries with independent DPAs, the appropriate DPA could provide the dispute resolution mechanism. In other countries, such as Japan, other private dispute resolution mechanisms are available.

The dispute resolution mechanism, to be effective, must be independent, readily available and affordable. Damages, penalties and/or sanctions may be awarded where the applicable law or private sector initiatives so provide. A business should also be obligated to remedy problems arising out of its failure to comply with its Code, and persistent failures of the business to comply with rulings could result in the loss of their Code certification.

If the dispute still cannot be resolved, then the matter would be referred to the applicable governmental or regulatory body responsible for privacy protection (such as the FTC, FCC, OCC, Securities Exchange Commission or other appropriate entity in the U.S.) or, where such an agency does not exist, the public prosecutor in that economy. The governmental or regulatory body would then work with the business and/or third party certification entity (if applicable) to resolve the dispute. If the business refuses to comply with the decision of the regulatory body, then it would also be subject to penalties and sanctions.

## VII. Enforcement

As we have seen in the EU context, significant concerns remain about how to make Corporate Privacy Rules "binding" when businesses volunteer to adhere to a set of rules. DPAs in the EU and around the world believe that existing laws do not provide them with the authority

to enforce BCRs or Corporate Privacy Rules. However, even where DPAs lack jurisdiction or do not have the legal means to enforce Corporate Privacy Rules, Corporate Privacy Rules can be legally enforceable and thus "binding" under a number of theories including: revision of corporate bylaws, unilateral declaration, and/or unfair commercial practice laws.

*United States*

In the United States, for the past ten years, the FTC has used its authority several times under Section 5 of the FTC Act to take action against companies that misrepresent their privacy practices.[80] Corporate Privacy Rules which are included in an on-line privacy policy or some other public statement that is posted on its website (or in the case of workers, on its intranet), could therefore be challenged as unfair or deceptive trade practices where the business fails to comply with its Corporate Privacy Rules.[81]

For example, in 2005, the FTC settled charges against an Internet company that provided shopping cart software to online merchants.[82] According to the FTC, the company rented personal information about merchants' customers to marketers, knowing that such disclosure contradicted merchant privacy policies. The company was barred from disclosing personal information it had previously collected and making future misrepresentations about the collection, use, or disclosure of personally identifiable information. It also required that the company's and merchants' privacy practices be consistent, or, if not, then that company had to disclose in a clear and conspicuous manner that personal information collected on the site would be used, sold, rented, or disclosed to third parties. The settlement also required that the company forfeit monies it made by selling the information and

80. For information on enforcement, see Federal Trade Commission, Enforcement Cases, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited March 23, 2007). For information regarding the FTC's overall investigative and law enforcement authority, see Federal Trade Commission Office of the General Council, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, Sept. 2002, *available at* http://www.ftc.gov/ogc/brfovrvw.htm.

81. Whether the FTC has jurisdiction over issues involving employee data is a matter that has not been settled. To date, the FTC has not taken action against an organization for false or deceptive practices with respect to employee data, and it is an open question whether the FTC can assert such jurisdiction.

82. Agreement Containing Consent Order, Vision I Properties, LLC, File No. 0423068 (Mar. 10, 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf.

adhere to certain record-keeping provisions that would allow the FTC to monitor compliance with its order.

In 2004, the FTC settled a case against Tower Records involving a security flaw in the company's website that exposed customers' personal information to other Internet users in violation of Tower's privacy policy representations and federal law.[83] Tower Records was barred from making future misrepresentations and was required to implement an appropriate security program and carry out regular outside audits of its website security for the next ten years.

The same year, Gateway Learning Corporation also agreed to settle FTC charges that it violated federal law when it rented consumers' personal information to target marketers.[84] According to the FTC, Gateway Learning rented consumers' information contrary to explicit promises made in its privacy policy and that, after collecting the information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or obtaining their consent. Gateway Learning was barred from making deceptive claims about how it will use consumers' information and from applying material changes in its privacy policy retroactively without consumers' consent. Gateway Learning was also required to forfeit the money it earned from renting the data.

In 2000, Toysmart.com ("Toysmart") agreed to settle FTC charges that the company misrepresented to consumers that personal information would *never* be shared with third parties and subsequently disclosed, sold or offered that information for sale in direct violation of the company's own privacy statement. The settlement agreement forbade the sale of Toysmart's customer information except under very limited circumstances.[85]

As the actions taken by the FTC over the past decade demonstrate, it is possible to enforce public representations about privacy practices under laws applicable to unfair commercial practices. Many countries around the world have similar laws in place that may enable the DPAs or other relevant authorities to prosecute businesses that fail to adhere to their Corporate Privacy Rules.

Other federal agencies have similar powers. For example the finan-

---

83. Agreement Containing Consent Order, MTS, Inc, File No. 032-3209 (Apr. 21, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.

84. Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (July 7, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf.

85. FTC v. Toysmart.com, LLC, No. 00-CV-11341, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000).

cial regulators have similar authority under the bank regulatory acts with respect to false and deceptive practices by banks.[86]

*European Union*

It is also possible to enforce Corporate Privacy Rules in the EU using an approach similar to that found in the U.S., under the theory of "unilateral undertakings" or a public declaration. Unfair trade practices laws, as well as general rules on misrepresentation and misleading advertisement, can in fact provide sufficient legal guarantees.[87] If businesses are obligated to publish Corporate Privacy Rules, as recommended in this article, and if they then fail to follow those rules, businesses could be challenged by national regulators and individuals. In this respect, the 2005 Directive on Unfair Commercial Practices[88] ("Unfair Commercial Practices Directive") harmonizes Member State laws in this area. The purpose of the Unfair Commercial Practices Directive is to protect consumers from unfair commercial practices and businesses from unfair business practices by their competitors. In particular, it introduced individual rights of action in all Member States that will enable individuals to enforce their rights against unfair commercial practices. According to a recently published article by Leonardo Cervera Navas, an official of the EU Commission who worked in the data protection field, a "definitive solution to the problem of the so-called 'external binding effect' of Binding Corporate Privacy Rules appears to be attainable in the EU context."[89]

Cervera argued that the Unfair Commercial Practices Directive provides the enforcement hook sought by the EU data protection community. Cervera argued that anything that impairs the consumer's ability to make an informed decision, and thus causes the consumer to make a decision that he or she might not otherwise make, would

86. *See* 12 U.S.C. § 1818(b) (2006); 15 U.S.C. § 45(a) (2006). *See also* Letter from Alan Greenspan, Chairman, Federal Reserve, to Congressman John LaFalce, Ranking Member, Committee on Financial Services (May 30, 2002), *available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2002/20020530/attachment.pdf.

87. Henning Kahlert: Unlautere Werbung mit Selbstverpflichtung, Wettbewerbsrechtliche Problem emit Datenschutz im Internet, DuD (2003), 412.

88. Parliament and Council Directive (EC) No. 29/2005 of 11 May 2005, 2005 O.J. (L 149) 22, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_149/l_14920050611en00220039.pdf.

89. Leonardo Cervera Navas, *The New Directive on the Unfair Commercial Practices in the Internal Market as a Promising Tool for the Uptake of Binding Corporate Rules*, 20 INT'L REV. L. COMPUTERS & TECH. 343 (2006).

constitute a material distortion of consumers' economic behavior.[90] Moreover, declaring that certain standards of data protection are being applied when that is, in fact, not the case would likely be considered contrary to the requirements of professional diligence and therefore constitute an unfair commercial practice as defined by the Directive.[91] Consequently, Cervera concluded that failure to honor Corporate Privacy Rules commitments would constitute an unfair trade practice.[92] In his view, it is reasonable to think that DPAs can be considered to be competent authorities for exercising the power confirmed by the Directive and hearing claims. Moreover, he suggested that the Directive may increase the enforcement power of some DPAs in certain Member States where enforcement powers are more limited.[93]

In addition, national labor laws are likely to provide redress to employees should the employer make erroneous statements about the processing of personnel data, for example, in the labor contract or on its intranet.

### *Other Countries*

A survey of consumer protection laws in Asia and the Americas has found that many countries in those regions have laws that prohibit false or misleading representation and/or unfair business practices. In Asia, countries such as Australia, India, Indonesia, Japan, Korea, New Zealand, the Philippines, and Thailand have laws in this area that provide individual redress and/or administrative sanctions including fines and injunctions. All of these countries have established enforcement bodies or delegated enforcement to particular executive departments.[94] In

90. *See id.* § 6.2.

91. *Id.*

92. *Id.*

93. *See id.* § 6.4.

94. The following are the respective designated authorities and consumer protection laws: *Australia*—Australian Competition and Consumer Commission, http://www.accc.gov.au/content/index.phtml/itemId/142, and the Trade Practices Act, 1974 (Austl.), *available at* http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/index.html; *India*—National Consumer Disputes Redress Commission, http://ncdrc.nic.in, and the Consumer Protection Act, No. 68 of 1986, *available at* http://ncdrc.nic.in; *Indonesia*—National Consumer Protection Board and the Law on Consumer Protection , No. 8 of 1999; *Japan*—Japanese Cabinet Office, Quality of Life Bureau, http://www.cao.go.jp/index-e.html, and the Consumer Protection Fundamental Act, Law No. 78 of 1968 (as amended), *available at* http://www.apeccp.org.tw/doc/Japan/Comlaw/jpiss01.html; *Korea*—Korea Consumer Protection Board, http://english.cpb.or.kr, and the Consumer Protection Act, Act No. 3921 of 1986 (as amended), *available at* http://english.cpb.or.kr; *New Zealand*—Ministry of Consumer Affairs, http://www.consumeraffairs.govt.nz, Commerce

the Americas, countries such as Mexico, Barbados, Brazil, Chile, Costa Rica, Panama, Paraguay, and Uruguay, have designated authorities and in most cases consumer protections laws that may provide appropriate legal bases on which to enforce Corporate Privacy Rules.[95] Particularly in Central and South America, where few privacy laws have been enacted, these consumer protection laws may provide a promising avenue for enforcement of public promises made by businesses.

More and more countries are adopting or strengthening their unfair commercial practices or consumer protection laws, largely in response to efforts underway at the OECD and the United Nations. Both the U.N. and the OECD have issued guidelines on consumer protection that call for protection against unfair and misleading commercial

---

Commission, http://www.comcom.govt.nz, and the Fair Trading Act , No. 121 of 1986, *available at* http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=3417260055&infobase=pal_statutes.nfo&jump=a1986-121&softpage=DOC; *Philippines*—Bureau of Trade Regulation and Consumer Protection, Ministry of Commerce, http://www.business.gov.ph/About_Organizational_Chart.php, and Consumer Act, Republic Act No. 7394 of 1991, *available at* http://www.business.gov.ph/uploads/files/Forms1_File_1104836450_RA7394.pdf; and *Thailand*—Consumer Protection Board, http://www.ocpb.go.th, and the Consumer Protection Act, B.E. 2522 (1979).

95. The following are the respective designated authorities and consumer protection laws: *Barbados*—Fair Trading Commission, http://www.ftc.gov.bb, and the Consumer Protection Act, 1 L.R.O. 2002, Cap.326D, *available at* http://www.commerce.gov.bb/Legislation/Documents/Consumer%20Protection%20Act,Cap326D.pdf; *Brazil*—Office of Consumer Protection, Ministry of Justice, http://www.mj.gov.br/DPDC/index.htm, and the Código de Defesa do Consumidor, Law No. 8.078 of Sept. 11, 1990, *available at* http://www.mj.gov.br/DPDC/servicos/legislacao/pdf/cdc.pdf; *Chile*—the National Consumer Service (SERNAC), http://www.sernac.cl, and Ley No. 19.496, *available at* http://www.sernac.cl/docs/texto_ley_del_consumidor.pdf; *Costa Rica*—Directorate of Consumer Support, http://www.meic.go.cr/esp2/consumidor, and Ley No. 7472 de Promoción de la Competencia y Defensa Efectiva del Consumidor [Law No. 7472 on Promotion of the Competition and Consumer Protection], Gaceta 14, Jan. 14, 1995, *available at* http://www.meic.go.cr/esp2/informacion/leypromo.html; *Mexico*—Profecco, http://www.profeco.gob.mx, and the Ley Federal de Protección al Consumidor, DOF Dec. 24, 1992, p. 26, *available at* http://www.diputados.gob.mx/LeyesBiblio/ref/lfpc/LFPC_orig_24dic92_ima.pdf; *Panama*—Authority for Consumer Protection and Competition Defense, http://www.autoridaddelconsumidor.gob.pa, and Ley No. 29 of 1 Feb. 1996, *available at* http://www.autoridaddelconsumidor-.gob.pa/pdf/ley29febrero96.pdf; *Paraguay*—National Integrated Consumer Protection System, http://www.mic.gov.py/snipc, and Ley No. 1334 De Defensa Del Consumidor Y Del Usuario [Law No. 1334 On Consumer and User Protection], *available at* http://www.mic.gov.py/snipc/marco_juridico/Ley_1334.pdf; and *Uruguay*—Ministry of Economy and Finance Office of Defense of Consumer, http://www.defcon.gub.uy, and Ley de Relaciones de Consumo [Law on Consumer Relations], No. 17.250 of 11 August 2000, *available at* http://www.defcon.gub.uy/informacion/index.php?IndexId=56.

practices.[96] Consumer protection laws, however, may not work to regulate public declarations made by businesses relating to personal information of their employees. Using existing unfair competition laws or consumer protection laws as a back stop to enforcing public declarations relating to consumer information could go a long way to creating an enforceable global privacy regime for consumer information without having to wait for new laws to be passed or an international accord to be reached.[97]

## VIII. CROSS-BORDER COOPERATION

In addition to having the appropriate legal basis on which to enforce Corporate Privacy Rules, there needs to be a commitment among the respective enforcement authorities to cooperate in the event of cross-border disputes or breaches. Such an agreement could take a form similar to a mutual recognition or cooperation agreement. While such cross-border cooperation and collaboration would not be easy to accomplish, it is not unprecedented. In fact, government agencies around the world are already collaborating closely in such areas as law enforcement, spam, and identity theft. The following are some examples of where such cooperation is already occurring; any of these existing networks could serve as a source or model for cooperation in the privacy area.

*Spam.* In October 2004, government agencies around the world joined forces to combat spam on a global level with an Action Plan on Spam Enforcement. The Action Plan, endorsed by nineteen agencies from fifteen countries, calls for increased investigative training, the establishment of contact points within each agency to respond quickly and effectively to enforcement inquiries, and the creation of an international working group for spam regulation.[98]

*Consumer Protection.* The International Consumer Protection and Enforcement Network (ICPEN), formerly known as the International Marketing Supervision Network (IMSN), is a membership business

96. *See* UNDESA, *United Nations Guidelines for Consumer Protection* (2003), http://www.un.org/esa/sustdev/publications/consumption_en.pdf; OECD, *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce* (2000), http://www.oecd.org/dataoecd/18/13/34023235.pdf .

97. During their 2006 meeting, the International Conference of Data Protection and Privacy Commissioners called for the development of an international privacy convention. The 2006 conference communiqué is available at http://ico.crl.uk.com/files/FinalConf.pdf.

98. *See The London Action Plan on International Spam Enforcement Cooperation* (2004), http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf.

consisting of the trade practice law enforcement authorities of more than two dozen countries.[99] The mandate of the ICPEN is to share information about cross-border commercial activities that may affect consumer interests and to encourage international cooperation among law enforcement agencies.

*Consumer Fraud/Identity Theft.* Consumer Sentinel members include more than 1000 law enforcement agencies in Australia, Canada, and the United States.[100] It helps them build cases and detect trends in consumer fraud and identity theft. Consumer Sentinel gives law enforcers access to over one million complaints, including consumer complaints from numerous Better Business Bureaus, the National Fraud Information Center and Canada's PhoneBusters.

*Anti-trust.* The International Competition Network (ICN) provides anti-trust agencies from developed and developing countries with a network for addressing practical anti-trust enforcement and policy issues of common concern.[101]

## CONCLUSION

Given the weaknesses in existing approaches to cross-border data transfers, a new truly global solution is needed sooner rather than later. Consumers, business, and countries are being disadvantaged by the existing patchwork of cross-border privacy rules. Countries with strict or complex cross-border restrictions, particularly those in the developing world, are likely to lose out on new business investment and outsourcing opportunities. Moreover, increased regulation does not mean increased privacy protection. To the contrary, the overly complex maze of regulation discourages compliance as well as the provision of products and services. Concern about the lack of business compliance was raised as an issue, for example, in Japan during the government's public consultation on the review of the Personal Information Protection Law.[102]

As we have discussed, the use of Corporate Privacy Rules offers a way

99. Information on the International Consumer Protection and Enforcement Network is available at http://icpen.cpb.or.kr/en.

100. Information on Consumer Sentinel is available at http://www.consumer.gov/sentinel.

101. Information on the International Competition Network is available at http://www.internationalcompetitionnetwork.org.

102. In particular, the discussion document questioned why there were such disparities in how businesses protect personal information and noted that some businesses have stopped providing services such as the public directories because they find the rules to be overly burdensome. *See* Personal Information Protection Committee, Quality of Life Policy Council,

to correct the problems associated with the current patchwork of cross-border privacy rules and provide significant benefits to companies and individuals alike. By enabling companies to implement consistent privacy policies and practices on a global basis, individuals will be afforded more meaningful privacy protections. Their personal information will be protected in a uniform and consistent manner across an organization no matter where the information may be transferred. In addition, because companies would be required to remain accountable for the protection of personal information under their control and address complaints when they arise, individuals would have recourse for the first time in jurisdictions with no privacy laws and, in some cases, more effective recourse in those jurisdictions with existing privacy laws.

Corporate Privacy Rules would also eliminate the need to determine the legal regime applicable to the cross-border data processing activities of the company since the processing would be subject to a single set of privacy principles, rather than the laws of the multiple countries from where the data emanate. In addition, Corporate Privacy Rules can be tailored to the needs of individual companies taking account of particular challenges and sensitivities, the corporate culture, processes and the organizational structure. Corporate Privacy Rules are also easier to administer than contracts and in some cases do not require approval by certain DPAs. In sum, providing companies the freedom to move data globally among affiliates in accordance with their Corporate Privacy Rules can provide important benefits to everyone, including the provision of seamless twenty-four-hour customer service, a wider array of products and services at lower prices, enhanced privacy protections, better and more uniform workforce training and education, and reduced corporate administrative burdens.

Nonetheless, many DPAs continue to call for the development of international data privacy standards or an international privacy convention as the best way to address the disparities in privacy protection around the world.[103] At best, however, this will take years

---

Japanese Cabinet Office, Main Issues for Consideration with Respect to the Protection of Personal Information (discussion paper) (July 28, 2006).

103. The International Conference of Data Protection and Privacy Commissioners has repeatedly called for the development of international data privacy standards since 2003 and, most recently, in 2006 for the establishment of an international privacy convention. *See* Data Protection and Privacy Commissioners 2003, Commissioner Resolutions, http://www.privacyconference2003.org/commissioners.asp; Press Release, Swiss Federal Data Protection

to accomplish, presuming that agreement can be reached within the international community to develop such a convention. Even if such a convention is agreed upon, several additional years will be required for countries to conform their national laws to the convention.

The attractiveness of Corporate Privacy Rules is that they can be implemented without, in most instances, enacting new laws or regulations. The challenge will be for governments to devote the necessary time and effort to:

- Identify existing means within national law to enforce Corporate Privacy Rules, such as through consumer protection, unfair trade practices, and/or privacy laws;
- Establish a national approach to verification and approval of Corporate Privacy Rules; and
- Establish a cross-border cooperation mechanism and a system for mutual recognition or acceptance of Corporate Privacy Rules.

These tasks, however, are eminently achievable. In any case, whatever global solution is ultimately agreed upon, it is clear that it has to greatly simplify the current arrangement. Once a practical global solution is developed, compliance will increase, thus increasing privacy protection for everyone concerned, and greater economic benefits will flow to countries that permit businesses to utilize a global solution for their cross-border data transfers.

While some companies are experimenting with the EU approach to BCRs, that approach is not likely to be widely embraced by global businesses because it seeks to apply EU standards on a global basis. In particular, it applies standards that are equivalent to or supersede those that a European company must abide by. For example, the EU approach to BCRs requires an entity established in the EU to be the guarantor for the entire global corporate family.[104]

Attainment of a global solution is within reach if governments show sufficient flexibility and strive for comparable rather than equivalent

---

and Information Commissioner, 27th International Conference of Data Protection and Privacy Commissioners, Montreux (14-16 September 2005) Towards the Recognition of a Universal Right to Data Protection and Privacy (Sept. 16, 2005), http://www.edoeb.admin.ch/dokumentation/00438/00465/00888/00893/index.html?lang=en; 28th International Conference of Data Protection and Privacy Commissioners, Closing Communiqué, http://ico.crl.uk.com/files/FinalConf.pdf.

104. *See* Karin Retzer, *Land in Sight: The Latest Developments Concerning Data Transfers from the EU*, http://www.mofo.com/news/updates/files/update1428.html.

protection. Moreover, a strong commitment to finding a common solution and creative "can do" thinking will be needed. Individuals, businesses and governments all have a stake in resolving this issue so that individuals can have meaningful protections for their personal information as well as access to a wide variety of products and services at competitive prices.

**Before the**
**U.S. Department of Commerce**

| | | |
|---|---|---|
| **In the Matter of the Request for Comments on National Telecommunications and Information Administration's Notice of Inquiry, "National Privacy and Innovation in the Internet Economy"** | ) | **Docket No. 100402174-0175-01** |

---

**COMMENTS**

**OF THE**

**NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY**

---

**/s/ Thomas M. Boyd**
Thomas M. Boyd

DLA Piper
500 Eighth Street, NW
Washington, DC 20004
(202) 799-4000

**June 17, 2010**

**June 17, 2010**

**FILED ELECTRONICALLY**

**National Telecommunications and Information Administration**
**US Department of Commerce**

**In the Matter of the Request for Comments on**
**National Privacy and Innovation in the Internet Economy**
**Docket No. 100402174-0175-01**

# Comments of the National Business Coalition on E-Commerce and Privacy

## I. INTRODUCTION

The National Business Coalition on E-Commerce and Privacy very much appreciates both the Department's undertaking this inquiry and this opportunity to submit comments.

The National Business Coalition on E-Commerce and Privacy (the "Coalition") represents sixteen name brand corporations engaged in both offline and online commercial activity. Its membership is also diverse, ranging from major financial institutions to equally well-known retailers. All have the same goal: to contribute to the public policy debate in such a way as to help assure that policymakers undertake changes in law and regulation which are both commercially and economically prudent and workable.

We particularly appreciate the opportunity to participate in the Department of Commerce's National Telecommunications Administration's Notice of Inquiry ("NOI"), "National Privacy and innovation in the Internet Economy", and we hope our comments will prove to be of value as the Department deliberates incorporating its public policy positions into the Administration's evolving policies on Internet privacy.

The NOI lists several areas in which it invites comment, so we will present our thoughts to correspond to each one, as appropriate.

### 1. US Privacy Framework Going Forward

The NOI seems to predicate this question on the assumption, based on the Department of Commerce's extensive "listening sessions", that "the customary notice and choice approach to consumer protection may be outdated, especially in the context of information-intensive, highly interactive, web-based services." It goes on to say that "in lieu of, or in addition to notice and

choice, some have advanced the notion that sophisticated data managers migrate to a 'use based' model."

The view of the Coalition is that notice and choice have NOT outlived their value, that both are, and continue to be, essential to giving the consumer an understanding about how data collected from him/her will be used and whether that consumer wishes such collection to continue. We already have a "use based" system in place, with functional regulators responsible for supervising the use and collection of data used within their areas of oversight. This is a system that has worked well and has encouraged market-based solutions and industry "best practices" in response to demonstrated consumer needs and expectations. It is our belief that robust notice that is "clear and conspicuous" is key to the ability of consumers to exercise informed choice. And that choice need not default to the affirmative consent requirement that is observed in the breach overseas and which is both generally unnecessarily costly and counterproductive in this country. The sole exception, in our judgment, ought to be "sensitive personal information," such as a credit or debit card, in combination with factors that might lead one to identify the holder of the card and access those accounts, or the first and last name of the consumer, in combination with a series of factors that, like the credit or debit card, might lead to the disclosure of, and thereby access to, the consumer's sensitive financial or personal information. This category of information is clearly in need of a higher level of security and stricter access and use, but absent a compelling societal need, we do not think an affirmative consent, or "opt-in," is either necessary or desirable, as a matter of public policy.

Our concern, and it is deeply held, is that a move away from traditional notice and choice is tantamount, ultimately, to prohibition of access, without justification or the establishment of demonstrable economic harm. "Use" is a sufficient distinction, and it is already in place, but any efforts to modify existing notice and choice practices should face strict scrutiny as to the economic consequences and the public policy need. The solution is NOT to redefine "notice" to such an extent that written notices themselves are required to focus, as one policymaker has suggested, on a wide array of intended uses, with such detail as how data is collected, how it is stored and for how long, and how the data is disposed of, among others. In trying to cover every possible use of personal data in a notice, the purpose of which should be to make the consumer aware that personal data pertaining to him/her is being collected and to provide a means by which to learn more details, this kind of approach is self-defeating, for if few consumers care to read notices now, they will surely decline the opportunity if the notices become even longer and more detailed than they already are.

It is our view that the existing framework is working, and adjustments to it should be pursued with extreme delicacy and enhanced sensitivity to the likely "real world" consequences. Most notably has been the recent focus, on the part of some policymakers, on the use of personal data for use in marketing, as though marketing products and services to the public is somehow inherently suspect. On the contrary, it is absolutely essential to the growth of the economy. Without effective marketing, especially when enhanced with data which permits consumers to be presented with and educated about products and services for which they have already demonstrated an interest, companies will have to resort to less efficient and more intrusive mass marketing. The First Amendment precludes an outright ban against commercial speech, which marketing clearly is, so efforts to restrain corporate marketing initiatives through the

broad application of affirmative consent requirements has been the approach of choice recently. And it is both misguided and counterproductive. It is, instead, an academic and highly political solution to a complicated economic reality, and such tools as mailing and prospect lists, catalogues, consumer prospecting mail and customer development are critical to the continued viability of the free market. Without their ready availability, many companies will simply wither and die over time. To the Coalition, any federal efforts to further restrict marketing should first be required to establish a demonstrable economic or personal harm which requires the force of government intervention; nebulous social "harms," such as embarrassment or inconvenience, should be rejected outright as substitutes for the need to define harm strictly and unambiguously. The actual harm standard, unlike the "social" alternatives, are well established and quantifiable, and therefore reliable as a compliance guideline. Anything else is open to interpretation and conjecture, and therefore inconsistent application.

## 2. U.S. State Privacy Laws

As noted in the NOI, some 44 states already have data security or data breach laws in place, and some have both. So far, these state laws have been more or less aligned, resulting in a manageable compliance environment for companies, such as our members, that are all engaged in interstate, if not global, commerce. But this general consistency of law is a product of both momentary good fortune and the use by some states of the legislative templates developed by another. It is NOT an empirical basis on which to make a public policy assumption that continued and unrestricted state regulation over economic activity with clear interstate implications is either wise or prudent.

The Coalition believes that offline and online laws affecting privacy should be similar, if not virtually identical, and that such laws should be accompanied by effective federal preemption. It makes no public policy sense to enact federal law that can either be enhanced at the State level, as allowed by section 507(b) of the Gramm-Leach-Bliley Act, or by federal law that is accompanied by vague, ambiguous or practically non-existent presumption. Our members are happy to comply with whatever policies are enacted into law, but they simply do not wish to have to comply, nor should they have to, with an ever-shifting "patchwork" of different State laws that can actually change, as between the various States, several times in any given year.

The obvious trade-off for effective preemption is vigorous and effective enforcement of federal law at the State level, and we endorse that exchange of responsibility. Federal agencies simply do not have the resources that would be necessary to enforce the application of federal privacy law across the country. State Attorneys General have an inherent responsibility to protect their citizens from violations of such personal intrusions as the use of personal data, especially sensitive personal data, for illegal purposes. Their active and augmented involvement in the federal framework for privacy protection is therefore useful and desirable.
However, the involvement of State Attorneys General should be limited to the four corners of the federal legislation and should find exclusive jurisdiction in federal court, not State court, both because that choice of forum enhances the prospects for the consistent application of federal law across State lines and because consumers and businesses alike can have better predictability over what their legal obligations and personal rights are. The extension of this enforcement authority, as has been proposed of late, to unidentified State agencies or bureaus, or to those State agencies

or bureaus "designated" by State Attorneys General, is neither legally warranted nor politically justified. The State Attorney General has the best sense for the consumer-based privacy needs of the citizens of his/her State, and that should be sufficient. Further delegation only serves to dilute the importance of the federal statute; if the alleged violations are indeed "serious", then they ought to be serious enough to warrant the attention of the State Attorney General.

**3. International Privacy Laws and Regulations.**

Virtually all of our members engage in global business, both online and offline, and so the nature of international privacy law -- and its level and consistency of enforcement, is of considerable interest to them. We have been engaged, on the periphery, in the recent deliberations of the Asia-Pacific Economic Cooperation (APEC) and are certainly aware of the European Union's recent interest in revisiting its 1995 Data Privacy Directive.

What is paramount to the Coalition is that, like our need for predictability and consistency in the application of federal US law, international law be equally sensitive to the need for cross border consistency in both what the law requires by way of compliance as well and how well and how consistently it is enforced. In fact, the latter is an area in which very little attention has been paid by global policymakers. It makes little difference what laws and regulations say if they are not adequately enforced, and to this point the European attitude has been to compare its 1995 Directive with US law and render the latter "inadequate", leading, in part, to the creation of the Commerce Department's US-EU "Safe Harbor" Framework. We believe, however, that a persuasive case can be made that the nature and level of enforcement applicable to US privacy laws are as "adequate", if not more so, than is the case in Europe. Internet commerce and technological innovation are inevitably impacted, in most cases negatively, by the inconsistent application of law, and global privacy law, especially European law, is without doubt inconsistently applied. We would therefore urge the Commerce Department to undertake what does not now exist, so far as we know, but which is absolutely necessary for a truly informed discussion about the delicate balance between economic need and personal privacy expectations: a detailed, comprehensive analysis of US and EU law AND enforcement so as to provide a full and accurate comparison of their respective application.

Unlike Europe, the United States has in place a highly regulatory, aggressively enforced enforcement regime, both at the federal and State level, whereas Europe depends exclusively on its Member State Data Protection Authorities (DPAs) for enforcement of its laws and regulations, and that enforcement can be fairly characterized as inconsistent at best and, at worst, as selectively non-existent. Our members are aware of the "flexibility" demonstrated by certain DPAs in the use and application of affirmative consent, and we believe that flexibility to be the product of regulatory hubris confronted by economic reality. It merely reflects the flexibility exercised regularly by functional regulators in the United States, but its broad and inconsistent application in the EU needs to be better understood by policymakers on both sides of the Atlantic; hence the recommendation for a detailed analysis of the two systems.

**4. Jurisdictional Conflicts and Competing Legal Obligations.**

This section duplicates the concerns stated above, in that consistency of law and its application are inextricably woven together, and both are at the very core of what a meaningful privacy compliance environment actually is, both here and abroad. Our members are constantly concerned about how European law will be enforced and under what guidelines, and they are equally concerned about the current "patchwork" of State laws that exist in this country, as well as about the periodic efforts of policymakers, both at the State and at the federal level, to put politics and a good press releases above the practical effect of law and regulation on their constituents and the economies in their States.

The impact of competing State laws on consumers is obvious. Companies are unable to afford a range of different compliance tools for use in different States depending on the law of that State. They instead tend to gravitate to conforming their compliance needs to the most restrictive States, thereby applying in one State law which another has adopted for itself. Also, the wide range of dates on which State legislatures are in session only adds to the uncertainty our members face on a regular basis. The same is true when extraterritorial jurisdiction is applied to otherwise domestic US actions, and the converse is also true.

**5. Sectoral Privacy Laws and Federal Guidelines.**

As we have said before, the sectoral approach to privacy that comprises the US framework is preferred over all others, and the EU's newly discovered "flexibility" is an admission that economic reality has begun to set in. This "de facto" compliance approach should be codified in Europe, as a result of its current re-examination of the 1995 Directive, so as to equalize cross border compliance expectations. Otherwise, US business conducted in the United States will be at a competitive disadvantage over the same business conducted in Europe, when both should be treated equally.

The absence in Europe of an "American Rule" pertaining to attorneys fees suggests that those governments and individuals are or should be aware of what constitutes an effective enforcement system an if the EU is not going to adjust its enforcement system to mirror our more aggressive litigation reality, then it needs to make allowances for the privacy enforcement regime that operates in this country and revisit the EU-US "Safe Harbor" and financial "adequacy" frameworks.

**6. New Privacy-Enhancing Technologies and Information Management Processes.**

Like everyone else who collects and uses personal data, our members are very sensitive to the need to secure and selectively use that data. Our members are brand name companies with decades if not centuries of history, and their customers are their first priority. We believe in industry self-regulation, carefully monitored by functional regulators, including the Federal Trade Commission, and we are open to the need for government action if the justification can be universally understood and accepted. For example, we recognize the need for strong and reliable data security, and we have helped write and promote preemptive federal legislation that would

require every covered entity to provide strong security and notice to consumers when and if a data breach might occur. Each and every time we have become so engaged, others in the policymaking arenas, who wish to stray beyond data security into other areas, such as online privacy, have either consciously or unconsciously side-railed any meaningful and necessary federal legislation. There is certainly a role for government, but it must be sparingly exercised and should not be the first option, as it is in Europe.

**7. Small and Medium-Sized Entities and Startup Companies.**

This is not a category which really applies to the Coalition, as our members are all large, multinational companies based in the US but doing business globally.

**8. The Role of the Government / Commerce Department.**

Having worked with the Commerce Department in this and in the previous Administration, it is our considered view that the Department's continued involvement, from both a political public policy as well as a implementation perspective, is necessary in order to provide the White House and Congress with a balanced view that incorporates all perspectives. The FTC plays an important role as the regulator of choice from within the "unregulated" community. But each of these entities are driven in part by its own vision of its specialized responsibility. Only the Commerce Department is positioned to arbitrate disagreements between the functional regulators and to help produce uniform public policy, in the form of research conducted in combination with the functional regulators, and actual coordination, where applicable, after which policy recommendations would then be approved by the White House for implementation or referred to the Congress for its consideration. The Department is also in the unique position to work with the functional regulators to assure that their oversight practices are consistent and that their resources are adequate. The Commerce Department also has relationships overseas through which they would be best positioned to try and harmonize their and our respective privacy regimes. The Department has been at the forefront of interaction with the OECD, the EU-US "Safe Harbor" framework and the APEC deliberations, and its global reach enables it to become an outspoken advocate for the proper balance between the marketplace and consumer privacy expectations.

**Conclusion**

Once again, the Coalition very much appreciates the opportunity to participate in the NOI, and we hope that our views will contribute to the Department's internal deliberations. Privacy is a broad and diverse subject, and it embodies the reasonable expectations of business and consumers alike. For that reason, and because it inevitably has economic implications, we encourage the Department to remain actively involved, as it represents the only entity within the Executive Branch which is uniquely positioned to reach across global and domestic boundaries and influence balanced and workable public policy solutions.

We look forward to the opportunity to remain involved and to be of whatever assistance we can be throughout.

Respectfully submitted,

/s/ Thomas M. Boyd

Thomas M. Boyd
Counsel

**U.S. DEPARTMENT OF COMMERCE**

**National Telecommunications and Information Administration**

---

| | | |
|---|---|---|
| Information Privacy and Innovation in the Internet Economy | ) ) | Docket No. 100402174-0175-01 |

# COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA")[1] hereby submits its comments in response to the Notice of Inquiry ("NOI") issued by the Office of the Secretary of the U.S. Department of Commerce , the National Telecommunications and Information Administration ("NTIA"), the International Trade Administration, and the National Institute of Standards and Technology (collectively "Department") on the nexus between privacy policy and innovation in the Internet economy.[2]

NCTA commends the Department for its recent creation of the Internet Policy Task Force and Privacy and Innovation Initiative, which seeks to engage in a policy analysis that balances the twin goals of preserving and enhancing innovation on the Internet while protecting individual privacy. The Department's recognition that privacy protection needs to be aligned with flexibility for innovators and new business opportunities is a critical input to the current privacy discussion among policymakers.

---

[1] NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 90 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest provider of high-speed Internet service ("broadband") after investing over $145 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to over 20 million customers.

[2] *Information Privacy and Innovation in the Internet Economy*, U.S. Department of Commerce, National Telecommunications and Information Administration, Notice of Inquiry, 75 Fed. Reg. 21226, April 23, 2010 ("NOI").

Indeed, innovation is the hallmark of the Internet ecosystem and "continues to drive U.S. commerce."[3] American businesses – from the more established to newly emerging – have developed and are developing information content, applications and services to meet consumers' needs and interests – supported by the electronic marketing of goods and services. Online advertising is the bedrock of the free content the public enjoys and often expects on the Internet and is essential to promoting the continued expansion of new content and services. And the rapid growth of high speed Internet services and online transactions over the past decade shows that consumers want and enjoy the benefits of e-commerce.

Targeted advertising, in particular, has many advantages for consumers. Advertising that is more relevant for the consumer is likely to be of more practical value to the consumer. Instead of receiving irrelevant ads, consumers receive information about products and services tailored to their specific interests based on prior purchases, and increasingly through self-managed preference profiles. Customized advertising enables them to make more accurate purchasing decisions in the marketplace, and more businesses, in turn, are empowered to compete by fostering their ability to reach receptive and intended audiences.

Consumers' actual behavior in the marketplace suggests that online advertising has not intruded significantly on their privacy interests. Yet the sophistication of data collection practices and a complex set of players and business models present concerns to some consumers about the collection and use of personal information online. Consumers are entitled to certain fundamental norms and ground rules that respect their legitimate privacy interests *and* are still flexible and adaptable enough to promote innovative and beneficial uses of online information. The complexity of the issues does not lend itself to definitive, line-drawing regulation that by

[3] *Id.* at 21227.

nature can not keep up with advancements in technology and unique user interests. The Internet is not static and customer expectations continually evolve. As NTIA Assistant Secretary Strickling recently observed: "the rate at which new services develop, and the pace at which users form expectations about acceptable and unacceptable uses of personal information, is measured in weeks or months."[4] Federal agency rulemakings take years and may result in "rules addressing services that may be long abandoned."[5] Similarly, as Federal Trade Commission Chairman Leibowitz recently stated:

> [S]o long as self-regulation is making forward progress, the FTC is not interested in regulating in this area. The FTC does not want to shut down responsible business practices or stifle innovative and efficient uses of the online marketplace – and we don't plan to do so. We want only, as behavioral advertising develops and spreads, to protect those two pillars of the growing, changing, thriving cyber-world: consumer choice and consumer control.[6]

From the cable industry's perspective, consumer choice and control over private data, providing clear notice and transparency of data practices, and protecting sensitive data are paramount to our companies' efforts to protect their customers' privacy.[7] This is not surprising. Cable system operators providing video services have long operated under a comprehensive

---

4 "Internet Policy 3.0: All Hands on Deck", Remarks of Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information, Internet Society's INET Series: Internet 2020: the Next Billion Users, April 29, 2010.

5 *Id.*

6 "Where's the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising", Remarks of FTC Chairman Jon Leibowitz at the National Cable & Telecommunications Association's Cable Show 2010, May 12, 2010.

7 *See e.g.* Testimony of Kyle McSlarrow, President and CEO, National Cable & Telecommunications Association, on Communications Networks and Consumer Privacy: Recent Developments, House Energy and Commerce Subcommittee on Communications, Technology and the Internet, April 23, 2009 at 3 (discussing that achieving and sustaining subscribers' trust requires adherence to a privacy framework addressing four main principles: 1) giving customers control; 2) providing transparency and notice; 3) safeguarding personal information and 4) providing customers with value; also noting that special care should be given to sensitive data, such as health or financial information, as well as protecting children online). *See also, In the Matter of A National Broadband Plan for Our Future* ("FCC NBP proceeding"), GN Docket No. 09-51, Public Notice, *Comments Sought on Privacy Issues Raised by the Center for Democracy and Technology*, NBP Notice # 29, DA 10-62, Comments of NCTA, Jan. 22, 2010 ("*NBP Notice #29*").

framework of protecting their customers' privacy pursuant to section 631 of the Communications Act.[8] Enacted in 1984, this provision:

- requires cable operators to provide annual written notice to consumers of the nature of personally identifiable information ("PII") collected, including clearly and conspicuously describing how it is used, disclosed to others, and maintained;

- prohibits cable operators from collecting PII over the cable system without prior customer consent, except as necessary to render service and detect service theft, and from disclosing PII without prior customer consent, except as necessary to render services or conduct other legitimate business activities related to rendering service;

- provides detailed requirements governing how subscriber records may be disclosed pursuant to court order;

- requires that subscribers be given access, at reasonable times and convenient locations, to all PII that is collected and maintained, and a reasonable opportunity to correct any errors in PII; and

- requires cable operators to take "such actions as are necessary" to prevent unauthorized access to PII, including destroying it if it is no longer necessary for the purposes for which it was collected and there are no pending court orders or requests for access to such information.

In providing digital voice service, cable providers comply with the privacy protections of Section 222 of the Communications Act regarding customer proprietary network information ("CPNI").[9] Between Section 631 and Section 222, the cable industry already operates in an enforceable privacy framework that substantively embodies well-recognized fair information principles.[10]

---

8 47 U.S.C. § 551.

9 47 U.S.C. § 222; 47 C.F.R. Part 64, Subpart U.

10 Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"; http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

The cable industry regards the protection of its customers' privacy as a fundamental part of our broadband Internet service. Cable companies operate pursuant to a robust set of self-regulatory principles and are working to incorporate and adapt well-accepted "fair information practices" to interactive advertising and related online activities. Moreover, privacy and security controls related to cable broadband access have become standard practice in protecting consumers from malware, spyware, viruses and other privacy invasions.[11]

Cable companies are exploring new broadband business models and network technologies with the full appreciation that new services must be deployed consistent with our long-standing commitment to protect customers' personal information and facilitate well-informed privacy decisions. No business benefits from disregarding customer privacy concerns and discarding their trust and confidence. Cable systems, in particular, operate in a highly competitive marketplace, and their ability to succeed depends on winning and retaining the trust of their customers.

As the Department and other federal agencies, as well as Congress, review the global and U.S. privacy legal and regulatory framework, we urge federal policymakers to adopt a privacy framework that incorporates the following major considerations:

First, the government should seek to rely on competitive market forces, existing safeguards and industry self-regulation to protect consumers' privacy interests rather than further regulatory mandates. In today's dynamic, competitive Internet ecosystem, reliance on market-driven business incentives to protect consumers' privacy – bolstered by self-regulation at the company and multi-stakeholder level – is the best course to ensure that entities collecting and using private consumer information meet widely-agreed upon standards for consumer choice and

[11] *See e.g.* FCC NBP proceeding, Comments of Time Warner Cable Inc. at 13 (June 8, 2009), citing variety of privacy tools; Comments of Comcast Corporation at 25 (June 8, 2009); NCTA Comments on NBP Notice #29.

control. Given the complexities involved in a rapidly evolving Internet world, where consumer concerns vary and new services and technologies must respond in these unique contexts, it is important for all industry stakeholders to continue to work together to establish best practices and self-regulatory principles.[12] These codes of conduct, backed by FTC and other government enforcement authority over unfair and deceptive practices, should give consumers the certainty and predictability that they need in an era of rapid data flow and use of personal information in the provision of Internet services.

The Department's review of existing self-regulatory principles may yield further recommendations to ensure that ongoing self-regulation meets consumer expectations of privacy and incorporates other privacy objectives but absent evidence of a breakdown in market-driven approaches, the government should not intervene with regulation that has the potential to constrain the development of online advertising, and innovative online content and services, and thereby undermine the growth and prosperity of our web-centric information environment.

Second, the government should fully take into account the privacy protection tools in place today and on the near horizon. The various tools currently being offered and in development will more fully engage consumers in their privacy choices and give them the ability to control their choices. As the Department notes, for example, there are new privacy-enhancing technologies and consumer information management tools that seek to effectively anonymize and aggregate personal information, as well as the emergence of innovative ways to make consumers more aware of data collection practices and make it easier for them to set their privacy preferences. Furthermore, consumer education goes hand-in-hand with personal data

[12] *See e.g*. FCC NBP proceeding, Comments of Cox Communications, "Improving the U.S. Broadband Experience" (industry should establish "meaningful and transparent self-regulatory principles or best practices for broadband data security, privacy and online safety") (June 8, 2009); Comments of Time Warner Cable at 12 (Sept. 4, 2009); Comments of Comcast Corporation at 26 (June 8, 2009); Charter Communications, Ex Parte, "Providing Regulatory Clarity to Enable Ad-Supported Models" (Sept. 15, 2009).

management tools in ensuring a well-informed and more engaged public on the use and sharing of their data.

The Federal Trade Commission's recent series of roundtables featuring a cross-section of privacy experts and technology demonstrations, as well as the Department's recent symposium on privacy and innovation, showed that technology can play a key role in ensuring that consumers' privacy interests are protected. We believe that current and next generation interactive tools combined with baseline self-regulation principles should empower consumers to direct their online experience. The federal government, working with the private sector, also can help raise awareness and educate consumers on how to create an Internet environment that addresses their individual privacy concerns.

Third, the privacy policy framework should remain technology neutral and should promote competitive entry of new innovative behavioral advertising and other online content and services. The government should refrain from policies that disadvantage new approaches to the delivery of marketing and information services or freeze today's online advertising models. And it should be cautious not to pick winners and losers by favoring certain technologies, and even inadvertently certain players, over new, yet-defined innovators and business opportunities. This will only artificially distort to the detriment of consumers what should continue to be a constantly-evolving and expanding Internet marketplace.

Today's headlines demonstrate that the dominant players in the online Internet commerce ecosystem – whose ranks do not include cable companies – are being called to answer for their privacy policies and practices as new applications are deployed. And recent events have shown that the gathering of personal data may implicate a host of entities that possess the means to collect and use personal data in a way that raises privacy concerns. From the consumer's

perspective, what matters are the clearly discernable privacy principles that apply to their usage of the Internet, not the technologies or business models operating in this space today or invented tomorrow.

The dynamic and complex broadband ecosystem presents new opportunities and challenges for protecting consumer privacy. As the Department weighs in on the global Internet privacy debate, we urge it to trumpet the benefits of new entrants in a marketplace characterized by rapid technological change and recommend policies that fulfill its goal of "the continued development of new business models and the free flow of data across state and international borders in support of domestic and global trade."[13]

[13] NOI at 21227.

## CONCLUSION

In a constantly-evolving online environment with many different actors and situations, the current dialogue addressing online privacy issues is producing the desired outcome – a concrete focus on developing privacy policies and imperatives for the 21st century Internet age. We believe that the government should encourage a framework that strikes the appropriate balance between legitimate privacy concerns and promoting the tremendous value of online information for consumers. And the emphasis should be on principles that both ensure a vibrant Internet that supports current and emerging content and services and protects consumers in the use and collection of their personal information. NCTA and its members remain committed to working cooperatively and constructively with the government and other stakeholders to address these issues.

Respectfully submitted,

**/s/ Rick Chessen**

Rick Chessen
Loretta Polk
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

June 14, 2010


*Promoting Convenience, Choice, and Commerce on the Net*

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
202.420.7482
www.netchoice.org

June 14, 2010

FILED ELECTRONICALLY

National Telecommunications and Information Administration
US Department of Commerce

In the Matter of the Request for Comments on
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01

**Comments of NetChoice on Information Privacy and Innovation in the Internet Economy**

NetChoice welcomes this opportunity to comment on the nexus between privacy policy and innovation. In its Notice of Inquiry (NOI), the Department of Commerce rightly recognizes that Internet commerce is vital to US innovation and prosperity, and that public policies can help or harm the growth of e-commerce.

NetChoice is a coalition of trade associations and e-commerce companies, plus over 13,000 small businesses that rely on e-commerce. NetChoice works to promote the integrity and availability of the global Internet, and is significantly engaged in privacy issues in the states, in Washington, and in international internet governance organizations.

NetChoice has a long history of breaking down regulatory barriers, beginning with helping travel agents, contact lens suppliers, and real estate brokers to use online innovations that clashed with legacy regulations designed to protect traditional business models. Today, NetChoice members face proposals to regulate social networking websites, tax out of state retailers, and restrict marketing to teenagers.

Privacy-related laws that specify how data can be collected, used and shared also create barriers to legitimate online commerce. As Internet commerce knows no borders, online companies have had to be vigilant and work vigorously to keep state laws roughly consistent when it comes to information privacy. So while there is a constant threat of new state privacy regulations,

online companies have thus far managed to avoid an unworkable patchwork of inconsistent laws here in the United States.

However, as our members expand to international markets, they need an effective advocate before national governments and intergovernmental organizations.

The Department of Commerce can be this advocate. The Department was a champion for online commerce through the administration of the US - European Union (EU) Safe Harbor Framework. We encourage further involvement by the Department to ensure that public policies related to consumer privacy—both here in the US and abroad—are flexible enough to allow the innovation we all want to see.

At the Department's recent symposium on privacy and innovation, one of the panelists, Leslie Harris of the Center for Democracy and Technology, remarked on how the US is often viewed by other countries as an outlier on privacy regulation.[1] Yet, she followed by noting that the US is the innovation leader in privacy-enabling technologies, and that we need to lead on privacy policy too.

NetChoice agrees that the US must lead in policy, just as our companies lead in privacy. In an effort to help the Department advocate for US interests on privacy and innovation, we focus our comments on four of the issues raised in the NOI: The US Privacy Framework Going Forward; US State Privacy Laws; International Privacy Laws and Regulations; and The Role for Government/Commerce Department.

**The Privacy Framework Going Forward** (NOI request 1)

The NOI seeks comment on "the current privacy framework" and ways in which such a framework needs adjusting to preserve and enhance innovation and privacy. This inquiry raises weighty issues that require more than a cursory analysis of current privacy-related laws and business practices. There must also be a fundamental discussion of what privacy is, how it is valued by some consumers, and what should be the proper focus of privacy-related public policy.

*Defining the privacy framework*

When studying the interplay between privacy and innovation, the Department should recognize that privacy is often an abstract and individualized concept. Privacy is a subjective condition people experience when they have power to control information about themselves. But privacy is also objective, and can be measured against terms of service or on the basis of unfair or deceptive practices that result in measurable harm to consumers.

[1] Department of Commerce, *A Dialogue on Privacy and Innovation*, Washington, DC, May 7, 2010, agenda available at http://www.ntia.doc.gov/internetpolicytaskforce/privacy/symposiumagenda_05072010.pdf

As the Italian Google case revealed, Europeans and Americans attach different meanings to privacy.[2] Europeans view privacy as a fundamental human-dignity right, to be protected by government. Americans view privacy as a protection *against* government overreaching, and as part of a consumer's relationship with providers of products and services.

Therefore, in today's globally connected society, innovation and international harmonization will be best served when policymakers focus on regulating objective aspects of privacy. Policymakers can and should continue to focus on a "harms-based" approach toward enforcement. The abuse and misuse of data should be considered unfair or deceptive.

The Obama Administration should encourage the Federal Trade Commission (FTC) to increase its enforcement efforts against unfair or deceptive data practices. Enforcement actions based on fraud and other unfair practices would be consistent with the NOI's reference to a "use-based model." This model would apply rules not to the collection of personal information, but to purposes for which personal information may be used.[3] However, any use-based privacy model should first derive its rules from consumers in the marketplace, as we explore in the next section.

*Consumer Expectations are Evolving*

As consumers disclose and share more of their personal information, users of online sites have been demanding more control over their information. Online companies are responding to customer feedback and creating more flexible and more granular privacy controls. Consumers have the ability to change their preferences or leave the service—the latter being the ultimate expression of customer feedback.

Consumer expectations about new technologies are always in flux. In the 1990s, telephone caller ID services that displayed the caller's phone number were feared by some as privacy invasions. But now we expect to see caller ID or message sender information before we engage with an incoming phone call, text message, friend request, or tweet.

Innovative social media technologies are creating new ways for users of all ages to create and share content and information. At the same time, online business models increasingly depend on advertising revenue to offer their products free of charge to their users.

Online companies are therefore experimenting with new ways to make advertising more relevant to their customers, often by collecting and using information from and about their users. With this rise in the commercial use of data about a person (but not necessarily personally identifying information), we have seen rising expectations from users about how much control they have in sharing their information.

Some of the most popular companies on the 'Net are working hard to meet these expectations. Last month, Facebook unveiled new privacy controls that simplify how its users control who can

[2] See Adam Liptak, "When American and European Ideas of Privacy Collide", New York Times, Feb 26, 2010, available at http://www.nytimes.com/2010/02/28/weekinreview/28liptak.html
[3] NOI at 21229.

see photos, comments, and activities.[4] Facebook also allows users to easily turn-off information sharing with third party applications hosted on Facebook.

Facebook is offering new privacy controls at the same time it introduces new product features. Facebook's "instant personalization" feature helps selected websites customize content based on a user's Facebook profile. And a "social plugin" for third party websites allows Facebook users to seamlessly recommend content or news articles to their friends.

Facebook's innovations help create a personalized and social Internet experience, and they do it through the sharing of information. For online services to truly maximize the value of new product features, they will want to encourage users to try them, and will set user defaults accordingly. As we explore in the next section, defaults for how and to whom users share information are an integral part of online innovations.

*Privacy Frameworks Must Preserve Flexibility in Setting User Defaults for new forms of Information Sharing*

The NOI clearly captures the challenge facing policymakers: "Our challenge is to align flexibility for innovators along with privacy protection."[5] No matter what the privacy framework, online services need the flexibility to set user defaults when changing functionality or adding new features.

Flexibility means that online companies should have the legal ability to make decisions on how to best carry-over a user's preference from a prior product version to a new one. It also means that online services should be able to make assumptions on user privacy preferences for new features.

These considerations matter whenever an online service tries to increase its social networking functionality. As an example, Yahoo recently announced that it will change how status updates appear in its Yahoo Mail service.[6] Like Google and Facebook before it, Yahoo is adding features that make user information more public. According to Yahoo:

> Before Yahoo! Updates is expanded to Yahoo! Mail where many more people will see their Contacts' activity, we want you to explore your Updates settings and make sure you know who can see what you're publishing. Even if you are among the many Yahoo!

---

[4] See Mark Zuckerberg, The Facebook Blog, May 26, 2010, available at http://blog.facebook.com/blog.php?post=391922327130

[5] NOI at 21227.

[6] See Michael Arrington, "Yahoo Expands Yahoo Updates, Tiptoes on Privacy", May 31, 2010 at http://techcrunch.com/2010/05/31/yahoo-expands-yahoo-updates-tiptoes-on-privacy/ that describes the change:
[C]urrently to see status updates for others in Yahoo Mail, you have to have a mutual follow, meaning both people have agreed to be "friends." You can then see that user's Yahoo status updates as well as updates on third party services that they have added to their Yahoo profile as well. In the new version there will no longer be a requirement for a mutual follow. So, like on Twitter, users can follow whomever they choose. This isn't actually a dramatic change for Yahoo, since users can follow others in this way already on Yahoo Messenger.

> users who haven't ever generated an update, we want to encourage everyone to actively manage these settings. Because the majority of events listed within Updates are inherently public activities, our defaults are set to allow anyone to see them (that is, for people over 18; we have different defaults that are age-appropriate for people under 18 – learn more in our FAQ).[7]

As online services add features and functionality, they will strive to seek a balance. They will want to respect previously expressed user preferences, while defaulting settings so that people see and are encouraged to use new features.

In the case of Yahoo, its Messenger service makes user updates public, so Yahoo will also make updates public in Mail. But in another sense, Yahoo must make assumptions—that users want to have their updates be public. Hence the rationale for Yahoo's explanation: *Updates are inherently public activities, our defaults are set to allow anyone to see them*.

Yahoo is also making it easy for users to control and opt-out of sharing status updates:

> "[Y]ou can easily limit who sees your Updates stream either by editing the controls for each specific activity…or by turning your Updates stream off entirely in one simple step."

Thus the challenge for policymakers is a similar calling for online companies—"align flexibility for innovators along with privacy protection"—in order to earn consumer trust. But if the threat of regulation becomes too great, companies will be afraid to take risks and introduce new services. A privacy framework that mandates opt-in arrangements would force many online services to perpetually maintain original settings and limit innovative business models. In the case of Internet commerce, strict consistency will become a brake on innovation.

Companies won't always find the right balance right away. Online services need the freedom to experiment with new ways for publishing and sharing information, with the expectation that they will adjust quickly based on user response.

As the social web matures, we'll see more and more sites confronted with this balancing act. They'll need to carryover preferences from old to new versions, and make assumptions on what information most users will or will not want to disclose. If sites get it wrong, some users will change their settings, while others will leave—ultimately, either is a better expression of user preferences than any law or regulation.

In conclusion, no matter what the privacy framework, it should be flexible and based on harmful uses, not theoretical abuses.

**US State Privacy Laws** (NOI request 2)

Below we discuss some recent state proposals to regulate online privacy in ways that would harm innovation on the Internet.

[7] Yahoo Corporate Blog, available at http://ycorpblog.com/2010/05/31/yahoo-privacy/

*Examples of State Legislative Activity*

NetChoice has been active in state legislatures to oppose laws that govern how companies collect, use and disclose personal data. Compliance with a state law by a company that operates websites available nationally (and internationally) is difficult and burdensome.

For example, NetChoice was lead plaintiff in a lawsuit challenging a Maine law that placed broad restrictions on the collection and transfer of personal information about minors. The law, passed in 2009, required websites to obtain "verifiable parental consent" before collecting personal data or marketing to Maine teens under the age of eighteen.

As a result of the lawsuit, Maine's Attorney General agreed not to enforce the law, pending revision or repeal by the legislature. As a result, the legislature organized a two-day joint hearing of the judiciary committee where NetChoice and a number of affected companies filed comments and traveled to Augusta to testify and persuade the committee to recommend full repeal of the law.

Earlier this year, Maine's Senate took-up legislation to repeal the law, but added replacement language focused on medical products and services. The new language would have required verifiable parental consent for showing ads relating to any health concerns. Eventually, the sponsor dropped her replacement language and the legislature repealed the marketing to minors law.

NetChoice has also opposed online safety-related legislation that would have had serious privacy implications. Last year, New Jersey proposed a law to extend the federal COPPA requirements from children twelve and younger to include teens up to 17 years old.[8] As is the case under COPPA, Internet services and Web sites would have been required to obtain verifiable parental consent when attempting to collect personal information from teenagers in addition to children twelve and under.

The bill would have extended COPPA's reach to apply to all Internet websites "directed at adolescents" and dramatically altered the innovative landscape of online services. It would have effectively required parental consent before any teenager could obtain an e-mail address, Instant Message address or register to receive information from a website. It would also have clearly applied to many social networking websites.

The bill was withdrawn by its sponsors before it could be heard in committee, after a groundswell of opposition from child safety experts, public interest groups, legal experts, and industry.

Another variant of online safety bills are of the same variant of COPPA and the New Jersey bill, but would apply only to social networking websites. These bills required parental consent before a minor can become a registered user of a social networking website. Variants of this

[8] 213th Legislature, Reg. Sess. (N.J. 2008), available at http://www.njleg.state.nj.us/2008/Bills/A0500/108_I1.PDF

requirement were introduced in Connecticut, Georgia, Mississippi and North Carolina in 2007 or 2008, and in Illinois last year.[9]

The typical bill language used to create a duty on social networking websites to obtain verifiable parental consent goes something like this:

> No owner or operator of a commercial social networking website shall allow a minor using a protected computer to create or maintain a personal webpage on a social networking website without first obtaining the permission of the minor's parent or guardian and without providing the parent of guardian access to the personal webpage at all times the commercial social networking website is operational.

The typical bill language used to create a duty to authenticate age and parental identity is as follows:

> Any owner or operator of a social networking website shall adopt and implement procedures to confirm the identity and age of parents or guardians who are providing permission for their minor children and members at the time of registration by validating the accuracy of personal identification information submitted at the time of registration.

Finally, social networking websites would have to retain permission records, perhaps indefinitely:

> The owner or operator of a social networking website must keep either a hard copy or electronically scanned copy of the written permission of the parents or guardians in a database maintained by the social networking website.

NetChoice worked with other members of the online community to present the privacy pitfalls involved with collecting and keeping additional personal information just in order to comply with new legislation. To verify parental consent, for example, online services must require parents to provide personally-identifying data (such as credit card information). As a result, private companies would have to store vast amounts of parents' personal information and, by doing so, increase customers' vulnerability to security breaches and identity theft.

A 2008 report by the Berkman Center's Internet Safety Technical Task Force did not recommend remote age and identity verification for use by online forums and social networks, saying, *"there are significant potential privacy concerns and security issues given the type and amount of data aggregated and collected by the technology solutions…"*[10]

As mentioned above, state privacy laws do not yet present insurmountable compliance barriers. While there have been state legislative proposals on privacy, industry has thus far minimized the

---

[9] H.B. 6981 (Conn. 2007), S.B. 59 (Ga. 2008), S.B. 2586 (Miss. 2008), S.B 132 (N.C. 2008), HB 1312 (Ill. 2009).

[10] John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), available at http://cyber.law.harvard.edu/pubrelease/isttf/

patchwork problem for interstate e-commerce. However, as we note in the next section, if Congress were to enact federal privacy law, it should occupy the field and prevent states from burdening online companies with multiple, inconsistent laws.

*The Federal / State Balance: Preemption Should Establish a Ceiling, While Allowing for State Enforcement Action*

If Congress were to enact legislation to regulate information collection, use and sharing, it should broadly preempt the states. Different state-level privacy laws and regulations would increase compliance costs and frustrate the product development process of online services. Congress should therefore establish a ceiling, not merely a floor, for privacy-related legislation.

But we should emphasize that federal preemption does not mean that states are kept off the field entirely. Rather, states can and should retain their consumer protection role. The Department should coordinate with the FTC and state attorneys general to target bad actors that impact online commerce by reducing consumer trust and confidence.

Aggressive enforcement will help foster a better climate for innovation than would expanded regulation. New regulations are followed only by legitimate businesses who were already complying with the old regulations. Bad actors, on the other hand, ignore both old and new regulations with impunity (e.g., Spammers are still spamming even after the FTC issued new regulations pursuant to the CAN-SPAM Act). Moreover, the Internet knows no borders, and delivers advertising and services to US consumers from foreign companies that cannot be compelled to follow US law.

Still, as we discuss in the next section, the Internet allows for global commerce. Federal preemption applies to states, but will not impact the privacy laws of other countries. FTC enforcement does not apply extraterritorially. Continued innovation and growth for online companies based in the US means that they will have to navigate international privacy laws and regulations.

**International Privacy Laws and Regulations** (NOI request 3)

At the Department's symposium on privacy and innovation last month, we heard how laws are keeping us apart even as technologies are trying to bring us together.[11] We also heard that government demands for data from the private sector are fatal to international cooperation.[12]

These comments underscore the broad impact that government policies have in the information economy. Laws and regulation can help promote or harm the growth of online commerce across jurisdictions, particularly because data flows today are much more complex than they were even a decade ago. Simple one-way transfers between one country and another have been replaced by multinational corporations that transfer data across multiple jurisdictions on a daily basis.

[11] Fred Cate, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[12] Ibid.

As data flows become more complex and multi-jurisdictional, there must be a mutually recognized framework for information privacy. The Department's symposium exposed a lot of issues that remain to be addressed:

- EU data protection law requires multiple intercompany contracts, which are disproportionately expensive and challenging for small businesses.[13]

- US companies often launch new services in an unfinished "beta" format, but the EU doesn't favor this approach and wants privacy locked-down before a service is launched.[14]
- Inconsistent privacy regulations result in opportunity costs, because new products are not launched, or are not exported to other countries.[15]

The Department can work with foreign regulatory authorities and multi-governmental organizations to develop new mechanisms for achieving mutual recognition. The EU's policy toward Binding Corporate Rules (BCRs) could emerge as a key element of a mutual recognition framework. BCRs are corporate codes of conduct that legally bind a company and its partners to EU-compliant data management systems.[16] BCRs allow companies to share personal data on EU citizens, in-house and worldwide.

However, BCRs represent a serious commitment for companies, and they are out of reach for most American companies. They require extensive time and financial resources to implement. There are also ongoing costs for compliance, internal control and supervision, and auditing. These costs challenge even the largest of companies, but can be prohibitive for small businesses. Still, BCRs are a promising mechanism for cross-border compliance that should be made more widely available to companies of all sizes.

The Department should work with the European Commission to greatly simplify the BCR process and make it more accessible to small businesses. There should also be new rules that encourage and reward member states that implement BCRs. For online companies to be able to take full advantage of the BCR process, European Data Protection Authorities (DPAs) need to fully embrace the BCR process, as only 19 EU member states collaboratively work on BCR applications while others flatly refuse to recognize them.

**The Role for Government/Commerce Department** (NOI request 8)

Online companies welcome an increased role for the Department in promoting online commerce in a privacy-related context. As previously discussed, the Department should work with the FTC to step-up state and federal enforcement against unfair or deceptive information practices.

---

[13] Jim Halpert, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[14] Dan Burton, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[15] Fred Cate, *A Diologue on Privacy and* Innovation, Washington, DC, May 7, 2010.
[16] Christopher Wolf and Timothy P. Tobin, *The European Union ("EU") Data Privacy Directive* (2007), Proskauer on International Litigation and Arbitration: Managing, Resolving, and Avoiding Cross-Border or Regulatory Disputes.

The current process through which the FTC makes rules, as established by the Magnuson-Moss Act, is a proven and effective vehicle for the regulation of business and provides the Commission with enforcement authority to punish businesses that act in a deceptive manner or in ways that are unfair to the consumer.

But there's another important role for the Department: an international ambassador for innovative American online companies. Now is a critical time for online commerce as international policymakers assess their approaches to privacy. The Department can play an important role as a government-to-government advocate for flexible international rules to promote continued innovation and economic growth.

The Department already has an excellent track record in a number of international fora. ITA currently administers the US-EU Safe Harbor Framework and has worked with the Asia Pacific Economic Cooperation (APEC) member countries to develop a privacy framework. Both are successful efforts to mutually recognize different compliance laws and allow for innovation across borders.

As an international spokesman for online service innovation, the Department can promote privacy laws that are flexible enough to permit innovation, and oppose static laws that undermine consumer interests in improved online services. And as a government agency speaking to other government agencies, the Department can bring credibility and leverage that cannot be matched by corporate interests alone.

We note that this month NTIA Assistant Secretary for Communications and Information, Larry Strickling, is scheduled to meet with Neelie Kroes, EU Commissioner for the Information Society. Such a high-level meeting provides the opportunity to identify national regulations that become international barriers to innovation.

NetChoice members encourage the Department to increase its engagement with the EU, OECD, and at the United Nation's Internet Governance Forum. The Department should remain a consistent voice of American business interests in Europe, Asia and globally.

Respectfully submitted,

Steve DelBianco, Executive Director
Braden Cox, Policy Counsel

*NetChoice is a coalition of trade associations and e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. More information about NetChoice can be found at www.netchoice.org*

June 14, 2010

Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, D.C. 20230

Submitted electronically to: privacy-noi-2010@ntia.doc.gov

Re: Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01

## Introduction

The Network Advertising Initiative ("NAI") appreciates the opportunity to provide Comments to the Department of Commerce's Internet Policy Task Force ("Task Force"). The NAI is a coalition of more than 40 leading online advertising companies committed to developing actionable self-regulatory standards that establish and reward responsible business and data management practices and standards.[1] The NAI maintains a centralized choice mechanism that allows consumers to opt out of online behavioral advertising by some or all of the NAI's member companies, across the many different Web sites on which NAI members provide such targeting (at www.networkadvertising.org).

The NAI's comments will address the Task Force's questions as applied in the context of online behavioral advertising. Specifically, these comments: (1) explain how the free flow of data has been critical to innovation on the Internet by enabling new advertising models that permit increasingly diverse content and services to be offered to consumers free of charge; (2) address some of the Task Force's questions with respect to the U.S. privacy framework going forward, with particular emphasis on the importance of self-regulation; and (3) describe privacy-enhancing

[1] The NAI currently comprises 45 companies that span a significant cross section of the online advertising marketplace, including all 15 of the largest ad networks, as well as the leading data exchange and marketing analytics services providers. *See* comScore Media Metrix, *comSCore Releases December 2009 Ranking of Top 15 Ad Networks*, at http://www.comscore.com/Press_Events/Press_Releases/2010/1/comScore_Releases_December_2009_Ranking_of_Top_Ad_Networks.

technologies that have recently been developed by the NAI and its member companies to offer consumers greater transparency and choice with respect to the collection and use of data for online advertising.

## I. The Free Flow of Data is Critical to Ad-Supported Internet Innovation

As the Task Force recognizes, "companies need clear policies that enable the continued and free flow of data."[2] The free flow of data has been critical to the rapid growth of Internet content and services supported by advertising revenue.

*Role of Online Advertising in Innovation of the Internet*

Over the past 15 years, the World Wide Web has provided consumers access to an incredible variety of new content and services, ranging from online news, blogs, and other content to e-mail, search, social networking, video, and other Web-based services. The explosion in Web services and their ease-of-use have transformed consumers' ability to access public information and entertainment, and created entirely new platforms for community and collaboration. Web-based technologies have also radically enhanced the ability of small businesses and specialty content providers to establish and connect with new audiences, creating new jobs and substantially increasing the diversity of public discourse. Consumer consumption of such Web services has continued to grow rapidly.[3]

Advertising revenues have permitted the great majority of these Web sites and services to be provided to consumers free of charge. Instead of requiring visitors to register and pay a subscription fee, the operators of Web content and services subsidize their offerings with various types of advertising. These

---

[2] NOI at 21227.

[3] *See generally* Center for the Digital Future, USC Annenberg School for Communication, *Highlights from the 2009 Digital Future Report* (April 2009), *available at* http://www.digitalcenter.org/pdf/2009_Digital_Future_Project_Release_Highlights.pdf (noting that 51% of consumers prefer ad-supported online content); The Nielsen Company, *Television, Internet and Mobile Usage in the U.S. – A2 M2 Three Screen Report* (1st Quarter, May 2009), *available at* http://blog.nielsen.com/nielsenwire/wpcontent/uploads/2009/05/nielsen_threescreenreport_q109.pdf (noting continued growth in monthly Internet usage generally by over 160 million U.S. users, and of online video in particular). Cisco expects Internet traffic to grow fivefold by 2013. *See* Cisco, *Cisco® Visual Networking Index (VNI) Forecast and Methodology, 20082013* (Summary, June 2009), *available at* http://newsroom.cisco.com/dlls/2009/prod_060909.html. *See also* IAB/Hamilton Consultants Inc., Drs. John Deighton and John Quelch, *Economic Value of the AdvertisingSupported Internet Ecosystem* at 4 (June 10, 2009), *available at* http://www.iab.net/economicvalue (estimating that the advertising-supported Internet accounts for $300 billion of economic activity).

advertising revenues provide the creators of free Web content and services – site publishers, bloggers, and software developers – with the income they need to pay their staffs and build and expand their online offerings.

Display advertisements – sometimes called "banner" ads – are an important means by which many Web content and services providers (also called "Web publishers") generate such advertising revenue. Display-related ads generated approximately $8.0 billion in advertising revenue even during the recessionary period of 2009.[4] Among other things, display ads serve a vital role in online commerce by enhancing consumer brand awareness and Web traffic to retailers.[5] The Web sites that publish banner ads have a dual incentive to ensure that they serve their users with the most relevant ads possible: not only do more relevant advertisements generate greater user response and revenue for the publisher; greater ad relevance enhances the user experience and avoids the potential nuisance effect to users from less customized marketing.[6]

While "contextually" targeted ads (such as an ad for ocean cruise on a Web page devoted to Caribbean travel) can sometimes offer the most direct approach to reaching consumers, contextually-targeted advertisements are not feasible for every type of Web content. An online photo sharing service, or an online newspaper's section devoted to international affairs coverage, for example, often are not readily suited to contextual advertisements. Web publishers therefore must rely on other potential attributes of their Web site visitors to help ensure ad relevance, such as

---

[4] *See* Interactive Advertising Bureau, *2009 IAB/PricewaterhouseCoopers Internet Advertising Revenue Report*, at 9 (April 2010), *available at* http://www.iab.net/media/file/IAB-Ad-Revenue-Full-Year-2009.pdf). The report notes that display-related advertising includes display banner ads (22% of 2009 full year revenues or $5.1 billion), rich media (7% or $1.5 billion), digital video (4% or $1 billion), and sponsorship (2% or $383 million). *Id.* Moreover, e-commerce providers separately provide a substantial amount of proprietary advertising, encouraging commerce. IAB/Hamilton Consultants Inc., Deighton and Quelch, *Economic Value of the Advertising Supported Internet Ecosystem, supra* note 2 at 3. Of the amount spent on display advertising in 2008, it is also estimated that online behavioral advertising generated $775 million in revenue. *See* eMarketer, "Behavioral Targeting: Marketing Trends" (June 2008), *available at* http://www.emarketer.com/Reports/All/Emarketer_2000487.aspx.

[5] See AdAge, "Why Search May Not Click for Retailers: Consumers Going Directly To Retailers' Sites for Six Out of Ten Visits" (Nov. 3, 2009) (summarizing Nielsen Online survey results that less than 10% of online retailers' Web traffic comes from search engines, and that 61% results from consumers choosing to visit retailers' sites directly), *available at* http://adage.com/digital/article?article_id=140089.

[6] A TRUSTe study found that when online advertising for products and services is not relevant to consumers' wants and needs, 72% of consumers find the experience intrusive or annoying. *See* TRUSTe, *2008 Study: Consumer Attitudes about Behavioral Targeting* (March 28, 2008).

registration information reflecting their gender, age, or zip code; or, alternatively, other potential interests of their users inferred from prior Web activity, either on the publisher's site or elsewhere on the Web. And even for large Web sites or services providers, there is no assurance that they will be able to sell their entire potential advertising inventory at rates sufficient to support their operating costs.

Smaller-scale Web publishers – such as blogs and specialty interest content sites – face an additional challenge. The monthly audiences of these sites vary in size from hundreds of thousands to millions of visitors.[7] Such small Web publishers cannot employ their own dedicated sales force to sell banner inventory to potential advertisers. More importantly, the smaller audiences of such sites do not easily lend themselves to the execution of large-scale brand advertising campaigns preferred by major companies.

Over the past decade, technological innovation designed to bring more efficient and scalable approaches to online advertising has enhanced the potential revenue opportunities for both large and small Web publishers. Advertising networks, exchanges, and other business models constantly innovate to allow Web publishers to find the revenue needed to continue providing the content and services consumers want. These businesses, large and small, help to connect advertisers to interested audiences, while at the same time enhancing the relevance of the advertisements served to users. The important functions these companies provide include:

- Acting as intermediaries for Web publishers and advertisers, by acquiring unsold impressions from both large and smaller Web content sites, and aggregating them into broad potential audiences for advertisers (for example, generating a multi-site campaign for a movie's opening weekend);

- Supporting a variety of more flexible pricing models for advertisers, including cost-per-impression (CPM) pricing preferred by brand awareness advertisers; or cost-per-action or click (CPA or CPC) pricing favored by advertisers looking to generate direct online sales (for example, banner ads for online universities);

- Offering niche-based approaches for particular types of publishers (ad networks focused on auto or women's interest publisher sites); and

---

[7] The statistical diversity of smaller Web sites outside the large-traffic Web sites is sometimes referred to as the Web's "Long Tail." *See, e.g.,* Interactive Advertising Bureau, *I Am the Long Tail* (2009), *available at* http://iamthelongtail.com/ (offering video examples of the extraordinary diversity in subject matter and business types of small Web publishers).

- Using online advertising technologies to aggregate insights from single or multiple Web publishers to enhance the relevance and quality of user advertisements.

The technological innovation in the online advertising industry has grown exponentially even over the last year, bringing increasingly efficient and scalable approaches to online advertisers and publishers. Specifically, the advent of "real time bidding" and the growth of advertising exchanges have resulted in automated, algorithmic trading that allows advertisers to find optimal ad impression opportunities. Rather than requiring advertisers to purchase guaranteed advertising blocks on fixed, pre-negotiated prices, real-time bidding creates a far more efficient liquid market.[8] Publishers are able to fetch higher revenue for their inventory because advertisers can find, in real time, the audience most likely to be interested in their ads, resulting in optimal revenue for each ad impression. These models also benefit advertisers by giving them increased transparency into the audiences for their campaigns, resulting in greater flexibility, better value, and the ability to fine-tune media buys to meet audience needs.[9] Publishers and advertisers are also able to dynamically reduce irrelevant, uninteresting ad impressions that generate scant response. Consumers, in turn, get increasingly tailored and appealing web experiences based on their inferred preferences.

This technical innovation has provided myriad benefits to consumers, publishers, and advertisers. At the same time, the advertising networks, exchanges, and other online advertising business companies represented by the NAI have also engaged in extensive innovation around protecting consumers' privacy, and providing consumers with increased transparency and meaningful choice with respect to online behavioral advertising. Those innovations are discussed below.

*Benefits of Online Advertising Innovations to Consumers, Publishers, and Advertisers*

Consumers

The online advertising technological innovations developed by NAI member companies provide considerable economic and non-economic benefits across the entire online ecosystem, including consumers, publishers, and advertisers. From the perspective of the consumer, these benefits include the following:

- As previously discussed, the increased revenues associated with relevant advertising are vital to supporting the continued growth in ad-supported

---

[8] "Getting Real: Ad Exchanges, RTB, and the Future of Online Advertising" desilava & phillips LLC White Paper, at 4-5 (March 2010), *available at* http://www.mediabankers.com/PDF/Getting%20Real%20White%20Paper.pdf.

[9] *See id.*

Web content and services, which remains the predominant business model;[10]

- Online advertising makes useful information available to consumers, including information about product availability and comparative pricing;[11]

- Online advertising models using targeted information is of particular importance for smaller Web publishers, helping them generate the revenue needed to sustain a greater diversity of content offerings and viewpoints; and

- Ad-supported business models continue to remain the principal source of venture and investment capital for innovation in Web services that have enjoyed rapid consumer adoption (social networks, *e.g.*).

Publishers

From the Web publisher perspective, online advertising technologies enable and preserve the ability to operate their sites free of charge, without adopting subscription requirements that might significantly limit the size of their audience. A recent study commissioned by the NAI and performed by former Director of Consumer Protection for the Federal Trade Commission, Howard Beales, demonstrated that the average CPM paid for behaviorally-targeted advertising enabled by NAI member companies is twice as much as the average CPM for run of network advertising, and that the majority of ad network display ad revenues flow back to publishers because they are used to acquire inventory.[12] Additionally:

- Large Web sites derive incremental revenue for the sale of ad impressions that they themselves cannot sell, and that would otherwise generate no income;

---

[10] Most newspapers, for example, have not achieved broad-based adoption of fee-based services. *See* http://newsosaur.blogspot.com/2010/02/why-many-newspaper-pay-sites-may-fail.html#comments; http://newsosaur.blogspot.com/2010/01/only-24-subscribe-at-newspaper-pay.html (citing survey of newspaper sites that have established pay walls showing only an average of only 2.4% of paying subscribers).

[11] *See generally* Lenard & Rubin, "In Defense of Data: Information and the Costs of Privacy" (Technology Policy Institute, May 2009), at http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

[12] Howard Beales, "The Value of Behavioral Targeting" (March 24, 20101), *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

- Smaller Web sites – for example, specialty interest sites or regional online newspapers – can have their available advertising impressions aggregated into combined audiences attractive to larger-scale advertisers who may pay higher rates and thereby provide them the revenue they need to continue to operate; and

- Both types of Web sites gain access to online advertising technologies that enable them to serve more relevant and profitable ads on portions of their sites that do not lend themselves to contextual advertising approaches.

Advertisers

Finally, the innovations around online advertising provide advertisers the ability to reach an increasingly fragmented Web audience, as online usage continues to diversify across an ever-broader array of content and services:

- Through more relevant ads served to increasingly-focused audiences, the advertiser eliminates wasteful spending on irrelevant ads (for example, automotive advertisers can significantly reduce their advertising expenditures by serving ads for a new car model only to users who have actually expressed interest in that model by researching it, rather than blanketing a wider audience with such ads);

- Larger advertisers gain access to audiences that may be distributed across a great variety of small Web sites, and avoid the otherwise prohibitive costs of attempting to negotiate their ad campaigns on a site-by-site basis;

- Smaller-scale advertisers gain new opportunities to reach focused audiences online that would not have been available to them in the offline world;

- Technologies like retargeting allow an advertiser to offer an improved price offer to a prior visitor to the advertiser's Web site;

- Behavioral advertising technologies result in a several fold increase in user response;[13] and

- Compared to other forms of advertising, online ads continue to offer far greater insight into the effectiveness of advertisers' spending, as well as greater flexibility for advertisers to pay only for ads that actually produce

[13] *Id.* at 12-13.

a result (performance-based ads that may be particularly important for industries with limited ad budgets).

## II. US Privacy Framework Going Forward

The existing U.S. privacy framework, including self-regulation, has enabled the rapid growth of Internet content and services described above. Under this framework, online advertising technologies have flourished and publishers have found ever-expanding methods of supporting their content and services. At the same time, robust self-regulatory regimes have developed (against a backdrop of FTC enforcement) to provide baseline rules concerning the collection and use of consumers' data for advertising purposes. Any adjustments to the existing privacy framework must be carefully calibrated to preserve the growth of the Internet economy as well as the significant advances in privacy protection already provided by self-regulation.

Robust self-regulatory regimes monitored by third parties like the NAI play an important role in ensuring that companies that handle consumers' information are accountable for the commitments they make. The NAI's compliance program is modeled on the Commerce Department's EU self-regulatory framework. It establishes a set of minimum performance–based benchmarks, described in detail below, governing the collection and use of data for online advertising purposes. To participate in the NAI, all member companies must make a public attestation to their commitment to those rules, and this attestation is enforceable by the FTC. In this way, the NAI and other privacy self-regulatory frameworks weave basic privacy benchmarks into the business models of their members, thereby setting the stage for privacy by design.

At the same time, self-regulatory regimes like the Department's EU Safe Harbor and the NAI provide member companies flexibility with respect to the technical implementation of baseline principles. Self-regulation is scalable to large and small companies, and accordingly does not needlessly hamper innovation around the development of products and services. And it *encourages* innovation around the protection of consumers' privacy and the development of new tools to provide consumers increased transparency and choice with respect to the collection and use of their data, both because companies are not limited by overly-proscriptive rules and because self-regulatory programs promote and ease the sharing of best practices with respect to privacy practices and tools. When provided performance-based objectives that allow for flexibility in technical implementation, companies can far better implement consumer-facing tools that are adapted to their particular business models.

Another advantage of self-regulation is that allows for continuing input from "users and civil society,"[14] including consumers, policy makers, and advocates. The

[14] *See* NOI at 2129.

NAI, for example, put out its draft Code of Conduct for public comment. The comments provided to the NAI played a critical role in the ultimate Code of Conduct adopted in December 2008. In addition, the NAI responds to and investigates as necessary complaints raised by consumers, as well as concerns raised by the press and privacy advocates. More informally, the NAI and its member companies constantly engage in a dialogue with regulators and advocates concerning best practices for the protection of information collected and used for online advertising. Such input allows for the constant evolution of privacy-enhancing technologies.

Finally, self-regulation can reflect the advantages of the United States' sectoral approach to privacy. That approach implicitly recognizes that some data, such as that related to financial account numbers, health conditions, and children, is more sensitive and thus deserving of greater protection than others. The NAI Code, for example, requires opt-in consent for use of any such data for marketing purposes. While certain "minimum rules" governing all data – such as those adopted by the NAI – may be appropriate, law, regulation, and self-regulation should reflect that, even when used for marketing purposes, not all forms of data collection and use are equally material to consumers.

A proscriptive legislative or regulatory model would lack the adaptability and scalability of self-regulation. As discussed above, much of the diversity and utility of the online content and services popular with consumers today has developed as a result of advertising revenues, fueled in part by technological advances in the ability of companies to find audiences for their advertisements across websites. An overly-proscriptive legislative or regulatory framework for privacy could stifle this innovation and negatively impact the myriad of ad-supported content and services available to consumers today. Indeed, a recent study demonstrated that even modest privacy regulation has serious impacts on the effectiveness of ads served – and thus ultimately on the price publishers can fetch for their inventory and use to support the content and services they provide consumers.[15] Significant impediments to the collection and use of even non-personally identifiable information for marketing purposes could force online publishers to rely solely on contextual advertising, greatly limiting the ability of publishers to obtain the maximum revenue for their available advertising inventory. It is accordingly apparent that regulators and policymakers should tread lightly in this area if they hope to preserve a vibrant Internet. If "minimum or default

---

[15] *See generally* Avi Goldfarb and Catherine E. Tucker, Privacy Regulation and Online Advertising (May 19, 2010), *available at* http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1611803_code512675.pdf?abstractid=1600259&mirid=1. This study concluded that even moderate privacy regulation could reduce the effectiveness of ads so dramatically that online revenues for online display advertising could fall from their current level of $8 billion to $2.8 billion. *See id.* at 30.

requirements"[16] are incorporated into law, these requirements should be sufficiently broadly stated to permit different Web business models to develop their own frameworks for implementation, so as to not "freeze" technology or stifle innovation.

*Self-Regulatory Rules Governing Online Behavioral Advertising*

The NAI and its member companies believe that existing legal regimes and self-regulatory approaches strike an appropriate balance between privacy and innovation with respect to the collection and use of information for online advertising. The NAI believes that its approach, like the Commerce Department's Safe Harbor Program, could serve as a useful model for other self-regulatory approaches to privacy. While the NAI Code governs online behavioral advertising, its basic framework of attestation to a code of conduct, complaint mechanisms, periodic compliance reviews, and enforcement mechanisms is equally applicable to the collection and use of data for other purposes that are material to consumers.

While NAI member companies are prohibited from using PII for marketing purposes without opt-in consent, some consumers have expressed concerns with respect to the collection and use of data about them for advertising purposes. Self-regulatory organizations like the NAI, with a backdrop of FTC enforcement, have addressed these concerns by ensuring that consumers are provided meaningful notice and easy-to-use choice with respect to use of their information for online advertising purposes. Self-regulation of online behavioral advertising seeks to achieve an appropriate equilibrium: innovation on the Internet generally and in online advertising in particular continue to flourish, while consumers are provided ever-increasing transparency and easy-to-use tools for exercising choice with respect to behavioral advertising.

As noted above, the NAI sets and enforces rules by which all members must comply concerning the collection and use of data for online advertising. Specifically, all NAI members must publicly attest their commitment to the NAI Code of Conduct. The Code generally requires members to: (1) provide notice about their collection, transfer, and use of information for online advertising, both on their own websites and on the websites where data is collected for such purposes; (2) provide and honor consumers' choice with respect to the use of their information for advertising purposes (generally, opt out choice for non-PII and opt-in choice for sensitive information and PII); (3) provide consumers access to PII and other information associated with PII retained for online advertising purposes; and (4) provide reasonable security for such data. In addition, the NAI Code extends COPPA protections to non-PII, forbids the use of behavioral marketing data for purposes other than marketing, imposes particular obligations on companies with respect to the collection and transfer of PII and non-PII to be merged with PII for marketing purposes, requires members to make reasonable efforts to ensure that they obtain

16 *See* NOI at 21229.

advertising data from reliable sources, and limits the retention of marketing data.[17]

The NAI employs a variety of means to help ensure that its members adhere to the privacy commitments embodied in the NAI Code, including: (1) public attestations of compliance with its Code of Conduct (enforceable by the FTC); (2) annual reviews of member companies; and (3) a mechanism for consumer questions and complaints relating to NAI compliance. In the event of a compliance deficiency identified by any of these means that remains unaddressed by a member, the NAI also retains the power to impose a range of sanctions, further bolstering its enforcement powers. Together, these tools compose an effective accountability regime that complements governmental enforcement mechanisms, and that provides for meaningful assessment of participating companies' policies and practices with respect to the handling of consumer data. Despite the costs of enforcement, NAI member companies collectively understand that it *is* in their economic interests to maintain a strong self-regulatory regime.[18]

In addition to the adoption of its own Code of Conduct, the NAI also actively participated in the formulation of industry-wide self-regulatory principles for online behavioral advertising, across a broad spectrum of associations representing thousands of advertisers, publishers, and marketers.[19] The Associations Principles represent a significant widening of the self-regulatory approach to behavioral advertising. The NAI and its members are committed to supporting this initiative, and in particular the Principles' commitment to the provision of notice and choice by all players in the online advertising ecosystem and the deployment of "enhanced" notice (notice provided in or around the ad) mechanisms, described in detail below.

The NAI's policy-making role extends not only to the development and revision of its Code of Conduct, but also to the determination of specific policy responses to emerging issues of consumer concern. For example, when researchers focused attention on the question of whether Local Shared Objects (LSOs), such as Flash cookies, were being used to undermine consumer preferences for online advertising, the NAI consulted with its members and ultimately adopted a policy broadly limiting the use of LSOs like Flash cookies until such time as web browser tools provide the same level of transparency and control available today for

---

17 *See* Network Advertising Initiative's Self-Regulatory Conduct, *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf.

18 *See* NOI at 21229.

19 *See* DMA/IAB/ANA/AAAA/BBBB: Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising (July 2, 2009), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

standard HTML cookies.[20] Given the breadth of its membership, the NAI's willingness to establish such policies helps to reassure consumers that self-regulation of online behavioral advertising remains comprehensive for all relevant technologies.

## III. State of Privacy-Enhancing Technologies

Just as the NAI's member companies have supported technological innovation on the Internet by enabling and promoting the ad-supported content and services upon which consumers depend, the NAI and its member companies also have been responsible for advances in privacy-enhancing technical innovation. The rapid development of these technologies and tools demonstrates that companies increasingly compete on privacy grounds, and that the market, supplemented by an ongoing dialog with regulators, provides ample incentive for companies to innovate around privacy-enhancing technologies.

Industry's efforts to implement novel technological approaches to "enhanced" notice in or around ads offers an excellent demonstration of recent developments with respect to the delivery of notice and choice of behavioral advertising practices. Regulators and other thought leaders in the online advertising industry have suggested that consumer notice for online behavioral advertising might be enhanced through the provision of additional mechanisms that provide notice through the advertisement itself (i.e. by providing disclosures directly within, or immediately adjacent to, the ad). Several NAI members have deployed a variety of potential implementations of consumer notice in direct proximity to banner ads, which can inform potentially wider adoption by industry:

- Yahoo! has extensively tested a variety of implementations of notice "in or around" display ads, including significant Web publishers such as eBay;[21]

- FetchBack, a retargeting company, also deployed direct links to its Privacy Center (a single location incorporating consumer information and its opt-out link) within the ads it serves;[22] and

---

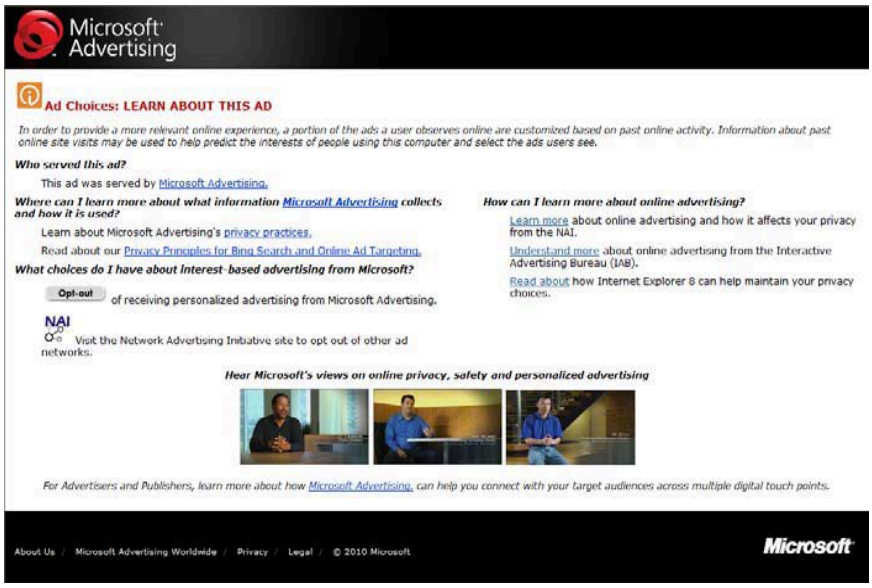
20 *See* http://networkadvertising.org/managing/faqs.asp - question_19.

21 An example of EBay's implementation is *available at* http://cgi6.ebay.com/ws/eBayISAPI.dll?DisplayAdChoice&w=1&y=3FwEhZwEEKTEEUCxpAAAsPQEEKVgCVC1RU1YtDlcCeA0AV3k%3D (accessed June 15, 2009).

22 *See* Press Release, *FetchBack to Provide Enhanced Notice in Behavioral Ads* (June 15, 2009), *available at* http://www.fetchback.com/press_061509.html.

- In October 2009, Google deployed clickable "Information"-icon links directly within the display advertisements it serves.[23]

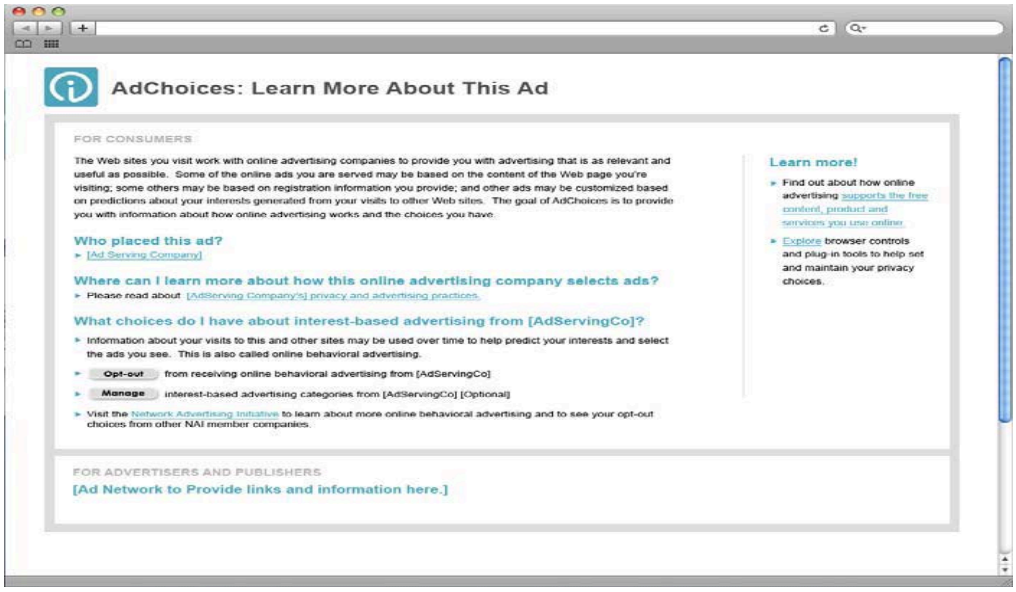
More recently, the NAI and the Interactive Advertising Bureau (IAB) released a set of technical specifications enabling enhanced notice in online ads. These CLEAR Ad Notice Technical Specifications are intended for use by all players in the online advertising ecosystem to convey metadata about the ad served during the ad serving process. The metadata conveyed includes information on which organization(s) served the ad, where to find their advertising policies, and how to opt-out of such targeting in the future. The specifications will allow advertisers and ad networks to begin offering a clickable icon in or near online ads that directs users to additional information, such as through a landing page, about online behavioral advertising and choices about such ads.[24] Two examples of how such information might be conveyed through a landing page are as follows:




---

23 *See* Pablo Chavez, Google Public Policy Blog, *Coming to an Online Ad Near You: More "Ads By Google" labels* (Oct. 15, 2009), *available at* http://googlepublicpolicy.blogspot.com/2009/10/coming-to-online-ad-near-you-more-ads.html. AlmondNet likewise offered a direct "Powered by Almondnet" hyperlink within behaviorally targeted banner advertisements for one of its product lines from 2004-2006, enabling consumers to access AlmondNet's opt-out choice more directly.

24 The NAI and IAB press release describing the specifications can be found at http://www.networkadvertising.org/pdfs/Clear_Ad_Notice_Tech_Specs_Release_Final.pdf. The specifications are *available at* http://www.networkadvertising.org/pdfs/CLEAR_Ad_NoticeApril2010.pdf.



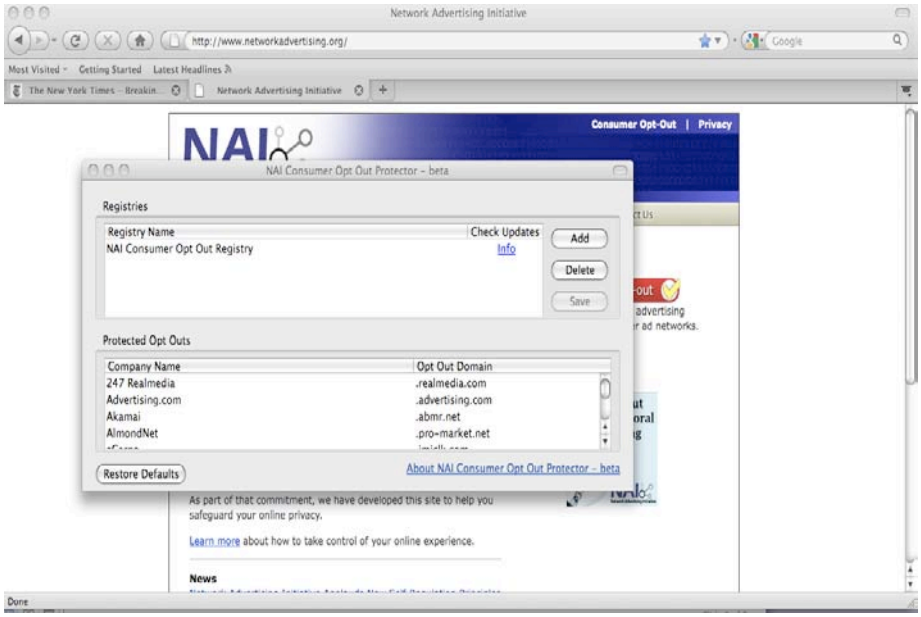

Another major advance in privacy-related innovation developed by NAI member companies (and applauded by regulators) is the deployment of ad preference management tools that allow consumers to see and adjust the inferred interest segments associated with their browsers. Such tools are already in use by seven NAI member companies, both large and small, and under development by several more.[25] The rapid adoption of preference managers illustrates how marketplace competition facilitates privacy-related innovation, and how self-regulatory frameworks like the NAI can facilitate adoption of such tools by smaller companies. The evidence available thus far from these tools indicates that they increase user trust that their information is appropriately collected and used; when consumers see the interest segments associated with their browsers, for example, they most often adjust those segments or do nothing at all, rather than "turn off" all targeting.[26]

---

25 For examples of preference management tools offered by NAI member companies, see BlueKai consumer preferences registry (http://tags.bluekai.com/registry); eXelate preference manager (http://www.exelate.com/new/consumers-optoutpreferencemanager.html); Google ad preference manager (www.google.com/ads/preferences); Lotame preferences manager (http://www.lotame.com/preferences.html); Microsoft Ad Preference Tool (https://choice.live.com/UserPreferences ); Safecount (http://www.safecount.net/yourdata.php); Yahoo! ad interest manager (http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/).

26 Exploring Privacy: An FTC Roundtable Discussion, December 7, 2009, Panel Two Transcript, at 7, *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/120709_sess2.pdf (Google's Alan Davidson explaining that four times as many people who come as visitors to the site change their preferences rather than opt out).

Still another recent technical privacy-protecting innovation by the NAI, building on software developed by NAI member company Blue Kai, is a Firefox browser Add On to protect user opt outs stored in browser cookies, pictured here.[27]




While the NAI has always given consumers the ability to opt out of the use of their information for advertising purposes through an opt-out cookie, some have raised concerns about the vulnerability of cookie-based opt outs to accidental user deletion. Leveraging extensible software developed by BlueKai that allows consumers to select multiple lists of opt out cookies (not just the NAI's), the NAI secured the participation of its entire membership to provide consumers with a tool that prevents opt-out cookies from being deleted when consumers delete their cookies, thereby providing them with a more durable opt-out mechanism.[28]

* * *

The NAI appreciates the chance to comment on these questions, and looks forward to working with the Task Force as it evaluates the nexus between privacy policy and innovation in the Internet economy.

---

27 The beta Add-On is available for download at: http://networkadvertising.org/staging/pre/managing/protector_license.asp.

28 Still another example of innovation around privacy with respect to advertising is the methods developed by companies to ensure that advertising profiles are not linked to PII. Microsoft, an NAI member company, has published a white paper on its efforts to ensure that it bases its ad selection solely on data that does not personally and directly identify individual users. *See* http://download.microsoft.com/download/3/1/d/31df6942-ed99-4024-a0e0-594b9d27a31a/privacy%20protections%20in%20microsoft%27s%20ad%20serving%20system%20and%20the%20process%20of%20de-identification.pdf.

Online Trust Alliance

Via electronic email to privacy-noi-2010@ntia.doc.gov

June 14, 2010

Office of the Secretary
National Telecommunications and Information Administration
International Trade Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Department of Commerce, Notice of Inquiry
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0238-02

The Online Trust Alliance (OTA) hereby submits its comments to the Department of Commerce's Notice of Inquiry, dated April 20, 2010.

OTA is encouraged by the dialog regarding the evolving role and importance of privacy protections and the way in which it balances the impact to the vitality of online services and commerce. Balanced legislation and market based incentives are needed to provide a framework for legitimate businesses to follow which neither imposes an unreasonable burden, nor prevents aggressive enforcement towards bad actors.

We agree on the importance of innovation to not only provide consumer choice and control, but to re-define it so it is intuitive and comprehendible. Ensuring public trust and confidence is the foundation for participation and the growth of the internet. We recognize this means the importance of moving from a harm based model to one of meeting evolving consumer privacy expectations.

For background, OTA was founded in late 2004 to address the global spam problem and the lack of standards and practices to help detect forged email. In the past six years, OTA has grown significantly. As an IRS approved 501c6 member based non-profit, we represent the broad internet ecosystem and are not beholden to any special interest group. OTA membership is comprised of over 70 business, industry and technology leaders who share our mission to enhance online trust while promoting business practices and technologies which support the vitality of ecommerce and online services. Through our members and organizational partners in over a dozen counties, OTA represents over 1 million businesses and 750 million consumers worldwide, https://otalliance.org.

OTA is active worldwide working with US agencies such as the Departments of Treasury and Justice, the White House, and the Federal Trade Commission. Supporting our global view, Internationally OTA is members of the London Action Plan, (LAP), German Internet Society (eco), Dutch Email Marketing Association and other international efforts.[1]

This past twelve months has marked several OTA milestones including the publishing of:

- Proposed Data Collection & Privacy Statement https://otalliance.org/privacy_demo.html
- Online Principles & Business Guidelines https://otalliance.org/resources/principles.html
- Data Loss & Breach Readiness Guide https://otalliance.org/resources/Incident.html
- Online Safety Honor Roll https://otalliance.org/news/releases/2010honor_roll.html
- Compliance & Online Trust Training programs held in San Francisco, Philadelphia, Singapore, Copenhagen, Amsterdam & Germany.
- Submissions to the Privacy Act staff discussion draft from Rep Boucher & Stearns https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf
- National Strategy for Secure Online Transactions (NS OST)

---

In response to the Department's Notice of Inquiry, the following is a summary of comments in areas most relevant to OTA members and representative of our members' subject matter expertise.

US Privacy Framework

OTA supports the concept of a standard and comprehensible set of laws and statues which enables businesses to understand and implement policies required for compliance. The recent staff discussion draft privacy act from Representatives Boucher and Stearns is a positive effort towards this goal. Today there is a patchwork of some 44 state laws and regulations which by their very nature become insurmountable for businesses to comply with. With inconsistent terminology, all but the largest businesses are often confused and may unknowingly find themselves out of compliance.

As the definition of privacy has evolved, so must the concept of notice and choice. Today privacy and data collections notices are typically overwhelming to the average consumer. As outlined in our submission to Representative Boucher and Stearns, we suggest the importance of moving to an enhanced notice framework, written for the intended site visitor and comparable from one site to another.[2]

We believe greater synchronization of such laws with Safe Harbor provisions and market based incentives are essential. We need to aid businesses who in general want to fulfill privacy requirements, but this can only be accomplished with clear direction in a consistent manner across jurisdictions without the need of excessive technical investments, legal and consulting fees.

[1] London Action Plan http://www.londonactionplan.org/
[2] OTA Standardized Privacy & Data Collection Statement https://www.otalliance.org/privacy_demo.html

Sectoral Privacy Laws & Guidelines

As data collection expands beyond the PC to mobile devices, the appending of data files and information grows and businesses expand internationally, the complexity of navigating laws and legal frameworks with overlapping jurisdictions is impacting businesses of all sizes. In the US alone, regulations are being directed by the Federal Trade Commission, Federal Communications Commission, FDIC with specific requirements under HIPAA, FCRA, COPPA and others.

Internationally "Safe Harbor" is critical for US business to avoid experiencing conflicts with the EU and the risk of facing prosecution under their respective privacy laws. Continued support of safe harbor certification will help assure that EU organizations recognize complying US businesses provide "adequate" privacy protection. Combined, efforts to reconcile these sectoral requirements must be supported, providing a means for US businesses to operate competitively and globally.[3]

New Privacy Enhancing Technologies

OTA sees significant promise and urgency to spur the development of integrated privacy enabling technologies in browsers and web sites. While today many of these are available via "add-ins", we believe they need to be integrated into all browsers and web sites. They need to be discoverable, with an intuitive explanation of their purpose, value-proposition and impact. We believe as a fundamental design requirement, users must be able to enable them at will and have them remain persistent if so selected. At the same time when a user visits a site when such features or technologies enabled, we believe it is reasonable to provide the sites they are visiting the ability to detect such usage. This is essential because such controls have the ability to potentially disable analytics and disrupt legitimate business models which rely on such data collection.[4]

Since the passage of CAN-SPAM we have seen several efforts of self-regulation emerge providing users and businesses preference controls. For example the development of an Internet Engineering Task Force (IETF) standard (RFC 2369) for the inclusion of an unsubscribe header has enabled the majority of email providers and email service providers to provide users a safer and more convenient mechanism to unsubscribe, versus relying on the unsubscribe footer.[5] When such a header is detected by the ISP and the email is verified coming from a known sender, an unsubscribe button is enabled in the email user interface.[6]

Other examples including the development of Extended Validation SSL Certificates (EV SSL), and the adoption of suppression list encryption (practices endorsed by OTA), Feedback Loops (FBLs) and Abuse Reporting Format (ARF) supported by ISPs worldwide. Further examples include email authentication technologies such as SPF, Sender ID (SIDF) and Domain Keys Identified Email (DKIM), which provide ISPs, government and corporate networks added control and ability to protect user's inboxes from spam, forged and malicious email. [7] [8]

---

[3] http://www.export.gov/safeharbor/eg_main_018236.asp

[4] To be provided via the "user string" or other mechanism. Vast majority if not all browsers provide baseline data including the browser version to the site to optimize page rendering. Specific to the use of privacy features, Internet Explorer 8 provides sites the ability to know if InPrivate Filtering is on. This is provided via a JavaScript API, http://msdn.microsoft.com/en-us/library/dd425013(VS.85).aspx.

[5] Required for all OTA members who send commercial email.

[6] Supported by Google Gmail, Microsoft Hotmail, Yahoo mail and others.

[7] OTA email authentication and industry resources https://otalliance.org/resources/authentication/index.html

Combined these are just a few examples of how industry and business are working together. These and other recommendations comprise the OTA Online Principles & Guidelines, a set of voluntary best practices.[9]

Companies are wrestling with the balance of providing users granular control and supporting their business objectives while at the same time trying not to overwhelm users with too many choices. Going forward such efforts need to be intuitive and consumer centric by design. Businesses need to focus on teachable moments, at the point of data collection, to help prevent unintended data collection from occurring.

Today we are starting to see similar efforts in the area of behavioral targeting, preference management and reputation systems. OTA member companies such as Authentication Metrics, Better Advertising, Lashback, Return Path, True Domain, TRUSTe and UnsubCentral are to be commended for their solutions which help address these issues. While is it too early to tell where these solutions, collaborative efforts and standards will land, they represent a strong commitment by business and industry towards consumer and privacy protection.

We believe through the promotion of research, public and private partnerships, and incentives that we can most effectively spur the development of such technologies and services. To support this goal we recommend any such policy and regulations should embrace market incentives.

Small & Medium Business Entities & Start Up Companies, (SMB)

It is essential policy recommendations take into the consideration the impact to SMBs. SMBs are the majority of businesses and often the most ill prepared to navigate the complex set of rules, laws and regulations. OTA annual score cards reports and research indicates the vast majority are unprepared to address privacy, data governance, and marketing or security issues.[10]

While such legislation is important, it can also be a barrier and limit new business formation, ultimately reducing market competitiveness and consumer choice. Since these emerging entities may become tomorrow's market leaders, we need to support the development and availability of resources and services to enable them to be compliant without imposing undue burden.

OTA is working with the US Chamber of Commerce, the Direct Marketing Association, OTA member companies and other stakeholders to help provide guidelines, prescriptive advice, resources and affordable training to small businesses and governmental agencies. Supporting this objective, OTA will be providing half-day training as part of the OTA Academy in September 2010 including CAN-SPAM compliance and email authentication. [11] [12]

---

[8] Submitted by OTA and currently recommended for all governmental agencies in the White House draft National Strategy for Secure Online Transactions (NS SOT).

[9] OTA Online Principles & Business Guidelines published Dec 2009, https://otalliance.org/resources/principles.html

[10] April 2010 Online Safety Scorecard https://otalliance.org/news/releases/2010honor_roll.html

[11] OTA Resource Center https://otalliance.org/resources/index.html

[12] 2010 Online Trust & Cybersecurity Forum Sept 22/24 Georgetown University http://guest.cvent.com/EVENTS/Info/Summary.aspx?e=a8dc654f-32fd-4cb5-8ed5-a518f88dbd43

As a leading non-profit, we are committed to aiding in these efforts and encourage assistance and funding be made available to qualified non-governmental organizations to make such efforts and resource more readily available to all businesses of all sizes and across all industry segments.

With the advent of cloud based services, SMBs are increasingly relying on service providers to provide integrated privacy, security and data governance enabling technologies. Leading email service providers today provide turnkey solutions for managing consumer email preferences including, and we need to look for similar privacy enhancing efforts.

Having exemptions for collection of covered information for small business is essential, but only with safeguards to prohibit data sharing and efforts to circumvent the exemptions. As recommended in OTA comments to the draft privacy bill from Representatives Boucher and Stearns, we recommended entities that collect less than 15,000 records annually be exempt from such regulations.[13]

The Role of Government and the Department of Commerce

OTA applauds the efforts of the Department and the long standing international thought leadership. We encourage the Department to continue its efforts to advance U.S. competitiveness by encouraging government and the private sector to work together to demonstrate U.S. leadership in developing and implementing best practices. Efforts to proactively engage businesses in this dialog will help assure the long term competitiveness and vitality of the market place.

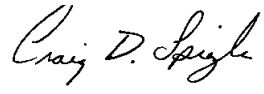
The free flow of information on the Internet is important to our Nation's fundamental democratic values, as is the protection of individual's privacy and business data. Without both, we significantly risk disenfranchising millions of consumers and segments of the population who increasingly rely on the internet for their communication services, information, education and employability.

Thank you for the opportunity to meet last month and provides this input. In summary, we believe that consumers and the internet economy at large will benefit by the consolidation of privacy and data breach regulations, and by the support of market based incentives, self-harbor and technology innovation which support the needs of all business segments from SMBs to the Fortune 500.

OTA looks forward to continuing collaboration with the Department of Commerce on this and other initiatives and work streams including cybersecurity, protection of intellectual property and the free flow of information.

Working together we can help ensure the vitality of online services and commerce.

Respectfully,



Craig Spiezle
Executive Director
Online Trust Alliance

Cc: OTA Board of Directors & Steering Committee

[13] OTA submission dated June 4, 2010 https://otalliance.org/docs/OTA_Privacy%20Bill_finalx.pdf

PRISM (Professional Records and Information Services Management) International is a 501(c)(6) trade association headquartered in North Carolina and serving members in more than 60 countries. The members of PRISM International provide paper records management, data protection services, imaging and conversion services and confidential destruction services to multiple clients for profit. Approximately 650 member companies belong to PRISM International. PRISM International also maintains a secretariat office in Brussels.

Since 2008, PRISM International has been actively engaged with members of the European Parliament and European Commission regarding the transposition and implementation of the Data Retention Directive. This directive was put in place as an anti-terrorism measure and was perceived by some telcom companies and European ISPs as an unfunded mandate to retain transactional data beyond the time limit for ordinary business use.

In general terms, the European Union has been more sensitive on issues related to privacy than Americans as evidenced by the European-driven Safe Harbour provisions and recent regulatory action by Germany regarding Google data collection practices. The European Data Retention Directive attempts to strike a balance between the need for individual privacy through limiting retention periods for telcom and ISP transaction data, and law enforcement's need to act quickly to trace the communication channels of terrorists. While the full effect of the directive's transposition has not been felt as yet, (the ISP provisions have not yet gone into effect), the need for balancing individual privacy on the Internet does seem to be an issue of growing concern among Americans. (The recent backlash against the change in privacy settings by Facebook is a recent example).

The following is an excerpt from a white paper provided to the European Commission from PRISM International, which articulates some of the European privacy concerns.

**"**Because the directive establishes limits on the length of time data can be retained, citizens of EU Member States have expressed concerns that there is some type of verification of the destruction of data. These types of concerns seem to be increasing with each incident where retained data are inadvertently released. This includes data from governments. MEP Alvaro expressed this concern very clearly in a September, 2008 speech in Plenary where he said, *"The Commission and Council are striving, with an incredible amount of activity, to take action in the field of the economic protection of personal data. When we see what is happening in the United Kingdom, Germany and other Member States, where there are cases of loss or theft of personal data administered by public authorities, we have just as urgent a need for action here. This is ultimately more than ever about citizens' rights, as they are not able to prevent their government behaving in this way. With enterprises, the citizen is still able to choose a different one in case of doubt."*

"MEP Alvaro's point regarding a citizen's choice in case of doubt is key. Even though telcom companies and ISPs use any and all means of verification that they have destroyed data, within

the minds of some citizens there is likely to remain some question as to whether this has been done unless the data moves beyond the control of the organization and is housed with a third party. In this scenario it is possible to imagine a much higher threshold of verification. Moreover, access to this data can also be made more secure by encrypting the data prior to sending it to a third party for storage. Data outsourced in this way is stored by a company who does not have the means to access it (an encryption key). The data owner no longer has physical possession of the data and thus has no without a means of preserving the data past its point of expiration (without the direct intervention of law enforcement due to an active investigation or legal hold). This type of arrangement works very similarly to a separation of duties control in accounting. There must be cooperation between the vendor and the client in order to act. Aside from the added benefits of data security in this arrangement, we believe the additional layer of verification and transparency of data will probably be of the most benefit to telcom companies and the public."

Thank you for the opportunity to submit these comments.

Respectfully,
James E. Booth
Executive Director

Jim Booth
Executive Director
PRISM International
1418 Aversboro Rd. Suite 201
Garner NC 27529  USA
Voice: +1-919-771-0657
Fax: +1-919-771-0457
jim@prismintl.org

June 14, 2010

National Telecommunications and Information Administration
United States Department of Commerce
Room 4725
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Docket Number 100402174-0175-01

Dear Sir or Madam:

Procter & Gamble is the world's largest consumer products company with over 250 brands used by 4 billion consumers across 180 countries. Our products are used in 59% of the world's households. Our culture is based on principles and values—Passion for Winning, Leadership, Ownership, Integrity and Trust—that have allowed us to continue to grow for 172 years. We are consistently ranked in the top 10 of Fortune Magazine's Most Admired Companies, Business Week's World's Most Innovative Companies, and Ponemon Institute's US Most Trusted Company surveys, to name a few examples.

P&G appreciates the opportunity to submit comments regarding the Information Privacy and Innovation in the Internet Economy Notice of Inquiry. We have provided input to comments that will be submitted by several of our industry partners, but want to highlight several common key points. To provide context for these key points, included below is a general overview of P&G's Global Privacy Program, as described in remarks to the Conference of International Data Protection Commissioners in Madrid, Spain in November 2009.

Global Privacy at P&G – Context for Key Points

At P&G, our purpose is to "Touch lives and Improve Life," and our internal corporate mantra is "The consumer is boss." We build brand franchises globally, which means we need to develop trusted relationships with consumers around the globe to better understand and deliver what they want, whenever and wherever they want it. This naturally requires global flow of data; the trust of our consumers who provide their personal data drives P&G's Global Privacy Program. It is supported and sponsored by the CEO and functional officers.

We have one Global Privacy Policy that applies to all types of personal data across all geographies and all media types—online, offline, mobile, wireless, etc. This Global Privacy Policy sets our corporate standard reflecting the strictest of privacy laws for every country where we have operations, whether or not local privacy laws exist in those countries.

Key measures for our global program include privacy comments from consumers and employees, incident response and tracking, mandatory training completions, control assessments and audit results, to name a few. We track these measures globally, learn from them and modify our procedures accordingly for continuous improvement. We share these with our senior leadership in periodic reviews.

We were one of the first companies to participate in Safe Harbor for all types of data and certify annually with the US Department of Commerce. The Better Business Bureau and the Direct Marketing Association are our third party intermediaries; we have had no reports to the DMA and very few to the BBB over the eight years we've had their seal. Our consumers come directly to us and we handle each complaint urgently and professionally. Consumers can contact us via the web, in writing, through email or by calling the toll-free number we have on product labels. These communications all come to our global consumer relations organization, which is well trained on whom to contact quickly if there is a significant incident or repeated incidents. We believe we have a world class privacy program, but accidents will still happen, especially with a company of our size. We need to make sure that when it does we can shut down or fix the problem quickly and then learn from the mistake to modify our controls and procedures holistically.

We realize that consumers don't always understand privacy and thus we have created a consumer privacy education webpage that has tips and articles on how to protect the personal information of a consumer's family. Among other topics in privacy, this site explains how to read and understand a privacy notice and how to 'stop the junk' for marketing messages consumers get online and offline.

P&G's Global Privacy Program is built on a foundation of trust, and we are accountable for this across the breadth of our Company. While our program is driven by the consumer, P&G does and always will comply with all laws in all jurisdictions. However, when we have to insert processes specific to state or country regulations—registering databases and applications, waiting for approval from notifying authorities to transfer data, requiring our global suppliers to provide individual country contracts for approval in local language—one has to wonder, how is this protecting consumers any more than we already do? Our brands have to delay or avoid launching initiatives in a state or country because of the extra time and cost to meet differing requirements. In some cases this is due to those DPA offices that have the requirements but not the resources to respond in a timely manner. This means consumers in some countries will not experience P&G products or services as quickly as those in other countries.

We are not alone in living this high level of corporate accountability; other multinational corporations have the same approach to their Global Privacy Programs; many are our global partners. Ideally, mechanisms such as International Data Protection Standards would drive the certification of accountability, mutually recognized by countries around the globe. In this scenario, companies that demonstrate the willingness and capacity to be responsible would be certified as accountable. These companies would be allowed to change processes and move data without filing notifications and waiting for approvals. This would benefit global commerce, reduce the work of the country data protection offices, and ensure that consumers have timely access to the product and services that enhance their lives. This type of model would incentivize

data protection, resulting in greater consumer trust in the corporations that hold their information.

Procter & Gamble believes that the Department of Commerce should take a leadership role in driving consistency in domestic and international privacy standards and accountability. The development of the APEC Privacy and Security Framework and the subsequent Pathfinder Pilot—both of which included P&G as a participant—is an excellent example of the positive leadership role the Department can play in privacy policy.

Summary – Key Points in Response to Notice of Inquiry

- The current maze of state and country laws, regulations and accountability systems is a deterrent to a thriving international digital economy. (See comments submitted by USCIB, Center for Information Policy Leadership.)
- Experience shows that a mix of principle-based laws & regulations, together with self-regulation (e.g. based on how data will be used and thus obligations to protect it), will be the most efficient and effective way to achieve policymaker objectives. (See comments submitted by GS1/EPCglobal, Business Forum for Consumer Privacy.)
- Incentives to "Do the Right Thing" should be built into any new accountability model to encourage adherence to principle-based laws & regulations. (Similar to the US Federal Sentencing Guidelines for effective Ethics & Compliance programs.)
- The Department of Commerce can play a lead and unbiased role in bringing together industry, advocates, policymakers and academics to focus on common objectives to protect and safeguard personal information and thus develop policy solutions that will work for companies of all sizes. (See comments submitted by USCIB, CIPL, the Forum, GS1/EPCglobal.)

Procter & Gamble looks forward to continued partnership with the Department of Commerce in our common goal—protecting the consumer in the international free-flow of the information economy. Please contact me with any questions.

Sincerely,

Sandra R. (Sandy) Hughes
Procter & Gamble
Global Information Governance and Privacy
2 P&G Plaza, TE-13
Cincinnati, Ohio 45202
hughes.sr@pg.com
513.983.4224

**Before the**
**UNITED STATES DEPARTMENT OF COMMERCE**
**NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION**
**Washington, DC 20230**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Notice of Inquiry from the | ) | Docket No. 100402174-0175-01 |
| National Telecommunications and Information | ) | Docket No. 100402174-0238-02 |
| Administration (NTIA) Regarding: | ) | |
| Information Privacy and Innovation in the | ) | |
| Internet Economy | ) | |

## COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.

Qwest appreciates the NTIA's Notice of Inquiry[1] on this topic and provides these brief comments in response to it. As the principal advisor to the President on telecommunications issues, the NTIA is a critical participant in the ongoing dialogue about federal privacy policy. Indeed, it has a strong record in the formation of policy on privacy, including at the international level where it has participated in the formation of the Safe Harbor Principles with the European Union. And it is uniquely suited to strike the right balance between the interests of consumers, who unquestionably deserve protection regarding the use of information about them, and the needs of businesses in the information economy to cost effectively respond to consumers, continue to add value to the economy, and maintain and create jobs.

Qwest is an interested participant in the federal privacy policy dialogue. Qwest is a high speed Internet, broadband and telecommunications provider in 14 states throughout the western United States. We use and need information about our customers to provide, refine and improve our services, and manage and plan for future development of our networks. We also publish content on the Internet at our own web sites and advertise through advertising networks in other places on the web. In short, we not only provide the infrastructure for the information economy but actively participate in it.

Unlike some other participants in the information economy, we have customers in the traditional sense of the word -- individuals who purchase our services. We value our relationships with our customers and know how important it is for us to be clear with them about our privacy practices and honor their expectations. Toward this end, we recently updated our privacy policy with the goal of making our privacy practices and our customers' choices about them easier to understand. And our commitment to the protection of information about our customers is reflected in our employment of a Chief Privacy Officer, and counsel and compliance staff dedicated to privacy.

---

[1] 75 Fed. Reg. 21226 (2010), 75 Fed. Reg. 32372 (2010).

In short, privacy is important to us and we have a vested interest in the federal government's development of a coherent policy on it.

Notice, choice, access and security remain the best tenets for federal policy on privacy. These tenets are well recognized and often referred to as fair information practices. They recognize that many businesses have responsibly collected and used customer information for basic operational, management, planning, and marketing and sales functions for years. Indeed, this collection and use of information is necessary for the provision of services and the fulfillment of customers' expectations with respect to both the existing commercial marketplace and the marketplace to come. In short, anticipating customer expectations is largely the result of the collection and analysis of information about individual consumers. And this analysis is essential for any meaningful communication with individuals about the choices that may be available to them to improve their economic and social well being.

Within the well established fair information practices framework, federal privacy policy must apply to all players in the information economy. It cannot be differentiated based on the technology or application in which information is collected, stored, or used.

Federal policy must also be broad enough to continue to allow businesses to grow and thrive by quickly and creatively meeting the needs of their customers. Federal prescriptive measures, if not crafted and adopted with a view toward flexibility and the vested interests of businesses like Qwest to honor the expectations of their customers, run the grave risk of freezing the Internet at some arbitrary point in time, thereby reducing its economic value. By way of example, according to a study commissioned by the Interactive Advertising Bureau,[2] the advertising-supported Internet represents 2.1% of the total U.S. gross domestic product. It directly employs more than 1.2 million Americans in jobs that did not exist twenty years ago, and another 1.8 million people that work to support those directly with Internet-related jobs. This commercial contribution to the United States economy cannot be overstated.

Broad policy tenets (along the lines of long-recognized fair information practices) leave open the way for continued rapid innovation -- the only way to meet consumers' expectations in the information economy. Indeed, most advances in online privacy protection to date have come as a result of industry initiatives that were quick and responsive to market imperatives. For example, the Direct Marketing Association and Interactive Advertising Bureau have crafted standards for their members designed to meet customer expectations. More recently, various groups -- including Yahoo and the Future of Privacy Forum -- have announced plans for simple depictions of the information used to deliver web based advertising in ways that consumers can understand and over which they can exercise control. And TRUSTe has developed an interactive tool that provides consumers with easily accessible and understandable information about advertising practices. Each of these steps is a quick and creative response to consumer concerns. And each reflects action taken within a framework of the fair information practices. Anything more prescriptive would surely be soon outdated and fail to address tomorrow's technologies and business models.

---

[2] http://www.iab.net/media/file/Economic-Value-Report.pdf.

A federal model based on the fair information practices would incorporate the ability to more specifically address sectoral protections regarding sensitive information about consumers, as currently embodied in the various federal laws referred to in the NTIA's Notice, such as the Telecommunications Act and the Federal Communications Commission's regulation of customer proprietary network information.

In closing, it is imperative that the federal government develop a clear, coherent, policy on privacy that reflects not only protection of consumers against harm but promotion of commerce. The NTIA's ability to balance the important business issues in a policy context makes it a key actor in the current privacy deliberations. A simple, and ideally preemptive, federal policy on privacy will give both industry and consumers a framework they can understand and manage. Absent such a preemptive policy, the complicated web of state standards on privacy and information security will continue to grow, creating not only operational costs and unduly prescriptive requirements for businesses but unequal treatment for consumers regarding the standards applicable to privacy protection of information about them. Qwest looks forward to working with the NTIA on this complex issue.

QWEST COMMUNICATIONS
INTERNATIONAL INC.

/s/Andy Holleman
Craig J. Brown
Andy Holleman
Associate General Counsel
Suite 1160
1801 California Street
Denver, CO 80202
Craig.brown@qwest.com
Andy.Holleman@qwest.com
303-992-7086

June 14, 2010

*Filed via e-mail at privacy-noi-2010@ntia.doc.gov.*

RETAIL INDUSTRY LEADERS ASSOCIATION
Educate. Innovate. Advocate.

1700 NORTH MOORE STREET
SUITE 2250
ARLINGTON, VA 22209
T (703) 841-2300 F (703) 841-1184
WWW.RILA.ORG

June 14, 2010

*Via electronic filing: privacy-noi-2010@ntia.doc.gov*

Internet Policy Task Force
National Telecommunications and
Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, D.C. 20230

**Re: Comments in Response to Notice of Inquiry on the Information Privacy and Innovation in the Internet Economy**

Dear Internet Policy Task Force:

I appreciate this opportunity to provide comments in response to the Department of Commerce's Internet Policy Task Force's Notice of Inquiry on information privacy and innovation in the Internet economy (NOI).[1] We offer these initial comments and look forward to working with the Department as it explores this important issue with an eye toward progressive and responsible commerce that strengthens our nation's international economic standing.

By way of background, the Retail Industry Leaders Association (RILA) promotes consumer choice and economic freedom through public policy and industry operational excellence. Our members include the largest and fastest growing companies in the retail industry – retailers, product manufacturers, and service suppliers – which together account for more than $1.5 trillion in annual sales. RILA members provide millions of jobs and operate more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

RILA shares the Commerce Department's commitment to ensuring that the Internet remains open for innovation.[2] The present system has fostered an environment that encourages and enables our member companies to incorporate novel information applications into their practices, and they have pursued creative ways to deliver existing goods and services across the globe via the Internet. Our comments highlight some of the many positive contributions that the Internet has provided to the economy.

## I. Businesses and Consumers Have Greatly Benefitted from e-Commerce

The retail industry is a vital player in the U.S. economy, and each day our members pursue

[1] Notice of Inquiry, Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226 (Apr. 23, 2010).
[2] 75 Fed. Reg. at 21227.

innovative ways to reach consumers, whether through brick-and-mortar stores or through other means, such as the Internet. As the NOI notes, even as the overall economy suffered during the recession, e-commerce continued to grow at an impressive rate.[3] We anticipate that e-commerce will only continue to increase in the future, with our member companies contributing to this important area of economic growth by adding new jobs to support their e-commerce practices. Such jobs include a variety of employment possibilities, from positions that focus on information technology to jobs in customer service, manufacturing and product distribution.

RILA members strive for excellence in serving their customers. In this competitive climate, our members gain and retain customers by fostering consumer trust in the transactions that take place online as well as offline. Our members protect the information that customers provide them and use it for a number of different purposes, ranging from product delivery to enhancing customers' online experiences. For example, many of our retailers collect information from customers to offer them loyalty and discount coupons for products they are likely to find useful. Our members also use customer information to complete product requests and to respond to customer service inquiries. Additionally, in the spirit of innovation, our members collect information to improve customers' e-commerce experiences by continually using such information to modify content presentation and offerings as well as to improve the efficiency of online transactions.

Much as catalogues have enabled consumers in remote locations to partake in commerce, e-commerce has also provided consumers with a new avenue to participate in the economy. Customers who are too busy to frequent shops in person or prefer the inventory of products available online also find value in e-commerce. RILA members have a vested interest in protecting the information provided by their customers because the retail industry is built on the business-to-consumer model.

## II. Innovation Has Led to a Rise in Mobile Commerce

As the NOI notes, mobile commerce is on the rise.[4] In addition to accessing the Internet through desktops and portable laptops, consumers increasingly now use mobile devices to access the Internet and engage in commerce. Encouraged by and supportive of this trend, many RILA members have begun to embrace mobile commerce. Retailers are exploring how to market and brand themselves on mobile devices. They are also experimenting with applications that enable consumers to make secure mobile payments.

Retailers are also beginning to explore integrating mobile technology into their brick-and-mortar stores. Applications are now in development that will enable consumers to scan product barcodes with their mobile devices while they are in stores and receive information delivered over the Internet that supplements their knowledge about a product. Additionally, retailers are using mobile devices to conduct inventory management.

To examine this new era of mobile commerce, RILA will be hosting the first-of-its-kind Retail Mobile Executive Summit this July 2010. The summit will explore the use of mobile technology

[3] *Id.*
[4] *Id.*

and address the challenges and opportunities presented by this progressive retail space. Our members are eager to explore this new innovative channel of commerce.

## III. The Current Regulatory Structure Promotes Online Commerce

The current regulatory environment has enabled RILA members to innovate in the e-commerce and mobile marketplaces. As Commerce Secretary Gary Locke stated at the Commerce Department's recent May 7th Privacy and Innovation Symposium, "we need to be careful to avoid creating an overly complicated economic and regulation environment."[5] Privacy concerns can be addressed while still promoting a regulatory structure that fosters global innovation.

Because of the Commerce Department's mission to promote progressive domestic growth, we welcome you to the privacy debate.

## IV. Notice and Choice are Not Outdated Models

We are concerned about the recent debate that notice and choice is an outdated or ineffective model. The fundamental construct of the U.S. economy revolves around consumer choice, with consumer protection being the regulatory protection against harmful practices. Retailers have a long history of managing consumer notice and choice options. As technology and marketing channels have evolved and expanded, retailers have reacted and adjusted their practices to meet the needs and wants of our customers.

* * *

Thank you for the opportunity to contribute to the dialogue on this important subject and look forward to working with the Department. Should you have additional questions about these comments or the retail industry, please do not hesitate to contact Sarah Arbes at 703-600-2021 or sarah.arbes@rila.org.

Sincerely,

Casey C. Chroust
Executive Vice President, Retail Operations

[5] Gary Locke, Secretary, Commerce Dep't, Prepared Remarks at the Privacy and Innovation Symposium (May 7, 2010), *available at* http://www.commerce.gov/NewsRoom/SecretarySpeeches/PROD01_009223.

salesforce.com
Success. Not Software.®

Diana Hynek
Departmental Paperwork Clearance Officer
Department of Commerce, Room 6625
14th and Constitution Avenue, NW
Washington, DC 20230

Dear Ms. Hynek:

Salesforce.com is pleased to respond to the Department of Commerce request for comments on "Information Privacy and Innovation in the Internet Economy." Specifically, we would like to comment on Section 4. *Jurisdictional Conflicts and Competing Legal Obligations*, which references cloud computing.

Cloud computing allows individuals and organizations to build, deploy and access applications over the Internet. According to Gartner, the cloud computing market was worth approximately $46 billion in 2009 and will increase to $150 billion by 2013. Gartner predicts that next year 25% of new software deployments will be based on software-as-as-service cloud computing applications. According to a recent Goldman Sachs technology software report, the shift toward cloud computing is "unstoppable." The remarkable growth of cloud computing is not limited to consumer and business applications. Numerous federal, provincial, and local governments in North America, Europe, and Asia have also implemented cloud computing solutions.

About Salesforce.com

Salesforce.com is a leading enterprise cloud computing company. We provide cloud solutions to organizations of all sizes in all industries globally. Our main service offering is an enterprise cloud computing application that allows organizations to input, store, process, and access data about their customers. Our customer relationship management services include salesforce automation, customer support, help desk, marketing automation, collaboration, and an on-demand technology platform that enables our customers and partners to build and sell entirely new on-demand cloud applications on our cloud platform.

Salesforce.com delivers its services over the Internet through commercially available Web connections and browser software. Customers log into salesforce.com's services from our Web site using a unique username and password. Our services allow for additional authentication and security methods that may be activated by customers. Salesforce.com serves its customers through secure hardware and software, using what is known in the industry as "multi-tenant" application architecture. A multi-tenant application can be accessed and used by many users simultaneously, with logical separation of data in hardware and software. The logical separation of data allows each salesforce.com customer to view only its "instance" of our services and associated data. Our multi-tenant architecture is similar to that used to provide online banking services to consumers (which can also be accessed and used securely by thousands of users simultaneously through the logical – not physical – separation of data).

Over 77,000 customers globally, including governments and businesses in highly regulated industries – such as financial services, healthcare, insurance, and communications – trust salesforce.com to host their customer data in our secure data centers.

Transborder Data Flows

Because cloud computing applications and the associated data can be accessed anywhere with a browser, transborder data flows are intrinsic to the cloud computing model. These data flows, in turn, have raised concerns about jurisdiction, privacy and security. Some of these concerns are justified, but others have been raised by those who simply want to slow down the shift to cloud services. Fortunately, these restrictions are limited to a few countries. Where restrictions on transborder data flows do exist, however, they impede cloud computing services. These regulations fall into two categories: 1) sector-specific regulations and 2) provincial government laws. It is important to note that these are not privacy regulations per se, but broader industry and government requirements.

Among the sector-specific regulations we have encountered are the following:

- Luxembourg banking regulations
- Swiss banking regulations
- Korean banking regulations
- Indian telecommunications regulations

Among the provincial government restrictions we have encountered are the following:

- British Columbia laws
- Nova Scotia laws

It is important to note that these Canadian provincial laws were enacted in large part to respond to concerns about undue U.S. government access to data stored in the United States as a result of passage of the USA Patriot Act.

Although these laws and regulations are limited to just a few sectors and provincial governments, they have led to widespread misperceptions in these countries that businesses and government agencies cannot take advantage of cloud computing services because of prohibitions on transborder data flows. This misperception has created confusion in the market for cloud computing in these countries and, at times, prevented outright sales of enterprise cloud services.

The focus on cloud computing and transborder data flows has also led to numerous requests to build data centers in other countries. Building multiple data centers around the world is not always practical or desirable. Moreover, it would not resolve the transborder data flow issue. Even if cloud computing companies built a data center in all the countries where they conduct business, their worldwide support operations and geographically distinct back-up data centers would result in transborder data flows.

Fortunately, there are some examples of countries that have relaxed their controls on transborder data flows. For example, India had controls in place that required all banks to keep data containing personal information inside India, but these controls were relaxed in 2006.

International Data Convention

The United States has a vested interest in the emergence of the cloud computing market, not only because it will spur job creation and boost the competitiveness of US IT firms, but also because it will boost productivity and innovation across the private and public sectors. Although it is incumbent on individual companies to put in place appropriate data security and privacy controls, it is beyond their ability to

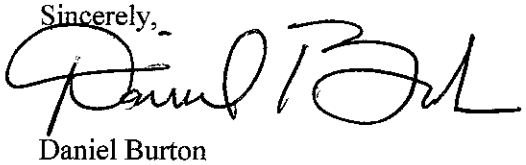
reconcile competing jurisdictional claims or to allay concerns about government access to the data they hold on behalf of their customers.

To address these concerns, we would encourage the US Department of Commerce to call for an International Convention on Transborder Data Flows. The Convention could take the form of a series of bilateral talks between the United States and key economic partners, or it could consist of multi-lateral discussions. Fortunately, many data controls are already in place and simply need to be updated to take into account the emergence of cloud computing.

The US Department of Commerce has a very good record of addressing global data issues in ways that facilitate international commerce. The US-EU Safe Harbor enabled US IT companies to demonstrate the adequacy of their privacy policies and thus comply with the EU Data Directive. The APEC deliberations also offer a potential path to address privacy issues in terms of accountability. An International Convention of Transborder Data Flows would build on these efforts to develop accepted norms for the storage, processing and access of data across countries.

We appreciate the opportunity to respond to the notice on Information privacy and Innovation in the Internet Economy and would be happy to provide additional information upon request.

Sincerely,



Daniel Burton
Senior Vice President, Global Public Policy
Salesforce.com

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

Samuelson Law, Technology
& Public Policy Clinic

University of California, Berkeley
School of Law
396 Simon Hall
Berkeley, CA 94720
510-643-4800
510-643-4625 (fax)
http://www.samuelsonclinic.org/

[Submitted by email: privacy-noi-2010@ntia.doc.gov]

June 7, 2010

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

**Re: Docket No. 100402174–0175–01, RIN 0660–XA12, Information Privacy and Innovation in the Internet Economy**

Dear Messrs. Locke, Strickling, Sanchez, and Gallagher,

Thank you for soliciting comments on information privacy and innovation in the internet economy.

We wish to bring to your attention the rich and diverse scholarship of the Samuelson Law, Technology & Public Policy Clinic and of our colleagues at Berkeley Law who concentrate on information privacy issues.

The Samuelson Law, Technology & Public Policy Clinic at UC Berkeley School of Law gives law students the opportunity to collaborate with other graduate students and attorney faculty members in representing clients and the public interest on important and emerging issues in technology law. Established in January 2001, the Samuelson Clinic was the first in the nation to provide students with the opportunity to represent the public interest in sound technology policy through client advocacy and participation in legislative, regulatory, litigation and technical standard setting activities.

Today, the Samuelson Clinic functions as both a traditional legal Clinic and as a site of interdisciplinary, policy-relevant research. Much of this research is directly relevant to the Department's inquiry, and it is summarized below along with relevant research from our Berkeley Law colleagues. We hope that this information is helpful; please do not hesitate to contact us with questions or if we can be of further help.

Respectfully Submitted,

Jason Schultz
Director

Jennifer Urban
Director

Jennifer Lynch
Clinical Fellow

Chris Jay Hoofnagle
Senior Staff Attorney

Attachments (8)

- New smart meters are being installed in homes around California and the country provide much more data on energy customers than ever before--up to 750 to 3000 data points per month per household. Energy usage information of this granularity can reveal not only the various appliances that are consuming power within the household, but also their current operations. This radical departure from the traditional once-a-month manual readings can reveal specific household activities such as sleep, work, and travel habits and allows utilities and third parties with access to the information to "see" what is going on inside the home. The Samuelson Clinic, on behalf of its client the Center for Democracy & Technology, has submitted formal comments on the Smart Grid and information privacy to the Federal Trade Commission in its National Broadband Plan proceeding; to the National Institute of Standards and Technology in its Smart Grid Standards Framework proceeding;[1] and in conjunction with the Electronic Frontier Foundation to the California Public Utility Commissions' Smart Grid Rulemaking.[2] The comments urge the Commission to build strong privacy protections into the Smart Grid and to issue privacy protecting regulations based upon the Fair Information Practice principles.

- Media reports teem with stories of young people posting salacious photos online, writing about alcohol-fueled misdeeds on social networking sites, and publicizing other ill-considered escapades that may haunt them in the future. These anecdotes are interpreted as representing a generation-wide shift in attitude toward information privacy. Many commentators therefore claim that young people "are less concerned with maintaining privacy than older people are." In *How Different Are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies*, we found the picture to be far more nuanced than portrayed in the popular media.[3] In this telephonic (wireline and wireless) survey of internet using Americans (N=1000). Large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions. In several cases, there are no statistically significant differences between young adults and older age categories on these topics. Where there were differences, over half of the young adult-respondents did answer in the direction of older adults. There clearly is social significance in that large numbers of young adults agree with older Americans on issues of information privacy. We conclude that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.

- Behavioral advertising is the subject of an international regulatory debate. Many advertisers have claimed that consumers want tailored advertising. However, in a national telephonic survey, we found that, contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising. In *Americans Reject Tailored Advertising and Three Activities that Enable It*,[4] we found that Americans favor much more vigorous privacy protections and severe penalties for violations of those protections. Further, we found a high degree of confusion about the protections that US law offers

---

[1] Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy, Docket Number 0909301329-91332-01. Available at http://www.cdt.org/content/cdt-comments-nist-smart-grid And Requirements

[2] Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining to the Smart Grid. Available at http://www.law.berkeley.edu/7973.htm

[3] Chris J. Hoofnagle et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*, SSRN ELIBRARY (2010), http://ssrn.com/paper=1589864.

[4] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.

consumers—most Americans mistakenly believe that privacy laws strongly limit information use.

- Despite the passage of sweeping financial services modernization and preemptive credit reporting legislation, identity theft still affects about 10 million Americans each year. In *Internalizing Identity Theft*,[5] Chris Hoofnagle finds in an empirical study of identity theft victims that credit grantors ignored obvious signs of fraud (and sometimes explicit warnings) on applications. Identity theft is the result of business incentives that prioritize quick credit granting over the avoidance of fraud. Of course, all businesses must find some reasonable balance between procedures and the avoidance of fraud, but the current identity theft landscape leaves victims with some costs of the crime—most notably in lost time. Hoofnagle proposes a system for credit grantors to compensate victims directly for out-of-pocket costs and lost time costs, because credit grantors are the least cost avoiders, because consumers cannot effectively insure against fraud, and because credit grantors are fully in control of the decision to issue a new account.

- In *Privacy on the Books and on the Ground*, Professors Ken Bamberger and Deirdre Mulligan explain that ambiguity is a *benefit* of the U.S. privacy framework.[6] Privacy law "on the ground" has benefitted from this ambiguity, because in order to manage shifting consumer expectations and regulator interests, companies have devoted significant resources to privacy management. This has resulted in the creation of C-level privacy officers in major companies, the professionalization of privacy officers, and the desire to satisfy the "soft law" of consumers privacy norms. Eliminating ambiguity from this system would likely result in more formalism and less substance—a world of "click through if you 'consent' to the privacy policy" approach.

- There have been many proposals to unify privacy law at the federal level, despite the historical role of states in consumer protection matters. Preemption is difficult policy issue, with all sides choosing positions that are outcome based, and frequently changing their attitude towards state legislation in different but similar contexts. In *Preemption and Privacy*, Paul Schwartz brings much light to this debate.[7] Schwartz clarifies where federal preemption can benefit regulation, such as where legislation can create field definitions to lower compliance costs. At the same time, Schwartz explains that the federalism "toolkit" contains many more options than ceiling or floor preemption—including options that allow a single state to create new privacy laws, preemption that is limited to "conduct" rather than the entire subject matter of the law, and creating sunsets on preemption that give industries and regulators incentives to regularly revisit the rules.

- The large majority of consumers believe that the term "privacy policy" describes a baseline level of information practices that protect their privacy. In short, Americans believe "privacy," like "free" before it, has taken on a normative meaning in the marketplace. When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. In *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, Joseph Turow, Chris Hoofnagle, Deirdre Mulligan, Nathaniel Good, and Jens Grossklags argue that because the term "privacy policy" has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission

---

[5] Chris Jay Hoofnagle, *Internalizing Identity Theft*, SSRN ELIBRARY, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1585564#.

[6] Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground. Stanford Law Review, Vol. 63, 2010; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: http://ssrn.com/abstract=1568385

[7] Schwartz, Paul M., Preemption and Privacy. Yale Law Journal, 2009; UC Berkeley Public Law Research Paper No. 1404082. Available at SSRN: http://ssrn.com/abstract=1404082

("FTC") should regulate the use of the term "privacy policy" to ensure that companies using the term deliver a set of protections that meet consumers' expectations and that the term "privacy policy" does not mislead consumers during marketplace transactions.[8]

- Spyware is software that monitors user actions, gathers personal data, and/or displays advertisements to users. While some spyware is installed surreptitiously, a surprising amount is installed on users' computers with their active participation. In *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, authors Nathaniel S. Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Joseph Konstan report on results of an experiment in which 31 users conducted computer configuration tasks and passed a thorough interview process. The results suggested that mutual assent, in the legal sense, is largely unachievable given the current state of notices and law.

[8] J Turow et al., *The Federal Trade Commission and Consumer Protection in the Coming Decade*, 3 I/S J. OF LAW & POLICY 723 (2007), http://www.is-journal.org/V03I03/Turow.pdf.

I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

JOSEPH TUROW,[a] CHRIS JAY HOOFNAGLE,[b] DEIRDRE K. MULLIGAN,[c] NATHANIEL GOOD,[d] & JENS GROSSKLAGS[e]

# The Federal Trade Commission and Consumer Privacy in the Coming Decade

**Abstract**:[f] The large majority of consumers believe that the term "privacy policy" describes a baseline level of information practices that protect their privacy. In short,

---

[a] Joseph Turow, Ph.D., is the Robert Lewis Shayon Professor of Communication at the University of Pennsylvania's Annenberg School for Communication, and the director of the Information & Society Program at the University of Pennsylvania's Annenberg Public Policy Center. He is the author of, among other books, *Niche Envy: Marketing Discrimination in the Digital Age* (Cambridge, MA: MIT Press, 2006).

[b] Chris Jay Hoofnagle, J.D., is a senior staff attorney at the Samuelson Law, Technology & Public Policy Clinic, and a senior fellow at the Berkeley Center for Law & Technology of the Boalt Hall School of Law.

[c] Deirdre K. Mulligan, J.D., is the director of the Samuelson Law, Technology & Public Policy Clinic and the Clinical Program at the Boalt Hall School of Law. The work of the Samuelson Clinic is generously supported through an endowment from Professor Pamela Samuelson and Robert Glushko, Ph.D. Additional funding is provided by: The Rose Foundation for Communities and the Environment, the California Consumer Protection Foundation, and the National Science Foundation, Team for Research in Ubiquitous Secure Technologies, NSF CCF-0424422.

[d] Nathaniel Good is a Ph.D. candidate at the School of Information at the University of California, Berkeley.

[e] Jens Grossklags is a Ph.D. candidate at the School of Information at the University of California, Berkeley. His work is supported in part by the National Science Foundation through ITR award ANI-0331659.

[f] This article originally appeared as a paper presented under the same title at the Federal Trade Commission Tech-ade Workshop on November 8, 2006. The version published here contains additional information collected during a 2007 survey.

"privacy," like "free" before it, has taken on a normative meaning in the marketplace. When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. Of course, this is not the case. Privacy policies today come in all different flavors. Some companies make affirmative commitments not to share the personal information of their consumers. In other cases, however, privacy policies simply inform consumers that unless they "opt out" of sharing certain information, the company will communicate their personal information to other commercial entities.[1]

Given that consumers today associate the term "privacy policy" with specific practices that afford a normative level of privacy protection, the use of the term by a website that does not adhere to these baseline practices can mislead consumers to expect privacy that, in reality, does not exist. This is not to suggest that companies intend to mislead consumers, but rather that consumers today associate certain practices with "privacy policy" just as they associate certain terms and conditions with the word "free."

Because the term "privacy policy" has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission ("FTC") should regulate the use of the term "privacy policy" to ensure that companies using the term deliver a set of protections that meet consumers' expectations and that the term "privacy policy" does not mislead consumers during marketplace transactions.

[1] Often consumers are not provided with a means to "opt out" of information sharing.

## I. INTRODUCTION

Ten years have passed since the FTC's last comprehensive hearings on the future of consumer protection. In that time, the FTC has pursued a self-regulatory approach to protecting the privacy of personal information, working with industry to deliver market-based approaches ranging from industry best practices, self-regulatory initiatives, advances in technology, and consumer education.

A core goal of these efforts has been to publicize how personal information is handled by companies, in the belief that, if armed with accurate information, consumers will make privacy choices consistent with their personal needs. The FTC has established a set of disclosures that responsible companies should provide to consumers in order to facilitate the consumers' exercise of informed choice about privacy in the marketplace.

Ten years later, it is appropriate to ask what effects these disclosures have had on consumers' experiences in the marketplace. Have improved privacy disclosures allowed consumers to achieve the level of privacy they desire in marketplace transactions? Are consumers more at ease with respect to privacy in marketplace transactions today then they were ten years ago? What is the effect of the existence of "privacy policies" at most of the leading websites? What do consumers think when they see the term "privacy policy"?

This article attempts to answer these questions based on existing peer-reviewed research and consumer surveys conducted in the academic sector. The article examines the strengths and limitations of the notice-based approach to facilitating privacy in the consumer marketplace. Using (1) survey data on consumers' privacy expectations, (2) existing research on whether and in what instances consumers read and comprehend notices, (3) the role information asymmetry and psychological barriers to information processing and risk assessment play in privacy decision-making, and (4) insights about interface design and information presentation, this article identifies several factors that limit the ability of the notice-based approach, operating alone, to meet the varying privacy needs of consumers in the marketplace. It concludes that:

- Without a baseline set of information practices, the term "privacy policy" is confusing to the consumer;

- The lack of common disclosure language undermines consumers' ability to "shop for privacy," thereby undermining businesses' ability to compete on privacy;

- Shortened notices are a promising step toward encouraging a successful privacy marketplace for the consumers who read notices;

- Privacy must be "usable" if it is to serve consumer needs; therefore, incorporating expertise from fields such as human computer interaction and psychology is imperative; and

- If consumers are not able to make informed choices about information privacy and computer security, then it is inevitable that bad actors will undermine consumer privacy and the security of the network infrastructure.

At this ten-year interval, it is important to consider the effect of the FTC's approach to privacy. Research provides important information about the strengths and limitations of the FTC's work to date. The FTC should use this information to refine and adjust its policy to reflect what we know today about consumer expectations and actions in the marketplace. In addition, this article's conclusions, listed above, suggest several additional interventions in the marketplace:

- Require businesses that advertise a "privacy policy" to provide some baseline privacy protections that meet established consumer expectations;

- Standardize disclosures and terminology to facilitate comparison shopping by consumers and competition among firms based on privacy practices;

- Shorten notices to reduce the transaction costs associated with reading long, indecipherable End User License Agreements ("EULAs"); and,

- Include information from other disciplines, including usability and human computer interaction, in future privacy and security initiatives.

## II. THE FTC'S APPROACH TO CONSUMER PRIVACY

Just over ten years ago, the FTC conducted its last forward-looking proceeding in which it analyzed the future of consumer protection in a high-tech economy. In a report from that proceeding, the FTC concluded that the essential elements of a balanced consumer protection program are:

- Coordinated law enforcement by state and federal agencies against fraud and deception;
- Industry self-regulation and private initiatives to protect consumers; and
- Consumer education through the combined efforts of government, business, and consumer groups.[2]

The report continues:

> The hearing record is replete with examples of private initiatives: industry self-regulation programs and plans to develop and expand such programs, technology-based consumer protections and self-help opportunities, and commitments to undertake new consumer education programs. These and other initiatives will be crucial in providing consumer protection in the new marketplace.[3]

Over the past ten years, the FTC has pursued these three goals. It has brought an impressive array of actions under the agency's authority to prosecute unfair or deceptive trade practices.[4] It has fostered self-regulatory programs and it continues to operate multilingual consumer outreach both online and offline.

The FTC established five Fair Information Practice Principles ("FIPPS")—notice, choice, access, security and accountability—as the

---

[2] Federal Trade Commission, *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (hearing report, May 1996): 46 (formatting added). Also available online at http://www.ftc.gov/opp/global/report/gc_v2.pdf.

[3] Ibid.

[4] Marcia Hoffman, "Federal Trade Commission Enforcement of Privacy," in *Proskauer on Privacy* (New York: Practicing Law Institute, 2006).

framework for self-regulatory and regulatory initiatives. The Commission's approach omitted several important data protection principles that were recognized by the Organization for Economic Cooperation and Development Guidelines ("OECD"), including the concepts of "data minimization," which requires companies to restrict the amount of personal information collected to only that which is necessary for a transaction, and "purpose specification," which requires companies to have a clear and legitimate purpose for data collection.

The absence of these two principles has led firms to collect extraneous information and to repurpose information without consumer consent. After adopting its limited set of FIPPS, the FTC highlighted the importance of notice and security. The agency did intervene to set standards for children's privacy that are stronger than the norm; the Children's Online Privacy Protection Act ("COPPA") requires prior parental consent before personal information can be collected from children under the age of thirteen.[5] In general, though, the agency put substantial resources behind encouraging adaptation of notice, and the development of "short notices." The market-based approach to privacy in the electronic commerce sphere adopted by the FTC was a departure from a tradition of privacy laws, such as the Fair Credit Reporting Act of 1970 ("FCRA") and the Privacy Act of 1974, which embraced a full set of FIPPS to protect personal information.

Most e-commerce sites today have privacy policies, but whether these policies provide privacy protection remains an open question. The FTC has not evaluated the basic assumption of the market-based model to privacy protection: that with good information consumers will make good choices. Echoing the recommendations from the 1995 hearings, Chairman Majoras seeks to employ the same techniques used to protect privacy during the last decade:

> First, we must study and evaluate new technologies so that we are as prepared as possible to deal with harmful, collateral developments. Second, we need to bring appropriate law enforcement actions to reaffirm that fundamental principles of FTC law apply in the context of new technologies. Third, we must look to industry to implement self-regulatory regimes and, more importantly, to

---

[5] *Children's Online Privacy Protection Act of 1998*, Public Law 105-277, codified at *U.S. Code* 15 (2000), §§ 6501 *et seq.*

> develop new technologies. Finally, we need to educate consumers so that they can take steps to protect themselves.[6]

At this important juncture, it makes sense to evaluate the strengths and weaknesses of these techniques. Before the FTC decides what approaches to pursue during the next decade, we suggest that the agency critically reflect on research that explores the effectiveness of the self-regulatory system.

The FTC has held close the assumption that introducing additional information about companies' data practices into the marketplace through self-regulatory systems, combined with consumer self-help, will allow consumers to adequately protect their privacy as they see fit. But research shows that consumers continue to have high levels of concern for privacy of personal information. It also reveals that the EULAs and privacy policies used to convey this information to consumers are not effective—they are rarely read and are in many instances unreadable. More importantly, consumers appear to believe that the term "privacy policy" conveys a specific level of privacy protection. Confusion exists among consumers concerning what rights they have and can exercise over personal information. Interestingly, while the FTC has pursued self-regulatory solutions to consumer privacy, the large majority of consumers believe incorrectly that laws protect their personal information from secondary use.

## III. RESEARCH DEMONSTRATES THE LIMITS OF THE DISCLOSURE-BASED APPROACH

### A. CONSUMERS CARE DEEPLY ABOUT PRIVACY

Surveys conducted by the Annenberg Public Policy Center show that Americans care deeply about the privacy of their personal information and that despite the FTC's ten-year commitment to self-regulation, they are nevertheless concerned about information collection.[7] A 2003 Annenberg survey found that 70% of advanced

---

[6] Deborah Platt Majoras, "Finding the Solutions to Fight Spyware: The FTC's Three Enforcement Principles," (remarks, Anti-Spyware Coalition, Washington, D.C., February 9, 2006): 3, http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf.

[7] Unless otherwise noted, the public polling data presented are from two national surveys created by Professor Turow and carried out by the firm ICR/International Communication Research of Media, Pennsylvania. For the 2003 survey, *infra* note 8, ICR interviewed by phone a nationally representative sample of 1,200 adults who were using the Internet at home.

users agreed or agreed strongly with the statement, "I am nervous about websites having information about me."[8] In 2005, the same response was reported by 79% of respondents.[9] Individuals also believe that they are put at risk as a result of information collection. Only 17% agreed with the proposition, "What companies know about me won't hurt me."[10]

A high level of concern is also reported about both commercial and government collection of personal information. In 2003, 92% reported that they would be concerned if marketers were "collecting information about your household members' activities without your knowledge or consent."[11] Similarly 83% would be concerned if the government was "collecting information about your household members' activities without your knowledge or consent."[12] (52% believed the federal government was doing that.[13]) Respondents also believe that they should be in control of marketing communications. For instance, 94% reported that websites should ask for permission before sending ads.[14]

### B. CONSUMERS FUNDAMENTALLY MISUNDERSTAND THE "PRIVACY POLICY" LABEL

Supporters of privacy self-regulation suggest that Americans' high levels of concern will be alleviated when they begin to examine their options for releasing personal data. Professor Alan Westin, for

---

For the 2005 survey, *infra* note 9, ICR interviewed by phone a nationally representative sample of 1,200 adults who said they used the Internet in the past month.

[8] Joseph Turow, *Americans and Online Privacy: The System is Broken* (Philadelphia: Annenberg Public Policy Center, June 2003): 16. Also available online at http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

[9] Joseph Turow, Lauren Feldman and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline* (Philadelphia: Annenberg Public Policy Center, June 2005): 4. Also available online at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf.

[10] Ibid.

[11] Turow, *Americans and Online Privacy*, 19–20.

[12] Ibid.

[13] Ibid., 19.

[14] Ibid., 28.

example, has written that most Americans take an informed cost-benefit tack in relation to their information online and offline.[15] "They examined the benefits to them or society of the data collection and use, wanted to know the privacy risks and how organizations proposed to control those, and then decided whether to trust the organization or seek legal oversight."[16] This characterization of most Americans as being aware of their online privacy options supports the viewpoint of Internet industry players that posting an accurate privacy policy on every site would create a world of optimal consumer privacy in which each individual shopped with his or her mouse for privacy that matched his or her personal needs.

Unfortunately that does not appear to be happening. One could assume from this that consumers do not care, the argument being that companies give individuals information and they ignore it or fail to value the privacy choices it offers. However, research tells a far more complex story about why privacy disclosures alone have failed to alleviate the privacy concerns of individuals.

The push for privacy disclosures has resulted in a world of legalistically phrased privacy policies that begin by assuring the consumer that the site cares about his or her privacy, but then proceeds to confuse the consumer with technical language about "affiliate" and "non-affiliate" sharing, required disclosures, distinctions between personally identifiable information ("PII") and aggregate data, inapplicability with regard to other sites, or content that may be included or accessed from the site, and finish with the caveat that the privacy policy can change at any time, with or without notice.[17]

Both the 2003 and 2005 Annenberg surveys revealed, however, that American adults do not know that privacy policies merely tell people how the site will use their information: whether or not, and how, they will share it with affiliates and outside firms.[18] Most

---

[15] A. F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues* 59, no.2 (2003): 445.

[16] Ibid.

[17] For example, of 64 website privacy policies that were reviewed between 2001 and 2003, Jensen and Potts found that eight (13%) offered no mention of how changes to the policy would be conveyed to the user, twelve policies (19%) offered to notify users through email and a posting on the policy page, and 44 policies (69%) required users to check the policy page periodically. C. Jensen and C. Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices," in *CHI 2004 Connect: Conference Proceedings* (New York: ACM Press, 2004), 471–78.

[18] Turow, *Americans and Online Privacy*, 3; Turow, Feldman and Meltzer, *Open to Exploitation*, 3.

Americans believe, logically, that the phrase "privacy policy" signifies that *their information will be kept private*. In the 2003 survey, 57% of the nationally representative sample of 1,200 adults who were using the Internet at home agreed or agreed strongly with the statement, "When a web site has a privacy policy, I know that the site will not share my information with other websites or companies."[19] In the 2005 survey, questioners asked 1,200 nationally representative adults who said they had used the Internet in the past month whether that statement is true or false; 59% answered it is true.[20]

### C. CONSUMERS MISUNDERSTAND ONLINE DATA COLLECTION

The misunderstandings do not stop with the label. The 2003 survey found that 59% of adults who use the Internet at home know that websites collect information about them even if they do not register;[21] however, they do not understand that data-flows behind their screens connect seemingly unrelated bits about them.[22] The survey's interviewers asked respondents to name a site they valued and then went on to ask their reaction to click-stream advertising,[23] which is actually a common way that sites track, extract and share information to make money from advertising. Of the surveyed adults who go online at home, 85% stated that they did not agree to the collection and aggregation of their data across multiple sites for purposes of click-stream advertising, even by a "valued" site.[24] When offered a choice of using a valued site for free and letting information be collected, or paying for the site and not letting information be collected, 54% of adults who go online at home said that they would rather find the information offline than exercise either option presented.[25]

---

[19] Turow, *Americans and Online Privacy*, 3.

[20] Turow, Feldman and Meltzer, *Open to Exploitation,* 20.

[21] Turow, *Americans and Online Privacy*, 3.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] Ibid.

Among the 85% who did not accept the data-collection practice, one in two (52%) had earlier said that they gave or would likely give the valued site their real name and email address.[26] Yet those bits of information are what a site needs to begin creating a stream of data about them—the very flow, personally identifiable or not, that they refused to allow in response to the scenario. Moreover, 63% of the people who said they had provided this data had also agreed that the mere presence of a website privacy policy means that the website will not share data with other firms.[27] Bringing these two results together suggests that at least one out of every three respondents who refused to barter their information either do not understand or do not think through the privacy outcomes of basic data-collection activities on the Internet.

Similarly, other fundamental processes involved in online interactions are not very well understood by the consumer. In a related survey, Acquisti and Grossklags show that individuals are often unable to name obvious parties, beyond the merchant and the consumer, that have access to consumer data during and after an online credit card transaction, such as the credit card company.[28] These findings help uncover the important distinction between knowledge about commercial practices that is active and actionable, and knowledge that is passive or completely lacking. Most consumers have some passive knowledge about the roles played by credit card companies, other third parties, and technical processes, but it is doubtful that this knowledge is always available to them when they are actively making decisions.

## D. CONSUMERS MISUNDERSTAND MANY RULES ABOUT PRIVACY IN THE MARKETPLACE

These misconceptions about information privacy and data practices are, however, merely the tip of an iceberg of consumer confusion concerning their rights and merchants' rights to consumer information

---

[26] Ibid.

[27] Ibid., 23.

[28] When 119 university staff and students were confronted with the open-ended question: "You completed a credit-card purchase with an online merchant. Besides you and the merchant Web site, who else has data about parts of your transaction?" 34.5 percent of the sample answered "nobody," 21.9 percent answered "my credit card company or bank," and 19.3 percent answered "hackers or distributors of spyware." A. Acquisti and J. Grossklags, *Privacy and Rationality in Individual Decision Making*, *IEEE Sec. & Privacy* 3, no. 1 (2005): 26–33.

in the marketplace. Table 1 lists true-or-false statements that the 2005 Annenberg survey presented to its representative national sample.[29] The answers indicate a low level of understanding of consumer rights and redress in the marketplace. A high proportion of consumers believe they have certain privacy rights—notably consistent with those provided under FIPPS—when they do not. Others simply have no idea what rights they have.

**Table 1: True/false responses to statements about rules of profiling, behavioral targeting, price discrimination and recourse in the marketplace.** (1,500 persons sampled)

| | %T | %F | %DK |
|---|---|---|---|
| Most online merchants give me the opportunity to see the information they gather about me.<br>*47% did not know the right answer* | 23 | **53** | 25 |
| Most online merchants allow me the opportunity to erase information they have gathered about me.<br>*50% did not know the right answer* | 19 | **50** | 30 |
| A website is allowed to share information about me with affiliates without telling me the names of the affiliates.<br>*49% did not know the right answer* | **51** | 29 | 20 |
| It is legal for an online store to charge different people different prices at the same time of day.<br>*62% did not know the right answer* | **38** | 29 | 33 |
| Respondent correctly identifies the name of a credit-reporting agency.<br>*66% did not know the right answer* | **34** | 66 | -- |
| By law, a site such as Expedia or Orbitz that compares prices on different airlines must include the lowest airline prices.<br>*68% did not know the right answer* | 37 | **32** | 31 |

[29] Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

| **Table 1: (continued)** | | | |
|---|---|---|---|
| It is legal for an offline store to charge different people different prices at the same time of day.<br>*71% did not know the right answer* | **29** | 42 | 29 |
| | | | |
| Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know | | | |

A 2007 Golden Bear telephone survey of Californians reinforces the idea of consumer misunderstanding about online marketplace privacy policies and rules.[30] This survey focused on people who have actually purchased items on the Internet and, as such, would presumably be more informed than participants in the Annenberg studies, who were adults who used the Internet for any reason. Moreover, the statements about rules and privacy policies in the Golden Bear survey were more varied than those in the Annenberg study.

Despite their presumably greater stake in commerce and privacy than the Annenberg respondents, the Golden Bear respondents followed the same pattern; almost 70% of the respondents knew that sites are allowed to keep records of their addresses and purchase histories. The respondents' knowledge was much worse, however, with respect to the other statements about privacy policies and marketplace rules, as Table 2 shows. Note that when presented with a privacy-policy statement that was similar to the one in the Annenberg study—if a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies—the percentage of respondents who answered incorrectly was very similar, 55% in Golden Bear compared to 59% in Annenberg.

[30] The 2007 Golden Bear Omnibus Survey was a random-digit telephone survey of 1,186 English- and Spanish-speaking adults in California. It was conducted by the University of California's Survey Research Center using Computer-Assisted Telephone Interviewing (CATI) to landline and wireless phones from April 30, 2007, to September 2, 2007. It was funded by the Survey Research Center. The privacy questions were funded by the Samuelson Clinic.

**Table 2: True/false responses to statements about rules of the online marketplace.**

| | %T | %F | %DK |
|---|---|---|---|
| If a website has a privacy policy, it means that the site cannot keep records of your address and purchase history. (188 persons sampled)<br>*30.9% did not know the right answer* | 19.7 | **69.1** | 11.2 |
| If a website has a privacy policy, it means that the site cannot give information about your address and purchases to the government. (208 persons sampled)<br>*45.2% did not know the right answer* | 36.1 | **54.8** | 9.1 |
| If a website has a privacy policy, it means that the site cannot use information to analyze your online activities. (205 persons sampled)<br>*47.8% did not know the right answer* | 37.1 | **52.2** | 10.7 |
| If a website has a privacy policy, it means that the site cannot buy information about you from other sources to analyze your online activities. (251 persons sampled)<br>*50.6% did not know the right answer* | 39.8 | **49.4** | 10.8 |
| If a website has a privacy policy, it means that the site cannot share information about your address and purchases with affiliated companies that are owned by the website. (207 persons sampled)<br>*55% did not know the right answer* | 47.8 | **44.9** | 7.2 |
| If a website has a privacy policy, it means that you have the right to require the website to tell you what other businesses purchased your personal information. (208 persons sampled)<br>*60.1% did not know the right answer* | 51.9 | **39.9** | 8.2 |
| | | | |

| **Table 2: (continued)** | **%T** | **%F** | **%DK** |
|---|---|---|---|
| If a website has a privacy policy, it means that you have the right to obtain help from the website, if information you provided to it was used for identity theft. (198 persons sampled)<br>*64.1% did not know the right answer* | 49.5 | **35.9** | 14.6 |
| If a website has a privacy policy, it means that the site cannot sell information about your address and purchase information to other companies. (231 persons sampled)<br>*64.5% did not know the right answer* | 55.4 | **35.5** | 9.1 |
| If a website has a privacy policy, it means that you have the right to sue the website for damages if it violates your privacy. (230 persons sampled)<br>*65.6% did not know the right answer* | 53 | **34.3** | 12.6 |
| If a website has a privacy policy, it means that you have the right to access your personal information stored on the site and correct it. (222 persons sampled)<br>*72.1% did not know the right answer* | 56.8 | **27.9** | 15.3 |
| If a website has a privacy policy, it means that you have the right to be notified if the website has a security breach that leaks information about you to others. (215 persons sampled)<br>*75.4 did not know the right answer* | 64.7 | **24.7** | 10.7 |
| If a website has a privacy policy, it means that you have the right to require the company to delete your personal information upon your request. (213 persons sampled)<br>*77% did not know the right answer* | 68.1 | **23** | 8.9 |
| | | | |
| Bold numbers indicate the correct answer. Sums greater than 100% result from rounding errors. DK=Don't Know. | | | |

## E. PRIVACY NOTICES ALONE ARE INSUFFICIENT

Despite self-regulatory efforts, there remains substantial confusion among consumers about information privacy. Much of the FTC's attention has focused on the development of improved disclosures. Surveys, user studies, and focus groups do support the agency's belief that users would welcome well-crafted, short notices in the hope that they will ease comprehension of privacy policies.

In research supported by the National Science Foundation Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"),[31] researchers at U.C. Berkeley's Samuelson Clinic have examined the utility of short notices and variations on notice timing in communicating about privacy, security, and other consequences of software installation.[32] The installation of downloadable software almost always involves the click-through to privacy notices and EULAs. Notices are usually presented in a separate screen during installation and are reasonably accessible to the user. Users are involved in a main task of evaluating and deciding whether to install a piece of software. Given that information about security, privacy, and functionality are disclosed during the installation process, this is a natural context in which to explore the utility of such notices and disclosures.

Recent studies involving EULAs suggest that they are largely ineffective as a means of communicating with consumers. EULAs, terms-of-service agreements ("ToS"), and privacy policies present complex legal information. Research shows that notices' complexity

---

[31] This work was generously supported by the NSF Science and Technology Center, Team for Research in Ubiquitous Secure Technologies ("TRUST"), NSF CCF-0424422. Computer trustworthiness continues to increase in importance as a pressing scientific, economic, and social problem. As a consequence, there is an acute need for developing a much deeper understanding of the scientific foundations of cyber security and critical infrastructure systems, as well as their implications for economic and public policy. In response to this need, TRUST is devoted to the development of a new science and technology that will radically transform the ability of organizations (software vendors, operators, local and federal agencies) to design, build, and operate trustworthy information systems for our critical infrastructure. The Center brings together a team with a proven track record in relevant areas of computer security, systems modeling and analysis, software technology, economics, and social sciences. See http://trust.eecs.berkeley.edu/ for details of all of TRUST's research.

[32] For detailed results of the studies, see Nathaniel Good and others, "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware," in *Proceedings of the Symposium on Usable Privacy and Security* (New York: ACM Press, 2005), 43–52; Nathaniel Good and others, "Noticing Notice: A Large-scale Experiment on the Timing of Software License Agreements" in *Proceedings of CHI 2007* (New York: ACM Press, 2007), 607–16.

hampers users' ability to understand such agreements. For example, Jensen and Potts studied a sample of 64 privacy policies from high-traffic and healthcare websites.[33] They found that the policies' formats, locations on the websites, and legal content severely limit users' ability to make informed decisions based on them.[34]

In another study that produced similar results, Grossklags and Good evaluated the notice practices of 50 popular downloadable programs.[35] The location and presentation of the notices differed from vendor to vendor, which would make it more difficult for consumers to find relevant information. These notices were often difficult to understand or even read. The average EULA was over 2500 words long and would require approximately thirteen minutes for a consumer of average reading skill to parse, according to accepted reading metrics. Font sizes were often too small to be read easily and notices were displayed in comparatively small windows, for example, showing only one percent of the complete notice text at a time.

Research indicates that simplifying the notices has a limited effect. Masson and Waldron showed that simplifying the language of legal contracts, for example, by using easier words and replacing obscure terms with common ones, could not achieve very high degrees of comprehension.[36] This is because "non-experts have difficulty understanding complex legal concepts that sometimes conflict with prior knowledge and beliefs."[37]

Vila and others ask whether users will ever bother to read or believe privacy policies at all.[38] They claim that because the cost of

---

[33] Jensen and Potts, "Privacy Policies as Decision-making Tools: An Evaluation on Online Privacy Notices."

[34] Ibid.

[35] Jens Grossklags and Nathan Good, "Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers," in *Lecture Notes in Computer Science* (Berlin: Springer, 2008), 341–55. Originally presented at Useable Security (USEC'07), February 15–16, 2007. Also available online at http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-USEC.pdf.

[36] M.E.J. Masson and M.A. Waldron, "Comprehension of Legal Contracts by Non-experts: Effectiveness of Plain Language Redrafting," *Applied Cognitive Psychology* 8 (1994): 67–85.

[37] Ibid.

[38] T. Vila, R. Greenstadt and D. Molnar, "Why We Can't be Bothered Reading Privacy Policies - Models of Privacy Economics as a Lemons Market," in *Proceedings of the Fifth International Conference on Electronic Commerce* (Pittsburg: ICEC, 2005), 403–07. Also available online at http://www.eecs.harvard.edu/~greenie/econprivacy.pdf.

misrepresentation in a privacy policy is low and that some of the privacy policies are not trustworthy, users do not feel it is worth their time to read or pay attention to them.[39] In contrast, results from the 2003 Annenberg survey suggest that relatively high proportions of adults with the Internet at home trust privacy policies; 71% agreed or agreed strongly, "I look to see if a website has a privacy policy before answering any questions."[40] Anecdotal evidence does, however, support the impression that people do not read the policies. One software provider included a $1000 cash prize offer in a EULA that was displayed during every software installation. It took four months and 3,000 downloads of the software for someone to notice the clause and claim the prize.[41]

Among 222 study participants, the Samuelson Clinic found that only 1.4% reported reading EULAs often and thoroughly, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them.[42]

Short and layered notices are one method that has been proposed to overcome these problems. The Samuelson Clinic has performed a controlled study of short notices and timing of notices. The study examined whether consumers were happy with their installation decisions after they were fully informed of the program's activities; this is termed "regret." When downloading and installing programs, subjects were shown either the EULA by itself or the EULA and a short notice highlighting core aspects of performance, privacy and security.

During the post-experimental survey, all study participants were shown the short notices. When asked whether they would install the programs they chose to install during the experiment, participants who received the short notices during the study were less likely to reverse their earlier decision to install software. However, many users, both those who originally received the short notice and those who did not, expressed regret about their installation decisions after reading the short notice during the exit interview. Overall, the incidence of regret

---

[39] Ibid.

[40] Turow, *Americans and Online Privacy*, 18.

[41] Larry Magid, It Pays To Read License Agreements, http://www.pcpitstop.com/spycheck/eula.asp (accessed January 22, 2008).

[42] See 2007 Golden Bear Omnibus Survey.

was high. Importantly, however, the incidence of regret was lower when short notices were received before program installation.

### F. OTHER FORCES ALSO PREVENT CONSUMERS FROM SUCCESSFUL PRIVACY PROTECTION

Beyond the issues of whether consumers read and comprehend privacy policies, individuals' ability to make marketplace privacy decisions that reflect their needs is hampered by several factors. Incomplete information is a major difficulty. Even when they read privacy notices and EULAs, consumers have trouble evaluating the consequences of disclosing the bundles of information that companies say they are taking. Consumers have difficulty assessing and valuing certain privacy risks, which makes their decisions seem unpredictable, even random. Sometimes risks become known only after a security breach or privacy invasion.

Moreover, while many consumers are certainly aware of many privacy risks, they may not be well informed about the magnitude of these risks in certain circumstances. Acquisti and Grossklags report, for example, that 73% of respondents in their survey underestimated the risk of becoming a victim of identity theft.[43]

> Adding to the problem of incomplete information is the challenge of grasping the abilities of technologists to take seemingly innocuous items of information and link them in new, unexpected ways. For example, when asked, "Imagine that somebody does not know you but knows your date of birth, sex, and zip code. What do you think the probability is that this person can uniquely identify you based on those data?," 68.6% answered that the probability was 50% or less (and 45.5% of respondents believed that probability to be less than 25%). According to Carnegie Mellon University researcher Latanya Sweeney, however, 87% of the US population may be uniquely identified personally through a 5-digit zip code, birth date, and sex. To expect individuals to foresee such possibilities is unreasonable.[44]

---

[43] Acquisti and Grossklags, *Privacy and Rationality*.

[44] Ibid., 24.

Even if individuals have access to complete information about privacy risks and modes of protection, they might not be able to process enough data to formulate a rational privacy-sensitive decision. Human beings' rationality is bounded, which limits our ability to acquire and then apply information. Furthermore, consumers are busy and experience many demands on their attention. They cannot be expected to be familiar with all the vagaries of technologies, e-commerce, and evolving business practices.

### G. CONSUMERS ARE LIMITED IN THEIR ATTEMPTS TO PROTECT THEIR INFORMATION

Evidence abounds that consumers do try to protect their privacy. Survey results released in June 2004 by Privacy & American Business found that two-thirds of Americans have taken some steps to protect their privacy.[45] In fact, 87% indicated that they had asked a company to remove their information from a marketing database; 60% decided not to patronize a store because of doubts about the company's privacy protections; and 65% had declined to register at an e-commerce site because of privacy concerns.[46] Among individuals that Westin has described as the "privacy unconcerned," 47% reported that they engaged in four out of seven identified privacy-protecting behaviors, while 65% of the "privacy pragmatists" had engaged in these behaviors.[47]

Situational characteristics can reduce consumers' efforts to protect their information. For example, Spiekermann, Grossklags, and Berendt observed 171 study participants while they shopped online, specifically when they interacted with an anthropomorphic sales advisor. By answering questions posed by the advisor, study participants could receive recommendations about products. The advisor also asked questions that were highly intrusive of privacy or that requested irrelevant information. Participants could simply have refused to respond to these questions, thereby protecting themselves against potential threats. However, regardless of the strength of the participants' self-reported privacy preferences, their actual responses

---

[45] Privacy & American Business, "New National Survey on Consumer Privacy Attitudes to be Released at Privacy & American Business Landmark Conference," news release, June 10, 2004.

[46] Ibid.

[47] Westin, "Social and Political Dimensions of Privacy," 445.

to the advisor revealed much more information than their self-reported preferences predicted, even among the "privacy-concerned" individuals. These results demonstrate the power of interactive marketing techniques to lead even privacy-motivated consumers to behave in ways that appear contradictory to their stated preferences.[48] The similarity between the behavior of the "unconcerned" participants and the behavior of participants who claim to be highly concerned about privacy suggests that Westin's dichotomy may be less useful than previously thought in capturing the nuances of consumers' attitudes on privacy.

Further evidence that we need a more differentiated understanding of protection behaviors is provided by Acquisti and Grossklags.[49] They found that at least 75% of the consumers did adopt at least one strategy or technology, or otherwise took some action, to protect their privacy, such as interrupting purchases before entering personal information or providing incorrect information in website forms.[50] However, they also found that use of specific technologies was consistently low across the sample population.[51] For example, 67% of respondents never encrypted their email, 82% never put a credit alert on their credit report, and 82% never removed their phone numbers from public directories.[52]

Other findings suggest that while people would like to protect their privacy, and try to at the most basic levels, a large proportion of these people do not have the knowledge necessary to move beyond the very basics of privacy-protective behavior. Before concluding that people do not put a credit alert on their credit report because they are lazy or uncaring, recall the Annenberg survey finding that 66% do not know the name of a credit agency and 76% do not correctly respond "false" to the statement, "the Federal Trade Commission will correct errors in credit reports if it is shown proof of the errors."

---

[48] S. Spiekermann, J. Grossklags and B. Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, (New York: ACM Press, 2001), 38–47. Also available online at http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.

[49] Acquisti and Grossklags, *Privacy and Rationality in Individual Decision Making*, 26–33.

[50] Ibid.

[51] Ibid.

[52] Ibid.

In the online environment, the complexity of privacy-protecting actions increases, and thus the likelihood that Americans perform them decreases substantially. The 2003 Annenberg survey asked American adults who use the Internet at home if they performed certain activities in relation to controlling their information online; 65% said that the have erased unwanted cookies at least once. This finding is consistent with the finding that a clear majority of the sample—59%—was aware of what cookies do; people know that when they go online, sites collect information on them even if they do not register. The percentage applying other privacy tools drops steeply, however. Only 43% said that they have used filters to block unwanted email, 23% said they have used software that looks for spyware, and 17% said they have used anonymizers—"software that hides your computer's identity from websites that they visit."

## IV. WHAT THE FTC MUST CONFRONT IN THE NEXT DECADE

### A. AMERICANS' CONTINUING CONCERNS AND CONFUSIONS ABOUT INFORMATION PRIVACY

Research indicates that American consumers care deeply about information privacy and worry that it is not well protected. It also reveals that great majorities of American consumers do not grasp basic facts about companies' data collection practices, do not know the laws that govern data protection, do not read or comprehend the notices that are supposed to explain data practices and afford privacy choices, and are confronted with many social and psychological factors that undermine their ability to protect their privacy during marketplace transactions.

Most fundamentally, research indicates that a large majority of American adults believe that the existence of a "privacy policy" on a website indicates some level of substantive privacy protection for their personal information. The finding is not an aberration. Two major national surveys performed two years apart, in 2003 and 2005, revealed virtually the same percentage of Americans—almost 60%—believed that "when a website has a privacy policy, that means it will not share information about them with other websites or companies."[53] In the 2005 survey, where the statement was presented in true/false

[53] Turow, *Americans and Online Privacy*, 4; Turow, Feldman and Meltzer, *Open to Exploitation*, 20.

form, 59% incorrectly said the statement was true and an additional 16% said they did not know if it was true or false.[54]

Because American consumers mistakenly believe that a "privacy policy" indicates a level of substantive privacy protection, they do not read them. The failure to read privacy policies leaves consumers unaware of data practices such as data-mining and allows a wide range of practices that are inconsistent with consumer expectations to avoid consumer scrutiny.

Under the Federal Trade Commission's notice and choice regime, the operating assumption is that people will make good choices if they are provided with good information. Our studies have found that Americans do not have good, i.e., full and understandable, information about data practices that affect their privacy.[55] More significantly, even if full and understandable information is provided in a short format, consumers retain the belief that the mere invocation of the term "privacy policy" creates a baseline set of protections for their information. That belief, along with other cognitive biases, limits the number of consumers who read and act on such privacy notices. If a website contains a privacy policy that states it will reveal users' data to affiliates or other companies without the users' permission, then the privacy of consumers who stop reading once they see that a privacy policy exists is undermined.

### B. THE CURRENT NOTICE-BASED APPROACH HAS CONSEQUENCES FOR THE SECURITY OF THE NETWORK ITSELF

Consumers' basic misunderstanding of the purpose of privacy policies is one of many misconceptions that contribute to confusion in the online marketplace. When consumers do not read, or read but cannot understand, privacy notices and EULAs on websites and software, they may unwittingly install malicious programs that exploit consumer machines to the detriment of the entire Internet. Unless "privacy policies" provide some baseline privacy protections, the notice-based privacy regime will continue to unintentionally lead consumers to "consent" to invasive program installations and other practices. By doing so, they lower the security protections of the entire network, not just their own computers.

---

[54] Turow, Feldman and Meltzer, *Open to Exploitation*, 15.

[55] See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

One case in point is the 2005 wide-scale installation of a "rootkit" by purchasers of music CDs.[56] In an attempt to control the distribution of songs on the CD, Sony bundled a program that ran silently in the background and opened many computers to security vulnerabilities. Similarly, spyware, even if "consensually" installed pursuant to a EULA, can allow millions of computers to be controlled by others. This allows bad actors to create "botnets," e.g. zombie networks of consumers' computers, which can be remotely directed to engage in denial-of-service attacks and other malicious acts.

### C. THE NEED TO ADOPT THREE POLICIES TO SUPPORT INFORMATION PRIVACY

To advance privacy, the Federal Trade Commission should take the following three steps:

#### 1. THE FTC SHOULD POLICE THE TERM "PRIVACY POLICY"

Two national surveys by the Annenberg Public Policy Center revealed that to a majority of American consumers, "privacy policy" carries a particular meaning: that a website will not disclose personal information to others without the consumer's permission. While many websites begin their privacy policies with the claim that "your privacy is important to us," many of these same policies disclose further down that the websites collect quite a bit of the information from their users and often do share the information with affiliates, marketers, or other entities. Note, too, that information-sharing agreements with third parties generally are under no legal requirement to be disclosed; there is no other source for this omitted information. The result is a situation where consumers assume that the privacy policy label indicates that the site will not share data, whereas the opposite may be true and the policy may or may not state what is done with the information.

Given consumers' expectations, the use of the term "privacy policy" absent some baseline privacy protections, ought to be considered deceptive. The Commission evaluates potentially deceptive marketing communications to consumers based upon

---

[56] Deirdre K. Mulligan and Aaron K. Perzanowski, "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident," *Berkeley Technology Law Journal* 22 (2007): 1157.

whether the representation is "likely to mislead reasonable consumers under the circumstances. The test is whether the consumers' interpretation or reaction is reasonable."[57] The FTC's guidance specifies that communications should be judged upon "the basis of the net general impression conveyed . . . ."[58] The Policy Statement on Deception advances five model questions for evaluating a representation: how clear is the representation, how conspicuous is any qualifying information, how important is the omitted information, do other sources for the omitted information exist, and how familiar is the public with the product or service?[59]

Given consumer expectations, the use of the label "privacy policy" by websites that share information about their users without user permission is deceptive. First, surveys demonstrate that reasonable consumers believe that the mere presence of a privacy policy means that substantive protections are in place to prevent the sharing of their information. Websites' top-level assertions about privacy are often very clear; sites abound with privacy seals and claims that "your privacy is important to us." As such, "privacy" is used as a marketing tool, a type of quality representation that consumers find meaning in and rely upon. Qualifying information, by contrast, is buried within privacy policies in the fine print. As we have shown, this qualifying information is often not understandable and often goes unread by consumers who presume that the policies extend many rights, and thus are not necessary to read.[60] In cases where sites share information without consumer consent, therefore, the use of the term "privacy policy" is deceptive under FTC guidelines.

The Federal Trade Commission should rule, then, that websites using the label "privacy policy" are deceptive unless those sites promise not to share information about their users without their permission. While sites that engage in such sharing without user permission should be required to make disclosures, they should not be allowed to refer to such disclosures as "privacy policies."

---

[57] James C. Miller III, *FTC Policy Statement on Deception* (October 14, 1983). Also available online at http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[58] Ibid.

[59] Ibid.

[60] See Turow, *Americans and Online Privacy*; Turow, Feldman and Meltzer, *Open to Exploitation*.

### 2. PRIVACY MECHANISMS SHOULD BE VETTED BY USABILITY AND OTHER EXPERTS

Currently, notices are written to satisfy lawyers. The notices do not help consumers make privacy choices that reflect their privacy interests. If the FTC wants consumers to make smart decisions on privacy, then experts in usability and other areas need a seat at the table. Such experts need to help craft privacy-protecting mechanisms. Consumers would benefit from the involvement of experts in usability and psychology in designing notices and other privacy mechanisms. Research at the Samuelson Clinic and elsewhere is beginning to identify the features that can improve the chances that consumers read, comprehend and act upon privacy notices in a manner consistent with their needs and expectations. The FTC needs to avail itself of that research and the expertise behind it.

### 3. THE FTC SHOULD SET BENCHMARKS FOR SELF-REGULATION

In announcing the 2006 Tech-ade hearings, Chairman Majoras asked:

> [W]hat have we learned over the past decade? How can we apply those lessons to what we do know, and what we cannot know, as we look to the future? And how can we best protect consumers in a marketplace that now knows no bounds, that is virtual, 24-7, and truly global?[61]

The FTC would be better equipped to evaluate what it has learned about self-regulation if it had adopted a reasonable recommendation offered by Privacy Rights Clearinghouse Executive Director Beth Givens in 1996—that the agency set performance benchmarks for self-regulation.[62] Without benchmarks, self-regulation and regulation, for that matter, have no clear metrics for measuring success. Accordingly, we recommend that the FTC define clear benchmarks for its privacy initiatives—educational, regulatory and self-regulatory—and evaluate its approach against those benchmarks between now and 2016.

---

[61] See Majoras, Anti-Spyware Coalition.

[62] FTC, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, n. 156 (Dec. 2006).

## V. CONCLUSION

The next decade will bring new technologies that will be able to extract far more information from and about Americans than was previously possible.[63] These technologies will raise new and complex privacy issues. The FTC should plan its activities for the next decade based on a reasoned assessment of its policy initiatives over the last ten years. While some progress has been made, it is clear that consumers remain unable to fully effectuate their privacy rights in the marketplace. Providing consumers with more information about data practices has not led to greater consumer confidence or to a rich marketplace of privacy options for consumers. It is clear that if the FTC continues to pursue a market-based approach, additional interventions are necessary to ensure that consumers are not misled and have straightforward information available that facilitates privacy choices.

---

[63] Turow, *supra* note 1.

# INTERNALIZING IDENTITY THEFT

Chris Jay Hoofnagle[1]



---

[1] This work was supported by the California Consumer Protection Foundation, Cassandra Malry, Executive Director and by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies. The protocol was approved by U.C. Berkeley Office for the Protection of Human Subjects CPHS#2007-9-7, the "FACTA Access Study." I am indebted to Professors Deirdre Mulligan, Daniel Solove, Alessandro Acquisti, Jason Schultz, and Jennifer Urban. Jennifer King, Maryanne McCormick, and Aaron Burstein provided valuable advice, as did identity theft experts Evan Hendricks and Mari Frank. Additionally, Madison Ayer and Rick Lunstrum of ID Watchdog were instrumental in the recruitment of data subjects. This article builds upon three earlier works by Chris Jay Hoofnagle focusing upon problems in identity theft: *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors*, *in* SECURING PRIVACY IN THE INTERNET AGE 207 (Anupam Chander et al. eds., Stan. Univ. Press 2008), *available at* http://ssrn.com/abstract=650162, *Towards a Market for Bank Safety*, 21 LOY. CONSUMER. L. REV. 155 (2008), *available at* http://www.luc.edu/law/activities/publications/clrdocs/vol21issue2/hoofnagle_bank_safety.pdf, and *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J.L. & TECH. 97 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf.

# ABSTRACT

Why has identity theft remained so prevalent, in light of the development of ever more sophisticated fraud detection tools? Identity theft remains at 2003 levels -- 9.9 million Americans fell victim to the crime in 2009.

One faction explains the identity theft as a problem of a lack of control over personal information. Another argues conversely that identity theft may be caused by a lack of access to personal information by credit grantors. This article presents data from a small sample of identity theft victims to explore a different dimension of the crime, one that suggests alternative interventions.

Drawing upon victim and impostor data now accessible because of updates to the Fair Credit Reporting Act, the data show that identity theft impostors supply obviously erroneous information on applications that is accepted as valid by credit grantors. Thus, the problem does not necessarily lie in control nor in more availability of personal information, but rather in the risk tolerances of credit grantors. An analysis of incentives in credit granting elucidates the problem: identity theft remains so prevalent because it is less costly to tolerate fraud. Adopting more aggressive and expensive anti-fraud measures is extremely costly and jeopardizes customer acquisition efforts.

These business decisions leave individuals and merchants with some of the externalities of identity theft. Victims sometimes spend their own money, and more often, valuable personal time dealing with identity theft externalities. This article concludes by reviewing several approaches to internalizing these costs. Popular approaches specify prescriptive rules to address particularly problematic practices in credit granting, such as using the Social Security number as a password for authentication. These approaches may lead to compliance-oriented approaches and reification. Several commenters have suggested negligence actions as a cure to identity theft, but uncertainty surrounding the duty of care would probably leave many consumers unremunerated. A strict liability regime is suggested because credit grantors are the least cost avoiders in the identity theft context, and because consumers cannot control the credit granting process nor insure against identity theft losses efficiently.

# I. INTRODUCTION

The legal academic literature frames the identity theft problem in two very different ways.

The first is based on the work of Professor Lynn LoPucki who made an early and substantial contribution to the study of identity theft with two articles examining the problem of credit authentication.[2] In his 2003 paper, LoPucki argues that identity theft exploded in incidence in the 1990s because of the inability of credit grantors to authenticate borrowers.[3] This inability was caused by the decline of public life, the gradual removal of contact information from public registers, such as the DMV database, city directories, and the phonebook.[4] Indeed, as Dennis Bailey argues, modern life is akin to a masquerade ball, where we go unrecognized and cannot recognize others.[5] LoPucki argues that this privacy itself -- the deprivation of publicly-available information about our lives -- might have caused the identity theft epidemic and might have also given impostors the ability to masquerade as others undetected:

> It is probably no coincidence that the rise of identity theft coincided with the decline in public identities. That decline began in the 1970s. Credit-based identity theft emerged as a significant problem in the 1980s, hitting epidemic proportions only in the 1990s. The inverse relationship between privacy and public identity -- logically and chronologically -- suggests that privacy is a cause, if not the principle cause, of identity theft.[6]

In the other paradigm, Professor Daniel J. Solove frames identity theft as a problem of a loss of control over personal information. He argues that the traditional model for protecting privacy, one that conceives of harms as discrete events that affect individuals, cannot address new social and technological developments that have created "systemic" changes.[7] For instance, the adoption of the Social Security number (SSN) without protections against misuse has put all Americans at greater risk of identity theft. Solove calls this an "architecture of vulnerability."

> Identity thieves, then, are only one of the culprits in identity theft. The government and private-sector entities bear a significant amount of responsibility, yet this is cloaked in the conception of identity theft as a discrete crime that the victim could have prevented had she exercised more care over her personal data. Identity theft does not merely happen; rather, it is manufactured by a legally constructed architecture.[8]

---

[2] *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89 (2001) [hereinafter LoPucki, *Human Identification Theory*]; Lynn LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003) [hereinafter LoPucki, *Privacy*].
[3] *See* LoPucki, *Privacy*, *supra* note 2, at 1278.
[4] *See id.* at 1277-78.
[5] *See* DENNIS BAILEY, THE OPEN SOCIETY PARADOX: WHY THE 21ST CENTURY CALLS FOR MORE OPENNESS-NOT LESS 26 (2004).
[6] LoPucki, *Privacy*, *supra* note 2, at 1278 (citation omitted).
[7] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (2003).
[8] *Id.* at 1261 (citation omitted).

Solove thus proposes a privacy architecture that reflects the liberal "privacy-control" paradigm identified by Paul Schwartz.[9] Under the Solove approach, individuals would have substantive and procedural rights to learn about credit authentication and to limit dissemination of data. This transparency and control would inhibit impostors from stealing identities.

This article enriches the dimensions explored by LoPucki and Solove through an analysis of a small sample of identity theft cases. Part II of this article explains the Fair and Accurate Credit Transactions Act ("FACTA") Access Study. In this study, impostors' credit applications and other materials were acquired for the purpose of analyzing how businesses authenticated credit applicants. Materials from 16 incidents of identity theft were obtained pertaining to 6 individuals who were victims of financial, medical, and criminal identity theft. Every financial credit application contained some type of incorrect personal information, yet credit grantors chose to extend products and services to the impostor. But the problem is not limited to the financial sector. Other institutions, such as medical care providers and jails, overlooked incorrect personal information when verifying individuals' identities.

In light of these findings, part III of this article adds a new dimension to the LoPucki and Solove approaches, explaining that identity theft cannot be framed as a problem of too much privacy or a lack of privacy-control. I argue that tolerating risk of identity theft and accepting its attendant losses is a rational decision from a business perspective. Of course, all businesses must tolerate some fraud risk. But incentives particular to the credit industry and competition in instant credit markets create an atmosphere that impostors can leverage. The risk of new account fraud is extremely low in light of the volume of new credit accounts that are granted in the United States. Anti-fraud interventions, when scaled to the enormous credit volume exercised by Americans, are often not cost effective. Further, anti-fraud interventions also cause opportunity costs and possible lost sales to competitors that are less circumspect in verifying identities. There is thus some rationality in accepting credit applications of dubious veracity.

Much of the identity theft debate has focused upon improving technical security measures. Some have even suggested adding biometric identifiers to harden payment systems. As Ross Anderson notes, it is common for information security issues to be seen as mere technical problems.[10] But upon deeper analysis, he argues that information security mechanisms "are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk. Often this is perfectly rational."[11] This article follows Anderson's theme: identity theft is a problem of misaligned incentives. This should not be so surprising in light of recent events. The recent economic downturn has elucidated some of the risks taken in mortgage lending, where much more money is at stake in any given transaction. In that

---

[9] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1659 (1999).
[10] Ross Anderson, *Why Information Security is Hard – An Economic Perspective,* CAMBRIDGE COMPUTER LABORATORY 1 (2001), *available at* http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf.
[11] *Id*. at 7.

context, the so called "NINJA" loan arose (No Income, No Job or Assets).[12] It would follow that similar low or no documentation practices would exist in the credit card market.

The consequences of granting credit to impostors is shared with victims and merchants. Victims pay directly and indirectly (through lost time) to remedy new account fraud. Part IV considers approaches to addressing the externalities of the crime. Most public policy interventions seek to address particular risky practices, such as the use of the SSN for authentication purposes. These approaches, including the "Red Flag Rules," create prescriptive rules requiring credit grantors to apply anti-fraud efforts when indications of fraud are present. The benefits and limitations of that approach are discussed, along with approaching identity theft through negligence and strict liability.

I conclude by arguing that strict liability is appropriate, because credit grantors are fully in control of the identity theft problem. Short of freezing one's credit, there is no option enabling consumers to leave the instant credit marketplace. Individuals cannot insure against the risk of identity theft, and exercising care with personal information has no practical effect because credit grantors accept even fabricated data on credit applications. Strict liability would establish a direct financial cost for poor authentication procedures, compensate victims more fairly than the current system, and fuel innovation in new account fraud detection. Additionally, this approach will more directly address the market failure at the heart of the problem: credit grantors that adopt more aggressive anti-fraud efforts will lose sales to less circumspect companies. The current landscape has created a kind of race to the bottom -- where competitors attempt to grant credit as quickly as possible. Proper incentives would introduce some braking where appropriate and create an atmosphere where more careful decisions are rewarded more richly.

# II. THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT ("FACTA") ACCESS STUDY

## A. BACKGROUND AND METHODS

This article concerns "new account fraud," where an impostor opens lines of credit using personal information of another. This is different from "account takeovers," where an impostor commandeers an existing account belonging to the victim. In surveying Americans, the FTC estimated that in 2005, between 1.2 and 2.8 million Americans had been a victim of new account identity theft in the previous year.[13]

Identity theft interventions have primarily focused upon increasing penalties for impostors[14] and on educating consumers. Until recently, credit grantors, the businesses that ultimately decide whether or not to open a new account for an applicant, have largely escaped the regulatory spotlight.

---

[12] Jack Rosenthal, A Sub Subprime Glossary For the Mortgage Scandal, N.Y. TIMES, Aug. 8, 2008, *available at* http://www.nytimes.com/2008/08/17/opinion/17iht-edsafire.1.15360694.html.
[13] FTC, 2006 IDENTITY THEFT SURVEY REPORT (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.
[14] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, (1998).

Good authentication practices among credit grantors are critical to preventing new account identity theft, but the literature points to many examples where impostors used false or erroneous information and were still authenticated as the victim by the business.[15] Credit cards have even been issued to dogs,[16] to children,[17] to fake people,[18] and in response to torn-up credit applications.[19]

The FACTA[20] provides a unique opportunity to examine business authentication practices. That law empowers victims of identity theft to obtain business records associated with the crime from the company that created an account for the impostor in the victim's name. That is, the victim can obtain records, such as the credit application that the impostor submitted to the company and billing statements generated by the fraud. Obtaining these business records serves several functions: it helps victims prove that they did not open the account, it helps victims determine who opened the account, and it causes companies to reevaluate these records when allegations of fraud arise. Prior to the passage of FACTA, this information was only available in the rare circumstance when a victim brought suit against a company for causing or contributing to identity theft.

Advertisements were placed on Craigslist.org offering gift cards for the participation of new account identity theft victims in the San Francisco Bay Area. The protocol called for making FACTA access requests on these victims' behalf to obtain the applications for credit made by impostors. Once obtained, the victims would review these applications for accuracy, and the methods of business authentication could be documented.

A large number of individuals responded to the Craigslist.org advertisements, but many challenges were encountered in securing the participation of qualifying victims. Upon learning the process, two responded that the experience of becoming a victim was upsetting, and they feared reopening the subject. Others were victims of credit card fraud, a form of account takeover identity theft that did not qualify for this study. A number called with dubious tales of fraud, in transparent attempts to get a gift card.

---

[15] *See, e.g.,* Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007) (permitting negligence claim against defendant bank to continue under Tennessee law where a fraudulent credit application was accepted despite having a false address, phone number, and mother's maiden name).

[16] *See, e.g., Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC SAN DIEGO, Jan. 28, 2004.

[17] Brigitte Yuille*, Stolen innocence: Child Identity Theft*, Bankrate.com, Jan. 3, 2007, http://www.bankrate.com/nltrack/news/debt/20070103_child_identity_theft_a1.asp.

[18] It is possible to manufacture "synthetic" identities using real SSNs and fake names in order to obtain credit; suggesting that some institutions do not even match SSNs to the applicant's name. Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 HARV. J. L. & TECH. 97, 101 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech097.pdf.

[19] *See, e.g.,* Bob Sullivan, Even Torn-up Credit Card Applications Aren't Safe, MSNBC, Mar. 14, 2006, *available at* http://redtape.msnbc.com/2006/03/what_if_a_despe.html; Identity Thieves Feed on Credit Firms' Lax Practices, USA TODAY, Sept. 12, 2003, at 11A; Kevin Hoffman, Lerner's Legacy: MBNA's Customers Wouldn't Write Such Flattering Obituaries, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, A Week in Bankruptcy Court, ST. PETERSBURG TIMES, Mar. 18, 2002, at 8E. A specific red flag rule addresses the problem of when "[a]n application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled." Identity Theft Rules, 16 C.F.R. § 681, supp. A to app. A (2009).

[20] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

Having failed to recruit victims through months of general solicitations, an identity theft remediation company, ID Watchdog, [21] was approached. ID Watchdog located five victims of new account theft who had undergone the FACTA access process. ID Watchdog, through an identity theft remediation service, regularly makes FACTA requests to identify impostors and to bolster claims that the victim did not commit the fraud. A sixth victim was recruited independently and performed the FACTA access process.

The materials obtained through the FACTA process were carefully reviewed and victims were interviewed. This process shed some light on the application phase of credit granting, and through this lens, one could see the personal information provided by impostors when obtaining credit in others' names.

Among the victims recruited from ID Watchdog, the requests for FACTA documents were abandoned if a creditor released a victim from the fraudulent obligation. Thus, many of the ID Watchdog victims (X1-X5) had other accounts opened in their name, but the application and materials from these other incidents of identity theft are not available. This obviously presents some bias. It could be that the creditors that released victims from obligations had application materials and other analyses that made it absolutely clear that fraud was present. In such cases, providing the FACTA documentation may expose the credit grantor to suit for negligence in enabling identity fraud.[22] Creditors may also be performing a risk-benefit analysis, where complying with the FACTA access provisions is more costly than simply releasing the victim from the obligation.

There is also bias presented from using the ID Watchdog victims. These are individuals who had identity theft incidents that they sought professional help to remedy. One could conclude that that therefore, the ID Watchdog victims must have experienced more severe forms of fraud. Subjects X1, X4, and X5 did experience significant fraud events, but X2 and X3 had more straightforward cases, consistent with that of X6.

Because of the small sample of victims, and because each victim's experience with fraud was different, an overview of each fraud incident is summarized below.

## 1. THE STUDY PARTICIPANTS

X1 is a victim of multiple incidents of medical identity theft and of criminal identity theft. X1's file contains five intake forms from medical institutions or medical services companies and one from a state jail from 2002-2006. X1's impostor was arrested by police and severed jail time at a state department of corrections using X1's identity; in a separate instance, the impostor's conduct resulted in an open warrant for X1's arrest in a different state. X1's credit report showed 26 fraudulent obligations, and had a credit score of 665 before remedying the fraud. X1 learned of the theft through pre-employment background screening. The impostor had obtained an official out-of-state drivers license with X1's name, SSN and date of birth.

---

[21] ID Watchdog is a for-profit company offering identity theft consultation and monitoring services. *See* ID Watchdog, http://www.idwatchdog.com (last visited March 10, 2010).

[22] Wolfe v. MBNA Am. Bank, 485 F. Supp. 2d 874 (W.D. Tenn. 2007).

X2 is a victim of financial identity theft. The impostor obtained a $400 loan in X2's name, at 126% APR in 2000. The credit grantor claimed to have verified both addresses provided by the impostor, but X2 never worked or lived at either address. X2's credit report showed four other fraudulent obligations, and had a credit score of 530 before remedying the fraud. All four of these other obligations were for private-label credit cards. X2's impostor had a state-issued identification card in X2's name, and many physical differences separated X2 and the impostor. There is over 100 pound difference in weight, a significant difference in height, different eye color, and the impostor is a different race than X2.

X3 is a victim of financial identity theft. X3 had a credit score of 634 before remedying the fraud, which occurred in 1999.

X4 is a victim of financial, medical, and criminal identity theft. X4's file contains one credit application, an intake form from a medical institution, and an intake form from a state criminal court. X4 is a member of the armed services who lost his wallet in 1999, and did not notice subsequent frauds until 2004, when he received a letter from a collections agency. X4's credit report showed 20 fraudulent obligations, and had a credit score of 662 before remedying the fraud. Other medical institutions were billing X4 over $20,000 for unpaid hospital stays by the impostor. Additionally, the impostor was arrested for committing serious crimes while using X4's identity, accrued traffic tickets, and was in an automobile accident resulting in a civil lawsuit against X4.

X5 is a victim of financial identity theft. X5's file contains four fraudulent successful mortgage applications for well over $1,000,000 in loans, all obtained in 2005. Two other mortgages were successfully acquired by the impostor, but those applications are not available. The impostor's early mortgage loans polluted X5's consumer report; thus while the Consumer Reporting Agencies properly flagged three mortgage loan applications as suspicious, the fourth was not because false information from the earlier loans was incorporated into X5's consumer report. The impostor had a drivers license in X5's name. X5 reports that upon learning that mortgage loans were fraudulent, the holder of the loan would sell the obligation to another company. This resulted in collections agencies pursing X5 three years after the loans were approved. X5 claims that remedying the fraud took over 1,000 hours, but when the impostor was ultimately arrested, X5 could not collect restitution, because X5 did not suffer direct financial loss.

X6 is a victim of financial identity theft. The impostor obtained a private-label credit card in X6's name in 2007. The private-label issuer appears to have only collected a name, signature, and SSN in granting the card. The paper application used does not solicit address, date of birth, or other information. A separate sales authorization slip obtained contains X6's correct SSN.


**Figure 1: In an application used to obtain a private-label credit card in X6's name, the impostor misspelled X6's name (should be Grimmelmann, but appears to be Grimmelan), had a forged signature, and omitted basic metadata. Provided with permission by X6, who has publicly revealed his participation in the study.**

## B. RESULTS

A common pattern of errors emerges from a comparison of the 6 victims. The table below compares the 6 victims, and notes the number of incidences that incorrect information was used by the impostor over the number of applications in the victim's file.

**Table 1: Overview of the Most Common Errors on Applications and Other Impostor Materials**

| Victim Number | Wrong* Address | Wrong Phone | Wrong DOB | Wrong SSN | Wrong DLN | Misspelled Name | Red Flags |
|---|---|---|---|---|---|---|---|
| X1 (6 applications) | 4 | 2 | 1 | | | | |
| X2 (1 application) | 2 | 1 | | | | | |
| X3 (1 application) | 1 | | | | | | |
| X4 (3 applications) | 2 | | | 1 | | | |
| X5 (4 applications) | 3 | | 3 | | 1 | | 3 |
| X6 (1 application) | | | | | | 1 | |

*In this context, "wrong" means an address or phone number never belonging to the victim.

For instance, in X1's case, there were 4 incidents were a wrong address was used, 2 with a wrong phone number, and 1 with an incorrect date of birth. More than one error can occur for each application.

**Table 2: Breakdown of Correct and Incorrect Identifiers by Application Type**

| Victim | Application Type | Correct | Incorrect | Other |
|---|---|---|---|---|
| X1 | Medical | Name, sex | Address, DOB, Employer | SSN left blank |
| | Medical | Name, DOB, Sex | | |
| | Medical | Name, DOB, SSN | Address | Phone, Place of Birth left blank |
| | Medical | Name, DOB, Sex | Address, Phone | |
| | Medical | Name, DOB | Address, Phone | |
| | Jail Intake Form | Name, SSN, Sex, Race | Height and weight somewhat inconsistent with victim | |
| X2 | Short-term loan | Name, SSN, DOB | Work and home addresses, phone. | |
| X3 | Credit Card | Name, DOB | Address | |
| X4 | Credit Card | Name, DOB, SSN | Address, Employer | |
| | Medical | Name | Address | |
| | Court Information Sheet | Name, DOB, Sex, Height | SSN, significant weight difference, Race | |
| X5 | Mortgage | Name, SSN | Drivers license number fake, Address, DOB, Race, Employer, Nearest Relative | 3 CRAs red flag on address discrepancy |
| | Mortgage | Name, SSN | Drivers license number, Address, DOB, Employer | 3 CRAs red flag address discrepancy |
| | Mortgage | Name, SSN | Address, DOB, Employer | 3 CRAs red flag address discrepancy; 1 CRA reports DOB error; appears to be low-documentation loan |
| | Mortgage | Name, SSN | Address, DOB, Employer | Red flags no longer raised because previous mortgages polluted report |
| X6 | Credit Card | SSN | Name misspelled | No addresses or other information collected by application |

These errors cannot be described as minor, transcription errors (e.g., when a single digit is transposed or the like).

### 1. WRONG ADDRESSES

The most common form of error on applications submitted by impostors is an incorrect addresses. Of the 6 fraudulent applications concerning X1, the impostor provided an address never belonging to X1 on 4 of them. X2's single fraudulent application had 2 addresses never belonging to X2; the creditor claimed to have verified both. X3's single fraudulent application had an address never belonging to X3. Of the 3 fraudulent applications concerning X4, 2 had addresses never belonging to X4. Of the 4 fraudulent mortgage applications concerning X5, 3 used addresses never belonging to X5. The fourth mortgage application in X5's name did not belong to her either, but the previous mortgaged polluted her consumer report with false addresses. Thus the fourth mortgage lender may not have detected an address discrepancy at all. X6's application did not solicit an address.

Address Verification Service (AVS) is popularly used in the electronic transaction context to ensure that goods ordered are delivered to the billing address. Merchant acquirers will impose higher liability on businesses that are willing to ship merchandise to a non-billing address, thus, many businesses will not accept unverified addresses. This inexpensive means of verification was either not used or ignored in these cases.

### 2. WRONG PHONE NUMBERS

Of the 6 fraudulent applications concerning X1, the impostor provided a phone number never belonging to X1 on 2 of them. X2's single fraudulent application had a fake phone number. As with addresses, imperfect, but inexpensive phone verification services are commonly available, but apparently not used or ignored in these cases.

### 3. INCORRECT DATES OF BIRTH

Of the 6 fraudulent applications concerning X1, the impostor provided an incorrect DOB on 1 of them. Of the 4 fraudulent mortgage applications concerning X5, the impostor provided an incorrect DOB on 3 of them.

X5's impostor smartly used a DOB in the same month and year of X5's real DOB. Because the issuance of SSNs is often linked to the month in which an individual is born, the impostor's technique successfully fooled a "SSN Validation" tool.[23] Nevertheless, commercially-available tools (most notably, the consumer report) are available to validate SSNs to the applicant's name, but they were either not used or ignored here.

### 4. INCORRECT SOCIAL SECURITY NUMBER

X4's court intake sheet for serious crimes committed by the impostor lists a SSN that does not belong to X4.

---

[23] There is no standard for "validation" of SSNs. Some SSN validation services only match the number to date of birth and do not have the capability of matching to name. This means that impostors can fabricate identities with SSNs that match a certain birth month. *See*, Hoofnagle, *supra* note 18, at 116 (describing "synthetic" identities).

Numerous companies and the federal government itself offer SSN validation tools to check the internal consistency of the number; many also match name to SSN.

### 5. WRONG DRIVERS LICENSE NUMBER

The impostor who acquired mortgages using X5's personal information had a drivers license with X5's name, but a fake drivers license number. This drivers license number had never been issued by the state.

This drivers license number could have been identified as fraudulent using a number of validation tools.

### 6. VICTIM'S NAME MISSPELLED

The application for a private-label card in X6's name was notable for its sloppiness. The impostor scrawled X6's name, misspelling it in two different ways on the application. The credit issuer only required name and signature on the application, but may have requested a SSN orally. The application is undated and does not identify the specific store where the impostor applied. In a receipt accompanying the application, X6's correct SSN is listed, but X6's name is misspelled, but in a different way than the impostor listed it on the application.

It is difficult to visualize this case without illustration, but such a description would breach confidentiality. Imagine instead that an impostor stole the author's identity, must misspelled "Hoofnagle" as "Hoofnle" on the application. Processing the application, the store improves the misspelling to "Hoofnagl." That is the level of error that occurred here.

### 7. RED FLAGS RAISED

Sections 114 and 315 of the FACTA[24] required federal agencies to promulgate regulations "requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing . . . [identity theft guidelines] . . . to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers . . . ."[25] A "red flag" is a "pattern, practice, or specific activity that indicates the possible existence of identity theft."[26] In a supplement to the appendix to the Rule, the agencies identify 26 red flags. They include, warnings that the creditor grantor receives from a consumer reporting agency, the presence of suspicious documents, the provision of suspicious personal identifying information, suspicious account activity, and notice from individuals that fraud is afoot.[27]

Once detected, the rules require "appropriate responses" to the red flags "commensurate with the degree of risk posed."[28] Suggested responses include account

---

[24] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).
[25] 15 U.S.C. § 1681m(e)(1)(B) (2009).
[26] Identity Theft Rules, 16 C.F.R. § 681.1(b)(9) (2009).
[27] Identity Theft Rules, 16 C.F.R. § 681, app. A (2009).
[28] *Id.*

monitoring, contacting the customer, or not opening a new account in response to an application.[29]

Automated fraud detection systems at the consumer reporting agencies indicated that fraud could be present in 3 of the 4 mortgage applications in X5's file. One warned, "Substantial difference between address submitted in credit request and addresses in credit file." Two of these red flag warnings indicated that the applicant/impostor's DOB did not match X5's. It is unclear what steps the creditor grantor took to resolve these red flags before extending mortgages to the impostor.

## 8. OTHER OBSERVATIONS

### a) Poor Authentication in the Health Care Setting

Health care providers must balance the conflicting interests of verifying the identities of patients with providing a welcome environment to all who need care. Obviously, in many situations, it may be impossible to obtain reliable identification information from a patient. This in part has contributed to the problem of medical identity theft,[30] which carries with it both the frustrations of financial identity theft and the risk that one's medical file could be polluted with data pertaining to the impostor.

Six applications were from health care providers. In five of these applications, providers gave incorrect information.

### b) Significant Physical Differences Between Impostors and Victims

In two cases, impostors were a different race than their victims, but despite in-person interactions with the credit grantor, this disparity was apparently overlooked. Other significant physical differences were overlooked. X2, a Latino, is over 6 feet tall, and over 100 pounds heavier than the impostor, a significantly shorter African American. Similarly, X5 is white but the impostor is African American. X4's impostor weighed 250 pounds, but successfully masqueraded as X4 using X4's drivers license when arrested, despite outweighing X4 by 70 pounds.

### c) Fraud is Often Apparent within the "Four Corners" of the Consumer Report

Several of the ID Watchdog victims' consumer reports had obvious "intratexual" indicia of identity theft. That is, by simply analyzing the consumer report, with no extrinsic information, it should have been obvious that the fraud was present.

Several of the ID Watchdog victims had years of perfect payment history, but towards the end of their reports, one found numerous collections accounts. For instance, a summary of X4's credit score reads, "You paid 100% of your accounts on time." However, towards the end of X4's report, a reviewer would have found 20 unpaid obligations. These items that had been turned over to collections agencies indicated that X4 had never made any payment on these obligations. Similarly, X1 had a perfect payment history for legitimate accounts, but 26 delinquent, fraudulent tradelines.

---

[29] *Id.*

[30] *See generally,* Pam Dixon, World Privacy Forum, The Medical Identity Theft Information Page, http://www.worldprivacyforum.org/medicalidentitytheft.html (last visited Mar. 10, 2010).

Why would X1 and X4 faithfully pay account balances for years, and not make a single payment on others? This dichotomy between responsible and completely derelict payment could be an intratextual indication of identity theft. A study should be conducted to determine if fraud could be detected merely by reviewing consumer reports without any knowledge of the consumer or her credit activities. If this detection is possible, consumers could be automatically altered to suspicious activity on their consumer reports by consumer reporting agencies.

**d) Marginal Financial Services**

Subprime lending is present in many financial applications reviewed in this study. For instance, X5 had a good credit rating prior to becoming a victim of identity theft. The impostor applied for home loans with the following interest rates: 9.3%, 6.4%, 9.5%, and 10.5%. X2's impostor applied for a $400 loan at 126% APR.

This points to another avenue for further research: should subprime lenders suspect fraud when consumers with excellent credit apply for their products? Should that fact pattern constitute a "red flag," and if so, will subprime lenders have adequate incentives to properly vet the application if they are remunerated by fees rather than the lifetime profit from the loan?

# III. EFFICIENT IDENTITY THEFT

Recall that two paradigms have dominated the legal understanding of the identity theft problem. Lynn LoPucki frames it as a result of the modern, more private life: a decline of living in public has facilitated both the concealment of impostors and their ability to masquerade as others.[31] Daniel Solove, following a liberal privacy-control framework, argues that identity theft is a result of a broken privacy architecture, one where no one is in control of personal information. Thus, identity theft is a byproduct of a broken privacy architecture.

Much has been learned since LoPucki's first works in this field, and the factual landscape of identity theft is richer. The landscape and recent developments place strains on the LoPucki conception of the problem. For instance, LoPucki laments the decline of public life at the dawn of blogging and social networking services, on which millions of Americans are posting personal details never published in a phonebook or city directory. We seem to be entering a new era of personal revelation and disclosure about others, thus changing notions of interpersonal privacy.

But even if one accepts the idea that public identity is in decline, credit grantors do not use the sources LoPucki cites (city registers, phonebooks, and the like) for credit authentication. While privacy laws were enacted in the 1990s, credit grantors amassed databases and anti-fraud tools far richer than any phonebook or DMV database. Data brokers developed tools to aggregate a complete history of individuals' addresses, phone numbers, and other personal information.[32] Credit grantors can buy proprietary tools to help verify identity and rely upon internal databases to go beyond simply matching

---

[31] *See* LoPucki, *Privacy, supra* note 2, at 1278.

[32] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (2004).

application information to the credit header. In fact, never in history have so many anti-fraud tools been available to credit grantors. Thus, the LoPucki narrative describing the decline of public life misses the mark because Americans' lives are very much public to companies involved in the credit markets.

Solove frames the problem as a lack of control over personal information. No one seems to be in control, and if collection of personal information involved limits on its use and dissemination, thieves would be less likely to commandeer others' credit. LoPucki critiques the Solove approach as impractical, since there is no reliable way to selectively prevent revelation of personal information to identity thieves.[33] But the findings of the FACTA Access study suggest that, in a way, privacy-control is the root of the problem. The cases reviewed in this study show that credit grantors are willing to accept even inaccurate information on applications. This article expands the Solove critique by identifying control over credit authentication as a prime remedy to identity theft.

### A. INCENTIVES FOR QUICK CREDIT GRANTING

An extensive economic literature addresses the problem of credit risk,[34] the chance that a borrower will not pay back an obligation. However, fraud risk,[35] the chance that an impostor will open a new account, is an underexamined problem in the economic literature. Also underexamined is the complex set of incentives in the new account credit market that can be leveraged by impostors to commit identity theft.

Credit granting companies have many compelling incentives to quickly open new accounts, and in light of this, some fully automate the process. These incentives create great rewards for the granting company, and significant opportunity costs if the delay in investigating the applicant causes the customer to go elsewhere. An effective anti-identity-theft approach would consider the incentives embedded in the credit granting markets. These incentives drive credit grantors to make decisions quickly and forgo some basic identity theft prevention strategies.

Anti-fraud efforts cost money and are subject to diminishing returns, and thus credit grantors will not try to completely eliminate identity theft.[36] Even basic efforts, such as requiring an in-person interaction as recommended by LoPucki and Solove, may be very expensive in comparison to a fully-automated credit granting procedure. Writing in the UK market, Steven Finlay estimates that a mail, phone or internet application (no face-to-face interaction) costs £5-£15 to administer.[37] In store applications could cost

---

[33] *See* LoPucki, *Privacy, supra* note 2, at 1278.
[34] *See, e.g.,* Charles M. Kahn & William Roberds, *Credit and Identity Theft*, 55 J. MONETARY ECON. 251 (2008).
[35] Kahn & Roberds define fraud risk as "the risk that a debt cannot be enforced because the identity of the person incurring the debt cannot be ascertained." *Id.* at 252. Of course, with enough resources, the actual debtor's identity can be determined. Many credit grantors will not investigate impostors because of the cost involved, unless a very large fraud occurred. Thus, a better definition for fraud risk would follow standard definitions of identity theft, such as the Federal Trade Commission's, which focus upon use of another's information without authorization for some illegal purpose. 16 C.F.R. § 603.2(a) (2007).
[36] Keith B. Anderson, Erik Durbin & Michael A. Salinger, *Identity Theft*, 22 J. ECON. PERSP. 171, 182 (2008).
[37] STEVEN FINLAY, CONSUMER CREDIT FUNDAMENTALS 74 (2005).

between £20-£50.[38] Obviously, once development costs are recouped, a fully automated approval process would generate lower costs than those requiring consultation with the fraud department or manual inspection.

Decisions about anti-fraud interventions must be balanced against risk. With respect to identity theft, the overall probability of fraud is quite low. The FTC estimated that in 2005, between 1.2 and 2.8 million Americans had been a victim of new account identity theft in the previous year.[39] The total number of credit applications in the US in any given year is unknown, but could easily be in the hundreds of millions. For instance, Bank of America alone processes 14 million applications a year through automated processes.[40]

Incentive conflicts may be baked into some credit marketing arrangements. Due diligence incentives may be reduced in relationships where an issuer uses some third party, such as a telemarketer, to acquire new customers. Consider the example of the student group that receives a fee for each credit card applicant they enroll on campus. The student group is fee remunerated; if the applicant never actually uses the card or is an impostor, the student group may still profit from the transaction.

Incentives peculiar to credit granting may also cause grantors to take on more risk. For instance, the "best customer" from the credit grantor perspective could be the consumer who will charge so much that they cannot afford to pay off the balance in full in any given month. These so called "credit revolvers" are the most profitable consumers because they pay compounded interest rates on their purchases and fees.[41] However, the worst customer is very similar to the best, as a fine line divides those who charge too much and can pay the minimum balance, and those who make no payments at all. The search for revolvers provides a rational basis to seek riskier applicants who may have thinner or wemmed credit histories.

Once accounts are opened, credit grantors have found ways to mitigate the cost of fraud. I suggest that five factors create incentives to prioritize quick credit granting over stronger initial anti-fraud due diligence. These incentives are so strong that grantors have chosen to address fraud primarily through mitigating losses after credit has been extended.

First, consumers want goods and services quickly, and there are opportunity costs associated with the delays inherent in investigations of credit applications. Incentives for due diligence may be outweighed by consumer preferences and competitors with lax practices. Thus, if Bank A delays the approval of a new credit card in order to investigate

---

[38] *Id.*

[39] FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 1 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[40] In a December 2007 workshop on SSNs held by the FTC, Trey French of Bank of America stated that the bank approved about 14 million credit applications a year mostly through a completely automated process, meaning that the institution had no human review of this account granting. FED. TRADE COMM'N, REMARKS AT SECURITY IN NUMBERS, SSNS AND ID THEFT 1, 82 (2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/DECEMBER11.pdf.

[41] *The Secret History of the Credit Card,* PBS FRONTLINE, Nov. 23, 2004, http://www.pbs.org/wgbh/pages/frontline/shows/credit/etc/synopsis.html.

a potential fraud risk, the consumer may move along to Bank B. Often the granting of a card is paired with an immediate discount for purchases of goods. A rejected application could mean a lost sale. Credit cards, in particular, are competing with other forms of credit that take a longer time to acquire. If credit cards fail to provide instant gratification, consumers may be more willing to obtain more advantageous bank loans.

Second, awards accrue to issuers that can recruit many customers. Despite the competitiveness of credit offers, many consumers stick with the same card even when more attractive offers exist. For instance, "affinity cards" encourage lock-in to a specific card in order to give flight benefits or donations to the customer's college. This gives the credit card company "wallet space" that might be later expanded into other product offerings.

Third, while consumers directly experience fees (along with late fees, penalties, cash withdrawal fees, payment protection insurance, etc) and interest charges, other merchant fees accrue to card issuing banks. The bulk of the lucrative "interchange fee," which generates $40-50 billion in income annually mostly accrues to issuing banks.[42] In a typical $100 sale, the card-issuing bank would receive $1.80 of the $2.25 fee paid by the merchant in the sale.[43] Thus, each card issued has the potential to capture a small percentage of revenue from each sale, giving banks strong incentives to capture the largest number of consumers possible.

Fourth, electronic payment increases "spend," meaning that consumers, divorced from the experience of parting with cash, are generally willing to spend more money on credit. Converting consumers from cash to credit results in more revenue in real dollars, but also fees from each sale.

Once an account is opened, credit issuers have found many ways to mitigate financial risks from identity theft. For instance, in some cases, liability for fraudulent charges is imposed upon merchants. A recent report by LexisNexis finds that merchants absorb $100B in losses annually because of identity theft, while financial institutions lose about $11B.[44] Consumers have been known to pay fraudulent charges in order to clear their credit report. LexisNexis estimates that consumers absorb almost $5B annually. Credit issuers can securitize credit card debts, and thus spread the risk of fraud among different investment vehicles, depending on investors' appetite for risk.[45] Finally, fraud losses are written off as business losses, and thus can offset tax burdens.

Credit issuance can be extremely lucrative, and because of customer biases and behavior, a successful issuer will attempt to obtain as many new accounts as possible. Risk of fraud can be mitigated, while risk of losing business to faster acting competitors cannot.

---

[42] Andrew Martin, *Card Fees Pit Retailers Against Banks*, N.Y. TIMES, July 16, 2009, at B1.
[43] *Id*.
[44] JAVELIN STRATEGY & RESEARCH, LEXISNEXIS, TRUE COST OF FRAUD STUDY 1, 14-23 (2009), *available at* http://risk.lexisnexis.com/literature/LexisNexisTotalCostFraud_09.pdf.
[45] Kathy Chu & Byron Acohido, *Why Banks are Boosting Credit Card Interest Rates and Fees*, USA TODAY, Nov. 14, 2008, *available at* http://www.usatoday.com/money/industries/banking/2008-11-09-bank-credit-card-interest-rates_N.htm?loc=interstitialskip.

Recall that LoPucki links the rise of identity theft to the perception that we live more private lives. Contrary to LoPucki's observations, credit grantors have more personal information today than ever, but this study shows that when impostors make errors in applying for credit, grantors override or ignore those errors. Thus, this is not a problem of public or private lives or the availability of information, it is a problem of business decisions to prioritize new account generation over due diligence.

In light of the FACTA Access Study results and of the incentives in credit granting, the advance of automated credit granting systems provides a better explanation for the identity theft problem. The "miracle of instant credit," the ability of anyone almost anywhere to apply for and obtain a new account in seconds, has a dark underbelly -- the miracle of instant identity theft. It allows impostors to be instantly rewarded for their crimes, with little risk of arrest or prosecution. Its rise in the 1990s offers a far more compelling explanation of the modern identity theft problem.

# IV. INTERNALIZING THE EXTERNALITIES

This section reviews the interventions proposed by LoPucki and Solove. Then, two alternative regulatory approaches are discussed: the newly promulgated Red Flag Rule and a proposal to fix the underlying incentives driving the problem.

## A. WHAT WOULD LOPUCKI & SOLOVE DO?

Despite their different paradigms, LoPucki and Solove agree on several identity theft interventions. Both agree that the SSN should not be used as an authenticator.[46] This means that credit grantors should not use knowledge of the SSN as proof of identity. Both agree that new credit applications should require an in-person interaction.[47] Both agree that consumers should be notified proactively of credit activity.[48]

At that point, the two diverge. LoPucki articulates a voluntary system where individuals can claim their identities, mediated through a trusted government agency, such as the department of motor vehicles.[49] Once one's identity is claimed, the individual could be more involved in the credit authentication process.

These interventions may reduce the incidence of identity theft, but they largely miss the incentives that are driving the identity theft problem. LoPucki and Solove attempt to address specific vectors that enable the crime, such as use of the SSN as an authenticator, and to harden the institutions currently used to commit the crime. But even if grantors are prohibited to use the SSN as an authenticator, the results of the FACTA Access study suggests that the incentive structure may still drive risky credit granting.

In-person credit application mandates suffer from several different problems. First, such an approach would create a great burden for both consumers and merchants. Internet credit transactions, and newly emerging instant credit products would likely not be profitable if costly personal visits were required.

---

[46] LoPucki, *Privacy, supra* note 2, at 1279; Solove, *supra* note 7, at 1270.
[47] LoPucki, *Privacy, supra* note 2, at 1279.
[48] *Id.*
[49] *See generally* LoPucki, *Human Identification Theory, supra* note 2.

More importantly, in-person interactions may not be very effective in reducing fraud. Such a mandate assumes that cashiers and store employees will be able to recognize impostors as such. These employees will have to be trained to look for data mismatches between what is presented on the application and on credit headers, to recognize fake credentials, and even to determine when someone is posing as another using a real credential. Generally speaking, many people are not proficient at these tasks. As any college student can attest, using a friend's drivers license to gain entry to a bar is usually as simple as having the same hair color.

The results of the FACTA Access study also suggest that in-person meetings would not have been very effective in reducing fraud. Impostors were authenticated as the victim in cases where significant physical differences were present, and even where the impostor and victim were different races. Furthermore, several impostors had either fabricated or real state-issued identity cards.

Proactive notice of credit activity would not prevent identity theft, but it would reduce the impact of the crime. Several studies have shown that early detection of fraud reduces harm to victims. Still, such a requirement would result in the dispatch of hundreds of millions of notices annually in cases where no fraud was present, in order to make individuals aware of 2-3 million actual cases of fraud.

## B. THE RED FLAG RULES APPROACH

Anecdotally, the problem of sloppy credit granting has been well documented. The FACTA Access study is the first to empirically demonstrate a problem, albeit, with a small sample of six victims of new account identity theft. As explained above, Congress included the Red Flags Rule mandate in the passage of FACTA in 2003. This mandate reflected a need to require better practices in the authentication process.

It would seem that the Red Flag approach would be effective in addressing the problems found in the FACTA Access study. Among 16 fraudulent applications presented by impostors to obtain credit from 1999-2007, one finds that credit grantors have extended new accounts despite the presence of basic contact information errors on the applications. This credit granting behavior fits squarely within the sample red flags specified by federal agencies. For instance, the regulations specify that a notice of an address discrepancy provided by a consumer reporting agency qualifies as a red flag. Three of X5's mortgage applications included address discrepancy notices, but the mortgages were extended anyway. Similarly, the regulations specify that when an applicant presents an address not currently in the consumer's report, a red flag is raised.

The Red Flag Rules also speak to physical differences between the applicant and the victim. Two cases concerned victims who were of a different race than their impostor. Outside the credit granting context, two cases involved significant weight differences between impostor and victim.

But will the Red Flag Rules be effective in practice? The mandate follows a very extended period of rulemaking--the Red Flag Rules were not issued until October 2007,[50]

[50] FED. TRADE COMM'N, AGENCIES ISSUE FINAL RULES ON IDENTITY THEFT RED FLAGS AND NOTICES OF ADDRESS DISCREPANCY (Oct. 31, 2007), *available at* http://ftc.gov/opa/2007/10/redflag.shtm.

and covered entities were given a full year to comply. However, once its effective date of November 2008 arrived, an extension was granted for compliance.[51] Credit grantors received the Rules with a collective groan. It became clear that by the November 2008 implementation date, there would be widespread non-compliance, both because of confusion over the Rules, but also because of a lack of alacrity among banks to implement them.

Credit grantors are given very broad discretion to respond to red flags. They must simply make "appropriate responses" to the red flags "commensurate with the degree of risk posed."[52] Thus, there is a risk that credit grantors will spot red flags, and apply weak "appropriate responses" that still result in a new account issued. For instance, in X5's case, consumer reporting agencies alerted the grantor to significant information discrepancies, but new accounts were still issued.

More importantly, because of incentives to quickly grant credit, issuers are not likely to identify new red flags. Identifying new red flags could hurt their ability to obtain new customers, because different grantors can develop their own indicia of fraud. Grantors that decide not to implement many red flags will be able to open new accounts more quickly than those that diligently comply with the regulation.

The FTC and banking agencies responsible for the Red Flags Rule can identify indicia of fraud that all credit grantors must follow. However, operating from outside the industry, the agencies are unlikely to be on the vanguard of fraud trends. As it has been in the past, agencies will develop new red flags in response to anecdotal information, especially tales of sloppy credit granting exposed in the media. Without the insight that fraud analysts obtain from datamining and years of experience in detecting fraud, agency-developed red flags are likely to lag behind, and once proposed, subject to intense lobbying campaigns to prevent changes to the rule, and to delay their implementation.

Simply put, if ignoring red flags or complying with the minimum mandated care is more expensive than tolerating fraud (and thereby acquiring more customers than a competitor), its incidence will not be reduced. Identity theft will still be rampant, and victims will still be uncompensated for the externalities of the crime.

The Red Flags Rule shares the same core problem as the LoPucki and Solove approaches: it does not address the underlying thirst for customer acquisition that drives high risk tolerances. A more effective approach would put a thumb on the economic scale that would encourage the marketplace towards more responsible practices.

### C. NEGLIGENCE AND STRICT LIABILITY APPROACHES

How the law should address the identity theft externality is a complex problem. Credit is essential to our modern economy. Barriers to access can stall the economy and darken the financial futures of all. At the same time, public policy norms that prioritize quick access to credit -- à la the "miracle of instant credit" evangelists -- have

---

[51] FED. TRADE COMM'N, FTC WILL GRANT SIX-MONTH DELAY OF ENFORCEMENT OF 'RED FLAGS' RULE REQUIRING CREDITORS AND FINANCIAL INSTITUTIONS TO HAVE IDENTITY THEFT PREVENTION PROGRAMS (Oct. 22, 2008), *available at* http://www.ftc.gov/opa/2008/10/redflags.shtm.

[52] Identity Theft Rules, 16 C.F.R. § 681, app. A (2009).

unintentionally encouraged a landscape ripe for fraud. Overreaction in the direction of restricting credit, or in encouraging its extension to anyone both are fraught with peril.

I argue that existing solutions to the identity theft problem have been too narrowly focused on particularly irresponsible practices among credit grantors. These approaches risk creating reification as credit grantors focus on complying with prescriptive rules. Further, highly regulated institutions operating in a compliance mindset are likely to follow the letter of the law rather than effectuate its purpose of reducing identity theft.

More attention is needed to the underlying incentives that drive sloppy credit granting. Identity theft is an externality that is the product of instant credit. And creditors control the instant credit valve. They can open it fully, or narrow it, by implementing greater controls. The FACTA Access Study shows that consumers cannot prevent this crime, because creditors are willing to accept even incorrect information in authenticating customers. The answer therefore is to align incentives, so that the costs currently accruing to millions of consumers fall back upon credit grantors.

Some commentators have suggested that credit granting institutions be subjected to suits in negligence for identity theft. Anecdotal evidence, and the participants in the FACTA Access Study suggest that credit grantors are overlooking disconfirming evidence in credit granting decisions. Sloppy procedures could be viewed as negligent behavior, with lawsuits for damages serving as an incentive to improve practices. Heather Howard has suggested this approach:[53]

> When financial institutions act negligently, they jeopardize the financial well-being of the individuals whose information they manage. Because a quasi-relationship arises between a financial institution and an individual in whose identity it opens an account, the institution should be responsible in tort for the consequences of its negligent actions or failures.[54]

Howard acknowledges that the traditional tort requirements of showing duty, breach, causation, and damages will be challenging for plaintiff/victims of identity theft. In the new account identity theft context, duty has proven to be the highest hurdle for litigants pursuing negligence theories. Credit issuers argue that they have no legal duties to non-customers, and that in any case, they should not be liable for the criminal actions of third party impostors.[55]

Credit issuers have had some success with these arguments. In a survey of negligence cases, David Szwak observes:

> These cases illustrate that a plaintiff seeking to recover against a bank or credit issuer following an identity theft must carefully plead and prove facts to support a negligent enablement or similar claim. Obviously a pre-existing relationship and duty . . . is helpful to the plaintiff and may even

---

[53] Heather Howard, *The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim*, 54 DUKE L.J. 1263, 1283 (2005), *available at* https://www.law.duke.edu/shell/ cite.pl?54+Duke+L.+J.+1263.

[54] *Id*. at 1283.

[55] Huggins v. Citibank, N.A., 585 S.E.2d 275 (2003).

> be essential. . . . [M]ost courts do not recognize a general fiduciary duty to the public on the part of banks or other business enterprises. Thus a separate relationship and duty . . . or perhaps under the FCRA, appears to be a requisite for recovery in most identity theft cases.[56]

Brendan Delany suggests that this limitation could be surmounted, if courts were willing to assume that identity theft is a foreseeable risk of negligent issuance of credit cards:

> By employing "liability beyond the risk," courts can establish a legal duty for an issuer of credit cards to confirm applicants' identities. "Limitation of liability to the risk" [requiring the plaintiff to prove that identity theft was foreseeable] enables CRAs [consumer reporting agencies] and banks to disseminate personal information and issue credit cards without serious inquiry or proof that the consumer is in fact who he or she claims to be. Indeed, the Polzer court refused to hold the bank liable "even when they failed to take any steps whatsoever to confirm the applicant's identity and where they could have easily and inexpensively done so." "Liability beyond the risk" will impose a greater duty on CRAs and creditors to exercise greater care and thus significantly reduce the possibility of identity theft.[57]

Still, the negligence approach's other hurdles present challenges to plaintiffs. Writing in the context of database security, Danielle Citron considers and rejects a negligence approach for addressing leaks of personal information.[58] Citron's analysis of an analogous situation is useful here. Citron considers the duties of companies that hold massive databases against leakage, which can take the forms of both accidental spills, and the intentional acts of malicious hackers.[59] Clearly, databases of personal information have much social utility; just as credit granting has provided economic development and social mobility. Quick credit granting could not even be possible without the databases that Citron describes, yet, like access to credit, these databases must be carefully managed to prevent harm to many people.

Citron argues that a negligence approach fails from both economic and moral perspectives. Economically, a negligence regime could create inefficiency, because uncertainty would surround the optimal level of care to prevent leaks of personal information.[60] In the context of sloppy credit grant systems, this threat loom large. Credit grantors may overreact by requiring burdensome authentication measures. This could result in a slowdown in credit issuance, leading to missed opportunities.

---

[56] David Szwak, *Update on Identity Theft and Negligent Enablement*, 58 CONSUMER FIN. L.Q. REP. 66, 71 (2004).
[57] Brendan Delany, *Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Impostor Fraud*, 54 CATH. U. L. REV. 553, 586 (2005) (citations omitted).
[58] Danielle Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 261-68 (2007).
[59] *Id.* at 243-46.
[60] *Id.* at 263-64.

Individuals with "thin" credit files or limited identity credentials may shut out of the credit markets.

Uncertainty would also lead to "battles of the experts" on credit granting procedures. The FACTA Access Study provides examples of what appears to be negligent credit granting.[61] Consider the example of the situation where the impostor provided an address at which the victim never lived. Is it not sometimes reasonable to open an account to an individual at a new address? In this situation, even if the credit grantor uses a commercially available database s to verify the address, a new address may not appear in the database for some time. What verification would be effective in such a circumstance?

Citron further identifies management of "residual risk" as problematic.[62] A negligence regime would leave victims uncompensated where due care was exercised, but a data leak occurred nevertheless.[63] Similarly, in the identity theft context, credit grantors will argue that their anti-fraud systems were sufficient, and although credit was granted, that in itself does not demonstrate negligence.[64] Consumers thus will be uncompensated for the harms related to beneficial economic activity over which they can neither exercise control nor profit from.

After rejecting negligence as a basis for liability in addressing database security, Citron turns to strict liability, using the example of ultrahazardous activities.[65] Citron leverages the seminal case of *Rylands v. Fletcher*[66] as a model.[67] *Rylands* considered the duty of care to safeguard water reservoirs.[68] Water reservoirs are socially useful and necessary, but can cause extraordinary damage if breached, by accident, negligence, or intentional action. The *Rylands* court's extension of liability without fault for their breach, and the subsequent acceptance of this approach in the US, offers a model for managing risks of database leakage, according to Citron.[69]

Strict liability will provide more efficiency, because database providers have ultimate control over use of personal information and protections that are in place:

> Database operators constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database. Database operators have distinct informational advantages about the vulnerabilities in their computer networks. Individuals, by contrast, cannot detect and understand the security offered by information brokers, employers, colleges, or biometric vendors. . . . [and] the database operator sits in the

---

[61] *See supra* Part II.B (revealing that credit granters approve applications with false addresses, false phone numbers, incorrect dates of birth, false social security numbers, and the wrong drivers license number).
[62] Citron, *supra* note 58, at 264-67.
[63] *Id.*
[64] Beard v. Goodyear Tire & Rubber Co. 587 A.2d 195, 201 (D.C. App. Ct. 1991).
[65] Citron, *supra* note 58, at 268-77.
[66] Rylands v. Fletcher, 3 L.R.E. & I. App. 330 (1868).
[67] Citron, *supra* note 58, at 270-71.
[68] *Id.*
[69] *Id.* at 278-80.

> best position to make decisions about the costs and benefits of its information-gathering.[70]

The FACTA Access Study indicates that consumers have no control over the credit authentication process taking place between grantors and imposters.[71] Even if a consumer invests time and money in avoiding revelation of personal information, some credit grantors will issue new accounts to impostors with incorrect personal information. There is no way to opt out of the credit markets -- even toddlers' identities are stolen in the current situation. The cheapest cost avoider in the identity theft context, thus is the credit issuer. The relationship is so asymmetric that the individual is literally at the mercy of the risk preferences of companies with which no relationship has even been established.

Residual risks would be addressed by a strict liability regime. In a discussion directly relevant to poor authentication in identity theft, Citron continues to explain why insurance does not offer a remedy to consumers:

> Experts report that identity-theft insurance is not "worth the money" because it does not cover direct monetary losses incurred as a result of such theft. On the other hand, database operators can most efficiently spread the costs of data leaks by obtaining a single cyber-risk insurance policy as opposed to the countless identity-theft insurance policies obtained by individuals.[72]

Indeed, as recounted in section III above, credit issuers have a number of strategies to mitigate financial lost because of identity theft. However, consumers have no reasonable strategies to address the harms of the crime, whether or not the credit grantor was negligent.

Given that credit grantors are in control of the new account identity theft problem and that credit grantors can manage risks related to that control while consumers practically cannot, a strict liability approach may create a more efficient allocation of costs among credit grantors and victims of identity theft. Presumed damages could be awarded, keyed to the average time that consumers spend remedying the crime. Statistics on average time and related cost to consumers are closely tracked by the FTC and by private parties, thus making it possible to place a certain value on a claim, even if the victim cannot show specific economic harm. Victims who can show economic damage, for instance, through lost opportunity and the like, would be able to plead those damages and recover.

# V. CONCLUSION

Throughout the 1990s and 2000s, lawmakers and regulators were urged not to create rights and responsibilities in personal data, because, among other things, it was

---

[70] Id. at 284-85 (citation omitted).
[71] *See supra* Part II.B (revealing the ease with which imposters can use only fragments of personal information to secure credit).
[72] *Id.* at 285 (citations omitted).

feared that privacy law would make anti-fraud efforts more difficult.[73] Congress largely heeded this advice, giving wide berth of anti-fraud uses of personal information. This, of course, is a common narrative in the privacy world: individuals trade off having rights and responsibilities in data because it is believed that we all will be more secure if data can be used for anti-fraud purposes.

This article has elucidated an unfortunate irony in this narrative: policymakers chose to leave many anti-fraud uses of data free from consumer privacy laws, and yet, identity fraud continues to affect almost ten million Americans each year. In analyzing 16 applications pertaining to 6 victims of identity theft, it is clear that the most basic anti-fraud tools would have spotted errors impostors made when masquerading as the victims. For instance, X5's impostor was using the wrong date of birth and an invalid drivers license number -- one never issued by the state. We are in an unfortunate situation where consumer privacy was subordinated to anti-fraud interests, and the very people who said it was important to have anti-fraud tools could not care to use them, or perhaps even worse, they used them and ignored signals that fraud was present.

Proposals to mitigate identity theft remain narrow, focused upon particularly troubling practices may be limited in effect. Incentives are at the core of the identity theft problem. More money can be made by tolerating high levels of fraud than by more carefully screening against impostors. The market rewards lax authentication practices, because market actors risk losing new customers to competitors if they delay transactions to prevent fraud. Identity theft is an externality of the instant credit marketplace. Consumers have no ability to control whether they are a victim of this externality, because consumers are not in control of credit authentication.

An effective approach to reducing the incidence and impact of identity theft would address the underlying incentives that drive the instant credit market. If credit grantors, the entities that enjoy the great fruits from quick access to credit, were fully liable for its costs, more care would be applied to protect individuals from identity theft. A negligence regime could shift these costs, but could also produce suboptimal outcomes. However, a strict liability approach would simplify the remedial process for victims, and create stronger, direct incentives to prevent fraud.

---

[73] Anti-fraud systems need not depend on personal information. For instance, German researchers have found that analysis of basic demographic information is highly effective in segmenting accountholders into different fraud buckets. Thomas Hartmann-Wendels, Thomas Mählmann & Tobias Versen, *Determinants of Banks' Risk Exposure to New Account Fraud – Evidence from Germany*, 33 J. BANKING & FIN., 347 (2009).

THE YALE LAW JOURNAL

PAUL M. SCHWARTZ

# Preemption and Privacy

**ABSTRACT.** A broad coalition, including companies formerly opposed to the enactment of privacy statutes, has now formed behind the idea of a national information privacy law. Among the benefits that proponents attribute to such a law is that it would harmonize the U.S. regulatory approach with that of the European Union and possibly minimize international regulatory conflicts about privacy. This Essay argues, however, that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law. In a sectoral approach, a privacy statute regulates only a specific context of information use. An omnibus federal privacy law would be a dubious proposition because of its impact on experimentation in federal and state sectoral laws, and the consequences of ossification in the statute itself. In contrast to its skepticism about a federal omnibus statute, this Essay views federal sectoral laws as a promising regulatory instrument. The critical question is the optimal nature of a dual federal-state system for information privacy law, and this Essay analyzes three aspects of this topic. First, there are general circumstances under which federal sectoral consolidation of state law can bring benefits. Second, the choice between federal ceilings and floors is far from the only preemptive decision that regulators face. Finally, there are second-best solutions that become important should Congress choose to engage in broad sectoral preemption.

**AUTHOR.** Professor of Law, University of California, Berkeley, School of Law; Director, Berkeley Center for Law and Technology. For helpful suggestions, I thank Michelle Wilde Anderson, Holly Doremus, Ira Ellman, Daniel Farber, Malcolm Feeley, Robert Gellman, Andrew Guzman, Patrick Hanlon, Kate Heinzelman, Chris Hoofnagle, Ian Kerr, Ira Rubinstein, James Rule, Pamela Samuelson, Jason Schultz, Spiros Simitis, David Sklansky, Daniel Solove, Sarah Song, Stephen Sugarman, and William Treanor.

## FEATURE CONTENTS

## INTRODUCTION

In March 2007, Bill Gates, Microsoft Chairman, called for the enactment of a comprehensive federal privacy law.[1] His voice became one of many asking Congress to take broad and preemptive action to regulate the collection, storage, and transfer of information across the private sector. A patchwork of information privacy laws now exists in the United States, and it is one with federal and state elements. In the view of Gates and many others, it would be preferable to create a single federal law for the private sector that would impose uniform standards.

A broad coalition, including companies formerly opposed to enactment of privacy statutes, has now formed in support of a national information privacy law. Businesses that have signed on to this policy include Microsoft, Google, eBay, Intel, Oracle, Sun Microsystems, Hewlett-Packard, and Procter & Gamble.[2] The Center for Democracy and Technology, a privacy advocacy group, is coordinating this drive for a nationwide privacy law.[3] Among the benefits that proponents attribute to such a law is that it would harmonize the U.S. regulatory approach with that of the European Union (EU), and possibly minimize international regulatory conflicts about privacy.

This Essay argues, however, that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law. An omnibus statute establishes regulatory standards for a large field, which can, in many countries, sweep in the entire public and private sectors. In contrast, a sectoral law has jurisdiction over a specific context of information use. As an example, the Video Privacy Protection Act of 1988 establishes rules for the use of video rental information,[4]

---

1. *See* Anne Broache, *Gates Urges Federal Data Privacy Law*, CNET NEWS, Mar. 8, 2007, http://www.news.com/2100-1014_3-6165395.html; Grant Gross, *Microsoft's Bill Gates Wants New Privacy Law*, CIO, Mar. 7, 2007, http://www.cio.com/article/29936/Microsoft_s_Bill_Gates_Wants_New_Privacy_Law. The Microsoft support for a federal privacy law did not begin, however, in 2007, but 2005. A white paper by Brad Smith, Microsoft's General Counsel, provides the most detailed explanation of the company's position. *See* Brad Smith, Senior Vice President, Gen. Counsel, Microsoft Corp., Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation (Nov. 2005), http://www.microsoft.com/presspass/download/features/2005/PrivacyLegislationCallWP.doc [hereinafter Microsoft White Paper].

2. *See* Riva Richmond, *Business Group Calls for Privacy Law*, WALL ST. J., June 21, 2006, at B2; Erika Morphy, *Tech Giants Form Consumer Privacy Rights Forum*, TECHNEWSWORLD, June 21, 2006, http://www.technewsworld.com/story/51272.html.

3. Morphy, *supra* note 2.

4. *See infra* text accompanying notes 34-39.

and the Fair Credit Reporting Act contains rules for the use of credit reports.[5] The EU has long adopted omnibus information privacy laws; the United States has chosen sectoral laws for its private sector.

This Essay traces the history of information privacy law in Part I, discusses different aspects of a federal omnibus privacy law in Part II, and explores the jurisprudence of sectoral law in Part III. Throughout all Parts, it examines privacy statutes from different sectors in the United States, including laws regulating credit information, financial data, and video rentals. It also considers laws in areas other than privacy, such as environmental and labor law, and looks at comparative examples with a special focus on the EU and Canada.

A comparative element of Part I demonstrates American exceptionalism. From the start, U.S. information privacy law has taken a sectoral approach while European information privacy law has centered on omnibus laws. Yet these differences are best explained by a modest historical account of initial choices, path dependency, and the influence within the EU of a longstanding project to harmonize law within different member states. Omnibus privacy laws cannot be said to be fundamentally incompatible with a federal government.

In Part II, this Essay first considers the case for and against a federal omnibus law that functions only as a gap-filler. Such a statute would provide general standards to be used in areas in which no sectoral law exists, or when there is silence or ambiguity in such a law. The case for such an omnibus law is a close one. This kind of omnibus law proves, however, at best a long shot for enactment. Congress is far more likely to enact an omnibus law with strong preemptive language built around regulatory ceilings. Industry has indicated its support for only such a statute, and it may be in a position to derail any other legislation.[6] Yet such a law would be a dubious proposition due to its impact on experimentation in federal and state sectoral laws, and the consequences of ossification in the statute itself.

In contrast, and as Part III examines, federal sectoral statutes have more promise for information privacy. Sectoral laws are also likely to be a future privacy growth field. Due to a regulatory dynamic that scholars have termed "defensive preemption," businesses often may react to statutory innovations at

---

5. See *infra* text accompanying notes 79-86 for a discussion of the Fair Credit Reporting Act in the context of its amendment by the Fair and Accurate Credit Transactions Act.

6. The Microsoft White Paper indicates the importance of preemption from the perspective of a leading industry participant in this debate. *See* Microsoft White Paper, *supra* note 1, at 4-5. On the presence of numerous veto points for federal legislation in the United States, see ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 60 (2008).

the state level by seeking legislation at the federal level.[7] The critical question is the optimal nature of a dual federal-state system for information privacy law, and this Essay concludes by considering three aspects of this question.

First, there are certain general circumstances under which federal sectoral consolidation of state law can bring benefits. These include the avoidance of inconsistent regulations in areas with high costs and little policy payoff, and the establishment of "field definitions" that can lower compliance costs. Second, the choice between federal ceilings and floors is far from the only preemptive decision that regulators face. In particular, the toolkit of privacy federalism should not be limited to the standard concept of "subject matter" preemption. As this Essay argues, privacy federalism can also include ceilings that extend only to the "conduct" regulated and not the entire subject matter of the regulation. As an example of such conduct preemption, I will discuss the Fair and Accurate Credit Transactions Act (FACTA), an important 2003 amendment to the Fair Credit Reporting Act.[8] Another important aspect of the toolkit of privacy federalism is a sharing of enforcement authority among federal and state regulators.

As a final aspect of its consideration of an optimal dual federal-state system for information privacy, this Essay develops a number of second-best solutions. These policy safeguards are important because Congress may engage at times in broader sectoral preemption than is fully merited. In such circumstances, important policy safeguards to consider include a "plus one" strategy, under which Congress allows at least a single state to retain higher standards or to develop standards different from the federal one. Another policy safeguard would be to subject preemption clauses in federal privacy legislation to a ten-year sunset.

## I. THE PAST AND PRESENT OF INFORMATION PRIVACY LAW

This Part looks at the emergence of modern information privacy law and its reliance on Fair Information Practices (FIPs). It then traces the development of omnibus and sectoral privacy laws in the United States and analyzes differences in the regulatory paths for information privacy in the United States and the European Union.

7. See *infra* text accompanying notes 166-167 for a discussion of defensive preemption.

8. 15 U.S.C. §§ 1681-1681x (Supp. V 2005).

### *A. The Roots of Privacy Law*

The roots of modern information privacy law are found in state common law, and, specifically, in the tort right of privacy. The genesis of this aspect of privacy law was the publication in 1890 of *The Right to Privacy* by Samuel Warren and Louis Brandeis.[9] Over the course of the twentieth century, and under the helpful influence of William Prosser, author of the relevant sections of the *Restatement (Second) of Torts*, nearly all states have recognized some branches of the tort right of privacy.[10] The process of adoption of the privacy tort was long, but its acceptance is now nearly universal. In 1998, one of the last three holdouts, Minnesota, adopted the tort of invasion of privacy in *Lake v. Wal-Mart Stores, Inc.*[11]

Tort privacy relies on litigation by injured parties and decisionmaking by juries. In Robert Post's seminal formulation, tort privacy is centered on civility norms that maintain and structure communal life.[12] It creates a legal process for negotiation of limits both on the community's access to personal information and on the individual's desire for zones without community scrutiny. Tort privacy's centrality to the law of information privacy has also waned over time. As Post rightfully observes, tort privacy is under stress today for two reasons. First, society's need for accountability has placed new emphasis on the community's access to information.[13] Second, the rise of an "instrumental world of large surveillance organizations" is in basic tension with the underlying logic of civility norms.[14] These large surveillance organizations are only one aspect, albeit an important one, of the information age, which is marked by computerized data processing, innovative means for collecting and sharing personal information, and detailed data trails left by all individuals in their daily lives.

The law's chief reaction to these new developments has not been through tort law, but FIPs.[15] This legal response, which began in the United States and

---

9. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

10. For a detailed overview of the privacy tort and its development, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 77-231 (3d ed. 2009).

11. 582 N.W.2d 231 (Minn. 1998).

12. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).

13. *See id.* at 1010.

14. *Id.* at 1009. Daniel Solove also has developed proposals to revitalize the tort right of privacy for the information age. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 113-24 (2007).

15. Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 779-81 [hereinafter Schwartz, *Lessig's*

Western Europe in the 1970s, defines obligations for bureaucratic organizations that process personal information. The basic toolkit of FIPs includes the following: (1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data.[16]

No single privacy statute contains all these rules in the same fashion or form. As a critical matter, the precise content of the rules will be different based on the context of data processing, the nature of the information collected, and the specific regulatory and organizational environment in which the rules are formulated. Of particular note is the enforcement of FIPs. Depending on the form that FIPs take, the law can include some combination of enforcement and oversight through a private right of action and governmental enforcement. Public entities involved in the process of FIPs include the Federal Trade Commission, various federal regulators of financial institutions, Privacy Act officers, and state attorneys general.

### *B. Omnibus and Sectoral Privacy Laws: U.S. and European Regulatory Paths*

The world's first comprehensive information privacy statute was a state law; the Hessian Parliament enacted this statute in Wiesbaden, Germany, on September 30, 1970.[17] In the accepted terminology, this statute is an "omnibus law." It establishes regulatory standards for a broad area—namely the state and local governments of Hessen. This law was followed by those of other German states, which then influenced the form and content of a federal omnibus law, the Federal German Data Protection Act (Bundesdatenschutzgesetz, or

*Code*]; *see* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999) (fair information practices "are the building blocks of modern information privacy law").

16. The expression of FIPs in different laws, regulations, and proposals varies in details, sometimes crucially. For my own attempts to summarize these standards, see Schwartz, *Lessig's Code*, *supra* note 15, at 779-80; and Paul M. Schwartz & William M. Treanor, Review Essay, *The New Privacy*, 101 MICH. L. REV. 2163, 2181 (2003).

17. For a masterful account of these developments, see Spiros Simitis, *Einleitung* [*Introduction*], *in* NOMOS KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [COMMENTARY ON THE FEDERAL PRIVACY LAW] 61, 62-63 (Spiros Simitis ed., 6th ed. 2006).

BDSG).[18] The term, "data protection," is the standard nomenclature in Europe for information privacy. The 1977 BDSG establishes standards for information processing by public and private entities alike.

The German preference for anchoring data protection law in omnibus privacy statutes is typical of European data protection law. The European Union's adoption in 1995 of the Data Protection Directive has played a key role in this process.[19] The Data Protection Directive envisions that all EU member states follow its requirements by "transposing" them into national law.[20] It leaves the choice of specific legal instruments to each member state, and, at least theoretically, an EU member state could choose to enact a combination of sectoral laws to comply with the Directive.[21] Yet all member states have enacted omnibus laws to transpose the Directive into national law. As Ulrich Dammann notes, the universal favoring of omnibus laws in the EU is unsurprising because the Directive requires a transposition in "its entire range of application."[22] A choice of sectoral laws would place a burden on each member state to enact "a multitude of sectoral regulations."[23] Moreover, each member state was faced with the relatively short deadline of three years that the Directive established for compliance with its standards.[24] Enacting a complete range of sectoral laws in this framework would have been a more than heroic endeavor. Even with omnibus statutes as the chosen method of regulation, only four member states were able to meet the established deadline, and the European Commission even initiated legal action in 1999 due to this

18. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) [Federal Data Protection Act], Jan. 27, 1977, BGBl. I at 201, Jan. 14, 2003, BGBl. I at 66, last amended by Gesetz, Aug. 22, 2006, BGBl. I at 1970.

19. Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive]. For background on the Directive, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 480-83 (1995).

20. Data Protection Directive, *supra* note 19, recital 69, at 37.

21. Recital 23 of the Directive leaves the choice of regulatory instruments open to the EU member state. It states, "Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes." *Id.* recital 23, at 33. This language probably is best read as permitting a combination of omnibus and sectoral laws by member states.

22. Ulrich Dammann, *in* EG-DATENSCHUTZRICHTLINIE: KOMMENTAR [COMMENTARY ON EUROPEAN COMMUNITY DATA PROTECTION DIRECTIVE] 133 (Ulrich Dammann & Spiros Simitis eds., 1997).

23. *Id.*

24. Data Protection Directive, *supra* note 19, art. 32, at 49.

delay in the European Court of Justice against France, Germany, Ireland, Luxemburg, and the Netherlands.[25]

The Directive's requirement that national laws reflect its principles has followed the EU in its eastward expansion. The typical omnibus statute also allows for further specification of regulatory norms through sectoral regulations. For example, the BDSG explicitly provides within its first section that federal sectoral laws take precedent over its provisions.[26] And there has been no shortage of sectoral laws in EU member states.

In the United States, by contrast, FIPs have generally developed through laws that regulate information use exclusively on a sector-by-sector basis. The one partial exception in the United States is the Privacy Act of 1974,[27] which is an omnibus law for the public sector, albeit a narrow one. The Privacy Act only regulates certain kinds of federal agencies, and only certain kinds of information use.[28] This Essay discusses the Privacy Act and its genesis in more detail below.

The divergent evolution of U.S. and European law raises the question of why these legal systems took different paths at the fork in the regulatory road. The puzzle is all the more intriguing because an omnibus bill for the private and public sectors, Senate Bill 3418 (S. 3418), was on the table, however briefly, during the formative period in the United States for information privacy. As originally introduced by Senator Samuel Ervin on May 1, 1974, S. 3418 had a broad jurisdictional sweep. It would have established requirements for "[a]ny Federal agency, State or local government, or any other organization maintaining an information system that includes personal information."[29] Before turning to analysis of the divergent regulatory paths in the United States and Europe, I discuss the road not taken by Congress. S. 3418 can also

25. *See* COMM'N OF THE EUROPEAN CMTYS., FIRST REPORT ON THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE (95/46/EC), at 3 n.1 (2003), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT.

26. "In so far as other legal provisions of the federal government are applicable to personal data . . . such provisions shall take precedence over the provisions of this Act." Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) [Federal Data Protection Act], Jan. 27, 1977, BGBl. I at 201, last amended by Gesetz, Aug. 22, 2006, BGBl. I at 1046, § 1(3).

27. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

28. Regarding the important limitations of the Privacy Act to only "federal agencies" and its narrow definition of "record," see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 92 n.4 (1996); and U.S. DEP'T OF JUSTICE, PRIVACY ACT OVERVIEW, MAY 2004 EDITION: DEFINITIONS (2004), *available at* http://www.usdoj.gov/oip/1974definitions.htm.

29. S. 3418, 93d Cong. § 201(a) (1974).

help illustrate differences between an omnibus bill and a sectoral law, whether in the United States or Europe.

The core of any omnibus bill is a reliance on general clauses; these provisions establish FIPs that are of necessity broadly worded because they cannot be directed to a specific area of information processing. As an initial example, S. 3418 would have required public and private entities to "collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization."[30] In the taxonomy of FIPs, which Section I.A discussed above, this language establishes a disclosure limitation. The bill would also have required organizations to "maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject"[31]—a data quality requirement. As a final example, the bill would have placed restrictions on onward transfers. S. 3418 would prohibit the regulated entities from making a "dissemination" of information without meeting certain requirements, such as "including limitations on access thereto, and . . . determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed."[32] In other words, the organization transferring personal data would be obliged to determine that the entity receiving the information followed FIPs, including drawing a line against further transfers.

From a contemporary perspective, one of the most interesting aspects of the proposed bill from 1974 is that it would have conditioned international transfers of information on either subject consent or equivalent protections abroad for the personal data. This proposed requirement of "equivalency" would have exceeded the protections later found in the European Data Protection Directive, which was enacted in 1995 and took effect in 1998. The Directive calls only for "adequate" protection before an organization, public or private, in an EU member state is permitted to transfer personal information to an organization in a third-party nation, such as the United States.[33] Yet, taken as a whole, the general clauses of S. 3418 would have proven similar to those in a typical, modern omnibus European data protection law.

In contrast to these omnibus privacy laws, a sectoral approach is necessarily more narrowly tailored and its terms, by their nature, are more specific. The

30. *Id.* § 201(a)(1).

31. *Id.* § 201(a)(4).

32. *Id.* § 201(a)(5).

33. Data Protection Directive, *supra* note 19, art. 25(1), at 45; *see* Schwartz, *supra* note 19, at 483-88.

U.S. Video Privacy Protection Act of 1988 (VPPA) provides a good example.[34] Its jurisdictional sweep is limited to a "video tape service provider," which is defined in technology-neutral terms.[35] As a result, the law has been easily extended to DVDs. The VPPA contains FIPs, but these are necessarily tailored to the specific context of the "rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[36] A description of its customization will provide a useful illustration of the basics of a sectoral information privacy statute.

As an initial example of this tailoring, the VPPA first forbids video tape service providers from disclosing personal information about their customers. It then provides a series of disclosure exceptions centered on the context of video rentals and sales. Thus, it allows disclosures "incident to the ordinary course of business of the video tape service provider."[37] The VPPA also permits disclosure of a limited subset of information, namely of the names and addresses of consumers, but only if an opt-out, or a chance to refuse this disclosure, is first offered to the consumer and the disclosure "does not identify the title, description, or subject matter of any video tapes."[38] A further exception for a different subset of information allows disclosure of the subject matter of videos, but limited to circumstances when "the disclosure is for the exclusive use of marketing goods and services directly to the consumer."[39] The idea here is that consumers will be able to make their wishes known to video providers if they do not wish to receive such marketing information.

I now return to the question of why the United States and Europe have taken divergent paths. The United States continues to lack an omnibus bill that covers the private sector and has, at best, only a relatively limited omnibus bill for part of the public sector. In contrast, as new countries have joined the EU, they have commenced their regulation of information privacy with omnibus laws and have supplemented these statutes with sectoral ones. In my view, the continuing differences can best be explained by a modest account that looks at (1) initial choices followed by path dependency, and (2) the usefulness of omnibus laws in multination systems that wish to harmonize their regulations.

---

**34.** 18 U.S.C. § 2710 (2000).

**35.** *Id.* § 2710(a)(4).

**36.** *Id.*

**37.** *Id.* § 2710(b)(2)(E).

**38.** *Id.* § 2710(b)(2)(D)(ii).

**39.** *Id.*

### 1. *The U.S. Path*

The original form of S. 3418 was quickly abandoned in favor of a scaled-back statute—the Privacy Act, which only regulates federal agencies. The Senate report on S. 3418 indicates legislators' concerns regarding an overly broad statutory response and their doubts as to whether the private sector even posed much of a threat to privacy beyond credit reporting.[40] Furthermore, Congress had reason at the time to believe that its enactment of the Fair Credit Reporting Act in 1970 had responded to the threats to privacy posed by credit reporting. Priscilla Regan notes that congressmen also wondered during the debate over S. 3418 if an omnibus law for the private sector represented "an impossible task; too many factors had to be taken into account to devise a policy that protected individuals and did not unreasonably burden organizations, while also allowing for government oversight."[41]

Thus, there was considerable caution in the United States in the 1970s against a broad regulation of information use that would include the private and public sectors in one fell swoop. This orientation demonstrates an ideology that I term "regulatory parsimony." As the medical profession expresses the idea, "above all, do no harm."[42] The same perspective is demonstrated in aspects of the Privacy Act of 1974, which, though a kind of omnibus bill for the public sector, is more limited than the typical omnibus EU law for the public sector.

---

40. STAFF OF S. COMM. ON GOV'T OPERATIONS & H. COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579): SOURCE BOOK ON PRIVACY 172 (Comm. Print 1976) [hereinafter PRIVACY SOURCEBOOK]. The Senate Committee on Government Operations in its report on the bill observed that it was persuaded to "delay a decision on total application by considerations of time and investigative resources for developing a full hearing record and for drafting the needed complex legislative solution for information abuses in the private sector, beyond those presently covered by the Fair Credit Reporting Act and its pending amendments." *Id.* As Priscilla Regan in her account of this period writes, "A major argument for removing the private sector from the purview of the 1974 legislation was that there was little concrete evidence of abuses in private sector personal information practices." PRISCILLA REGAN, LEGISLATING PRIVACY 78 (1995).

41. REGAN, *supra* note 40, at 78.

42. For a discussion of the origins of this phrase, see Cedric M. Smith, *Origin and Uses of* Primum Non Nocere—*Above All, Do No Harm!*, 45 J. CLINICAL PHARMACOLOGY 371 (2005).

### 2. *The EU Path*

Multiple factors contributed to the rise of the omnibus model in the EU. For one thing, the EU nations that enacted this kind of information privacy statute viewed preventive action to be more important than the risks of legislating under uncertainty. Instead of the parsimony principle used in the United States, the European nations were acting on a "precautionary principle." As Cass Sunstein, a critic of this concept, has explained, the idea is that it is wiser to act to prevent harm than to require unambiguous evidence to support a regulatory measure.[43]

Regarding the decision to enact omnibus laws from the first era of data protection law in Europe, Spiros Simitis observes that the European lawmaker began with the idea that it was necessary to analyze problems that cut across individual contexts of processing and for which, therefore, a uniform solution expressed in a single statute should be developed.[44] At the same time, the European legislator was also confronted with a considerable challenge because data processing was in its infancy and, therefore, the subject of regulation lacked clear contours.[45]

Despite uncertainty, European lawmakers decided to enact omnibus data protection statutes. Abraham Newman has identified different historically contingent factors that smoothed the path to enactment of data protection statutes in the 1970s in France and Germany,[46] two leaders in information privacy law. For example, Newman shows how French industry's potential opposition to the proposed French data protection legislation was muted by the past nationalization of many affected companies and the centralization of these industries, which minimized the impact of the statute.[47] As a further example, in Germany, a pro-privacy alliance benefited at the critical point in the late 1970s from a "particular alignment of political actors at that time [who] neutralized key barriers to the passage of the policy."[48]

After the initial choice in key European nations to enact omnibus laws, the EU's "harmonizing" project in the field of data protection exercised a strong

---

**43.** *See* CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 23-25 (2005).

**44.** Simitis, *supra* note 17, at 68.

**45.** *Id.*

**46.** NEWMAN, *supra* note 6, at 60-69.

**47.** *Id.* at 62. The impact was muted because in France, "[b]anks did not need to exchange intense amounts of information because they had relatively large, national customer pools and access to a wide range of information about those customers." *Id.*

**48.** *Id.* at 63-64.

influence on other nations. This term of European Community law refers to formal attempts to increase the similarity of legal measures in member states. As Joachim Jacob, the Federal Data Protection Commissioner of Germany, observed, "the European Community is also becoming an information and data community."[49] European integration increased the sharing of data among EU Member Nations and created new demands for personal information. Due to this data sharing throughout the EU, nations with privacy statutes had incentives to advocate equivalent safeguards in all member states. Without such shared levels of protection, previous efforts within individual nations to ensure privacy for their citizens' data would be for naught. The information could easily be transferred to other member states with weaker levels of data protection.

The resulting policy response was the movement to harmonize privacy law throughout the EU. Through the Data Protection Directive, the EU obliged lagging nations within its ranks to protect personal information and to follow the omnibus approach.[50] Moreover, as Newman has observed, the national data protection commissioners, already in place by the 1980s, played an important transgovernmental role in shaping the Directive and expanding privacy protection in Europe.[51] National privacy regulators worked so that their national legislation would be "exported upward regionally."[52] The benefit of an omnibus law for this project is that it provides a relatively limited series of benchmarks and sets them within a single statute. In contrast, an exclusively sectoral approach would lead to far greater complexity in assessing the "equivalency" of data protection for each of the now twenty-seven EU member states.

These differences in the regulatory form of information privacy do not demonstrate that an omnibus system would be incompatible with U.S. federalism. Indeed, omnibus laws are far from incompatible with this principle of governmental organization. Germany—one of the EU leaders in data protection law—has a federal system of government. Outside of the EU, Canada—a country with a federal form of government—enacted an omnibus

49. 14. TÄTIGKEITSBERICHT DES BUNDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ GEMÄß ABS. 1 DES BUNDESDATENSCHUTZGESETZES [REPORT OF THE COMMISSIONER FOR DATA PROTECTION IN ACCORDANCE WITH ABS. 1 OF THE FEDERAL DATA PROTECTION ACT] 12 (1993).

50. For a discussion of the influence of the European pressure on Margaret Thatcher's Tory government and how it led to the U.K. data protection law, see COLIN J. BENNETT, REGULATING PRIVACY 91 (1992).

51. NEWMAN, *supra* note 6, at 75. For an early discussion of the important role of the data protection commissioners in the EU, see Schwartz, *supra* note 19, at 492-95.

52. NEWMAN, *supra* note 6, at 3, 97-98.

privacy law for the private sector in 2000. Omnibus laws function no better or worse in Germany and Canada than in nonfederal countries, such as France or the United Kingdom. I am also skeptical about the role that cultural differences regarding information privacy in Europe and the United States play with regard to the resulting choices of respective regulatory forms.[53] This comparative topic must be reserved, however, for another day.

### *C. Recent Federal and State Trends and the Role of Preemption*

This Essay's brief history of information privacy in U.S. law has traced its roots from tort law to the start of the modern era. It also has drawn on comparative examples to illustrate U.S. regulatory exceptionalism centered on its lack of an omnibus statute for the private sector. To bring this account up to the present, this Essay returns to the formative decade for information privacy law in the United States—the 1970s. During this period, the U.S. Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act), the Fair Credit Reporting Act in 1970, the Family Educational Rights and Privacy Act of 1974, and the Right to Financial Privacy Act of 1978.[54] All of these laws are sector-specific except for the Privacy Act of 1974.

Against this background, the states in the United States have been especially important laboratories for innovations in information privacy law. As noted, the state tradition begins with the recognition of privacy torts throughout the twentieth century. Other innovations followed. Already in 1977, the blue ribbon Privacy Protection Study Commission commented on "the significant increase in State regulatory efforts to protect the interests of the individual in records kept about him . . . [which had] already led a number of

53. James Whitman provides the richest argument for the influences of cultural differences in the differing approaches to information privacy in Europe and the United States. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1163 (2004). For an interpretation of differences in EU and U.S. information privacy law that stresses the influence of historically contingent events, see NEWMAN, *supra* note 6, at 52-54. For a discussion that stresses both historically contingent factors and cultural ones in shaping European privacy law, see Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 684-88 (2007).

54. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2000); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681a-1681x; Wiretap Act, 18 U.S.C. §§ 2510-2522; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

States to try out innovative protections, particularly in their regulation of private-sector organizations."[55]

State privacy law has started the twenty-first century with renewed activity. The influence of state privacy law has been felt in three ways. First, states have often been the first to identify areas of regulatory significance and to take action. Laws requiring data security breach notifications began with California's Senate Bill 1386 (S.B. 1386) in 2002.[56] Another forty-four states, Puerto Rico, the Virgin Islands, and the District of Columbia have enacted similar statutes.[57] This activity can be contrasted with a lack of any federal response in this policy area. Congress remains unable to agree on a data breach notification bill—a perfect illustration, as noted earlier, of the slow trajectory of federal privacy legislation. As examples from a different area of privacy law, New York and Connecticut are now considering bills that would set limits on companies that track consumers across websites to deliver targeted advertisements based on their behavior.[58]

Second, states have provided innovative approaches. Such innovations are illustrated in the preceding paragraph. As a further example, states have taken legislative action to restrict the use of social security numbers.[59] They also have granted consumers who are victims of identity theft the ability to place freezes on their credit reports, and have obliged businesses to supply these victims with the relevant records of transactions associated with their stolen identity.[60] Moreover, state law preceded federal law in granting identity theft victims a right to free copies of their credit reports.[61]

---

55. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 491 (1977).

56. CAL. CIV. CODE §§ 1798.29, 1798.82 (West Supp. 2009); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007).

57. Nat'l Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Feb. 9, 2009).

58. For the Connecticut bill, see H.B. 5765, Gen. Assem., Feb. Sess. (Conn. 2008). In New York, there have been bills introduced in the Senate and House. *See* Assem. B. 9275, 2007 Leg., 230th Sess. (N.Y. 2007); S. 6441, 2007 Leg., 230th Sess. (N.Y. 2007).

59. National Conference of State Legislatures, Financial Privacy, http://www.ncsl.org/programs/lis/privacy/financeprivacy.htm (last visited Feb. 9, 2009).

60. Consumer Union, State Security Freeze Laws, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited Dec. 1, 2008). For an example of a state law requirement requiring the disclosure of transaction information to a victim of ID theft, see CAL. PENAL CODE § 530.8 (West Supp. 2009).

61. The applicable states are Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont. COLO. REV. STAT. §§ 12-14.3-104 to -105 (2008); GA. CODE. ANN. § 10-1-393(29)(C) (2000); ME. REV. STAT. ANN. tit. 10, §§ 1315-1316 (1997 & Supp. 2008); MD.

Third, states have created an opportunity for simultaneous experiments with different policies. As Malcolm Feeley and Edward Rubin dryly observe of the general idea of states-as-laboratories, these experiments are "desirable, presumably . . . not because of an abiding national commitment to pure research but because the variations may ultimately provide information about a range of alternative government policies and enable the nation to choose the most desirable one."[62] Justice Louis Brandeis famously pointed to this benefit of state regulation and also identified the ability of these "novel social and economic experiments" to take place, at least some of the time, "without risk to the rest of the country."[63] As an illustration of these simultaneous policy solutions, data breach notification statutes vary in their notification "triggers"—that is, the standard under which a company must share information about a data security incident.[64]

As Patricia Bellia correctly observes in her contribution to this Feature, there also have been important federal statutory contributions to this area as well as federal and state judicial inputs. Bellia points to the rich interplay between federal and state regulatory responses and provides a nuanced description of this process.[65] Yet this federal-state dialogue does not refute the notion that states have been significant innovators in this area. At the same time, certain kinds of federal choices are best seen as examples of predetermined (and sometimes useful) inputs to the privacy landscape and not as illustrations of "federal leadership in information privacy problems."[66]

In particular, a host of Bellia's examples drawn from the federal law of surveillance falls into this category of assigned tasks. After all, it is uniquely the

---

CODE ANN., COM. LAW §§ 14-1206 to -1209 (LexisNexis 2005); MASS. ANN. LAWS ch. 93, §§ 58-59 (LexisNexis 2006 & Supp. 2008); N.J. STAT. ANN. §§ 56:11-34 to -37 (West 2001 & Supp. 2008); VT. STAT. ANN. tit. 9, § 2480(b)-(c) (2006). Federal law permits these states to continue to determine how many free credit reports each year that their residents can receive. 15 U.S.C. § 1681t(b)(4) (Supp. V 2005). The result of these federal and state laws is that residents of these states each year can receive one free credit report under federal law and one free credit report under state law, or, in the case of the Georgia statute, two free reports.

62. MALCOLM M. FEELEY & EDWARD RUBIN, FEDERALISM: POLITICAL IDENTITY AND TRAGIC COMPROMISE 26 (2008).

63. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

64. Schwartz & Janger, *supra* note 56, at 960-70.

65. Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009).

66. *Id.* at 882.

task of the federal government to develop rules for federal law enforcement. Many of these federal inputs to the privacy landscape in the area of telecommunications surveillance have been notably unsuccessful.[67] Admittedly, the regulatory questions are thorny.[68] For instance, Congress has bungled even a relatively easy task—the creation and maintenance of a system for systematic collection of telecommunications surveillance statistics.[69]

As for preemption, federal statutes have taken varied approaches to state experimentation in the information privacy area. Some federal laws only establish a "floor"—that is, a minimum standard that states may exceed. As an example, consider the Video Privacy Protection Act of 1988 (VPPA), which regulates how video stores collect and share rental information.[70] The VPPA requires states to follow its list of prohibited disclosures but permits additional state safeguards, including reductions to its lists of permitted disclosures of rental information.[71] At least thirteen states have enacted their own video privacy statutes.[72]

The Wiretap Act provides another classic example of a federal privacy "floor." This federal statute permits the recording of telephone conversations by private parties if one party to the conversation has consented.[73] It also allows

---

**67.** For different critical perspectives, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 181 (2007); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008); and Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1292-98 (2004). Although not a critic in general of federal surveillance law, Orin Kerr has expressed strong criticisms of one branch of this law, the Stored Communications Act. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233-43 (2004).

**68.** As a single example, classic statutory assumptions in the Foreign Intelligence Surveillance Act regarding the location of the subject of surveillance have been undercut by modern telecommunications surveillance. *See* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008).

**69.** Schwartz, *supra* note 67, at 287.

**70.** 18 U.S.C. § 2710 (2000).

**71.** *Id.* § 2710(f).

**72.** *See* CAL. CIV. CODE § 1799.3 (Deering 2005); CONN. GEN. STAT. § 53-450 (2007); DEL. CODE ANN. tit. 11, § 925 (2008); IOWA CODE § 727.11 (2003); LA. REV. STAT. ANN. § 37:1748 (2007); MD. CODE ANN., CRIM. LAW § 3-907 (LexisNexis 2002); MASS. GEN. LAWS ch. 93, § 106 (2006); MICH. COMP. LAWS ANN. §§ 445.1711-.1715 (West 2002); MINN. STAT. ANN. § 325I.02-.03 (West 2004); N.H. REV. STAT. ANN. § 351-A:1 (2008); N.Y. GEN. BUS. LAW §§ 670-675 (McKinney 1996); R.I. GEN. LAWS § 11-18-32 (2002); TENN. CODE ANN. §§ 47-18-2201 to -2205 (2002).

**73.** 18 U.S.C. § 2511(2).

states to enact more restrictive laws.[74] As the Wiretap Act's legislative history notes, "The proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation."[75] Twelve states have enacted "all party" consent statutes.[76] Under these laws, all parties to a phone call must agree to have their telephone call recorded.

Another federal law with a similar approach to state regulation is the Gramm-Leach-Bliley Act (GLB Act), Title V of which regulates the personal information processing of financial institutions. This statute also sets a federal "floor" for privacy.[77] For example, the GLB Act allows states to set higher privacy standards regarding how financial institutions share personal information with outside organizations (termed "non-affiliated entities" in the statute).[78]

Federal privacy legislation has also preempted state legislation with the effect of weakening existing state standards. A statute from 2003, FACTA, which amends the Fair Credit Reporting Act, contains examples of such a downward revision.[79] To be sure, FACTA also has positive aspects. For example, it seeks to improve the accuracy of credit reports. Thus, it requires each national credit bureau to provide upon request a free report to consumers and to provide credit scores to consumers for a fee.[80] FACTA also takes a number of steps to heighten data security. For example, it mandates credit card truncation on receipts provided to consumers—a requirement that courts have found to apply not only to printed receipts in real space, but also to receipts for online purchases that are displayed electronically.[81] FACTA also forbids printing a credit card expiration date on a receipt.[82] Moreover, FACTA institutes strict data disposal rules that reach "any person that maintains or

74. *See* People v. Conklin, 522 P.2d 1049, 1057 (Cal. 1974).

75. S. REP. NO. 1097, at 98 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2187.

76. Reporters Committee for Freedom of the Press, Can We Tape?, http://www.rcfp.org/taping/index.html (last visited Dec. 1, 2008).

77. 15 U.S.C. § 6807.

78. For an analysis, see Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1241-46, 1257-59 (2002).

79. 15 U.S.C. §§ 1681-1681x (Supp. V 2005).

80. *Id.* §§ 1681g(a), 1681j(a).

81. *Id.* § 1681c(g). For these cases, see Grabein v. 1-800-Flowers.com, Inc., No. 07-22235-CIV, 2008 U.S. Dist. LEXIS 11757 (S.D. Fla. Jan. 29, 2008); Vasquez-Torres v. Stubhub, Inc., No. CV 07-1328, 2007 U.S. Dist. LEXIS 63719 (C.D. Cal. July 2, 2007).

82. 15 U.S.C. § 1681c(g)(1).

otherwise possesses consumer information."[83] It requires covered entities that hold customer accounts to implement programs to respond to so-called "Red Flags" that signal possible ID theft.[84]

These meritorious aspects of FACTA are accompanied, however, by a number of ceilings that restrict the ability of states to offer greater protections to consumers. Before FACTA, the Fair Credit Reporting Act contained a list of limited preemptions for certain specified "subject matters," and these preemptions were set to expire in 2004.[85] In FACTA, Congress made permanent all existing preemptions in the Fair Credit Reporting Act, and added a list of new and permanent preemptions. In so doing, it reversed some existing state safeguards.[86] As Part III explains, however, FACTA also makes an important innovation to the jurisprudence of preemption by limiting some of its ceiling preemptions to a narrow category of "required conduct" rather than the broader category of "subject matter."[87]

Here, then, is the landscape against which Bill Gates and others have called for a federal omnibus statute for privacy—and one with strong preemption requirements. Industry in the United States also has made clear that strong ceiling preemption is an essential condition of its support for any comprehensive legislation. As a Microsoft white paper from 2005 states, "federal privacy legislation should pre-empt state laws that impose requirements for the collection, use, disclosure and storage of personal information."[88] Any single drop of preemption language in a federal statute is, moreover, likely to go a long way. In recent litigation concerning other areas of law, the Supreme Court has demonstrated a willingness in the face of statutory

---

**83.** *Id.* § 1681w(a)(1).

**84.** *Id.* § 1681m(e). A Red Flag is a pattern, or activity that might indicate identity theft, and the law and applicable guidelines require covered companies that have consumer information to implement identity theft programs to respond to Red Flags. *Id.*

**85.** *See, e.g.*, *id.* §§ 1681h(e), 1681t(b).

**86.** For example, FACTA reversed one aspect of California's Senate Bill 1 (S.B. 1), which required customers to be permitted to "opt-out," or indicate their refusal to information sharing before an organization could share such personal information with their affiliates. *Id.* § 1681a(d)(1). For case law finding that FACTA's preemption voids some but not all of S.B. 1's affiliate sharing provisions, see *American Bankers Ass'n v. Lockyer*, 541 F.3d 1214 (9th Cir. 2008).

**87.** 15 U.S.C. §§ 1681c-1, 1681t(b)(5) (Supp. V 2005).

**88.** Microsoft White Paper, *supra* note 1, at 4.

ambiguity to identify a congressional intent to occupy a regulatory field and impose a "ceiling."[89]

## II. A FEDERAL OMNIBUS PRIVACY LAW: STRENGTHS AND WEAKNESSES

Overall, the approach in the United States to information privacy law in the private sector has been through sector-specific laws containing FIPs, which have been enacted by federal and state lawmakers. As I mentioned at the start of this Essay, Bill Gates and others support the creation of a federal omnibus law. Here there are two distinct issues, which I will treat sequentially. First, there is the issue of the general choice between an omnibus versus sectoral means of regulating information privacy law. The second issue, preemption, concerns how such a law would interact with state laws.

In this Part, while considering the possible merits of a federal omnibus law, I focus on the instrumental and normative implications for information privacy on the distribution of lawmaking authority among the federal government and the states. Thus, I assume that such legislation is constitutionally permissible. The scope of the Commerce Clause is broad, and the Supreme Court is likely to uphold a federal omnibus privacy law.[90] An omnibus privacy law might also have consequences for the overall distribution of political power between the federal government and the states. Rather than considering this larger federalism issue, however, I concentrate on the consequences for information privacy law of a federal omnibus law.

### *A. Federal Versus State Regulation of Information Privacy*

Imagine enactment of a law that would provide general standards to be used when there was no sectoral law, or when there was silence or an

89. *Compare* Watters v. Wachovia Bank, N.A., 127 S. Ct. 1559 (2007) (noting that under the National Bank Act, a national bank's mortgage business, including its operating subsidiaries in the states, is subject exclusively to regulation by the Federal Office of the Comptroller of the Currency), *with id.* at 1573 (Stevens, J., dissenting) (noting an "absence of relevant statutory authority" permitting "the laws of a sovereign State" to "yield to federal power" in the regulation of the business activities of mortgage brokers and lenders).

90. *See* Reno v. Condon, 528 U.S. 141 (2000). In *Reno*, the Supreme Court held in a unanimous decision that Congress had power to regulate the conditions under which states and private parties could use, share, and sell drivers' motor vehicle registration information. *Id.* The Supreme Court has considerable leeway to decide that personal information itself is a subject of interstate commerce, and to find that even intrastate information markets can have an impact on interstate commerce. *See* Gonzales v. Raich, 545 U.S. 1, 26 (2005).

ambiguity in a sectoral law. In this Section, I consider precisely such an omnibus privacy statute, which would function as a gap-filler. What would be the results of such a statute? The consequences would prove to be both positive and negative. First, an omnibus law would overcome the inability of sectoral laws, whether federal or state, to respond adequately to telecommunications convergence. Second, omnibus laws would level the regulatory playing field where sectoral laws can place unequal burdens on industries in closely related areas. Finally, an omnibus law might help convince the EU of the adequacy of U.S. privacy law and thereby assist in smoothing data flows to this country. As for the negative results, these are the costs of an extra layer of regulation, namely, the harms from disregard of the "parsimony principle"—which is a warning against taking broad action under uncertainty—and the risk of an omnibus law's obsolescence.

### *1. Positive Results*

Convergence is the idea that different kinds of telecommunications media are coming together in ways and with consequences that are often unexpected. In *Technologies of Freedom*, Ithiel de Sola Pool made an early and influential description of how convergence was affecting one area of telecommunications. As Pool noted in 1983, "Cable television systems no longer just distribute broadcast programs but also transmit data among business offices and sell alarm services, movies, news, and educational courses."[91] Such convergence is a result of the ease with which digital data can be shared, combined, and transmitted. Beyond such multifunctionality, convergence is also taking place because of the invention of new devices, applications, and software technologies.

In the face of convergence, sectoral laws run up against limits. I have already examined the VPPA and noted that it smoothly made the transition from the videocassette era to DVDs. It is now in the process of confronting the era of movies rented and watched online as well as YouTube and similar Internet sites, such as blogs with embedded vlogs. The statute's transition concerning traditional movies accessed online should be unproblematic, but more open questions are likely to confront the VPPA if it is to be applied to digital media that no longer seem to fit the regulatory paradigm from 1988 of "prerecorded video cassette tape[s] or similar audio visual materials."[92]

---

**91.** ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 27 (1983).

**92.** 18 U.S.C. § 2710(a)(4) (2000).

As another example of sectoral laws confronting convergence, the Children's Online Privacy Protection Act of 1998 (COPPA) regulates the use of children's personal information on the Internet. COPPA assigns enforcement power to the FTC, and this agency has already demonstrated through enforcement actions that COPPA applies to social networking sites that knowingly collect personal information from children without following the statute's requirements.[93] Yet COPPA does not regulate the new digital platforms that are independent of the Internet; it only applies to a "website or online service."[94] Moreover, scattered FTC enforcement actions pursuant to its general statutory authority neither provide comprehensive privacy protections nor completely close gaps in legal coverage.[95]

There is another problem that can follow from telecommunications convergence. A sectoral law might create competitive disadvantages for companies that fall under it and a corresponding subsidy to those outside of its reach. As an example, COPPA is a sectoral law that might bring comparative advantages to an industry that wishes to market to children on new digital platforms that fall outside its jurisdictional sweep.[96] As a further example, federal law regulates the use by telephone companies of a certain kind of customer information, which is termed "Customer Proprietary Network Information" (CPNI).[97] Yet Internet companies do not face analogous

---

**93.** 15 U.S.C. §§ 6501-6506. The two enforcement actions in question were settled in 2006 and 2008 respectively. United States v. Xanga.com, Inc., No. 06 Civ. 6853 (S.D.N.Y. filed Sept. 12, 2006), *available at* http://www.ftc.gov/os/caselist/0623073/xangaconsentdecree_image.pdf; United States v. Industrious Kid, Inc., No. 08-0639 (N.D. Cal. filed Jan. 30, 2008), *available at* http://www.ftc.gov/os/caselist/0723082/080730cons.pdf.

**94.** 15 U.S.C. § 6502(b)(1)(A).

**95.** *See generally* SOLOVE & SCHWARTZ, *supra* note 10, at 803 (describing FTC enforcement actions pursuant to COPPA).

**96.** There has been a dramatic increase in the marketing of food products, frequently unhealthy ones, to children on just such digital platforms. JEFF CHESTER & KATHRYN MONTGOMERY, INTERACTIVE FOOD & BEVERAGE MARKETING: TARGETING CHILDREN AND YOUTH IN THE DIGITAL AGE 13-18 (2007). At the same time, there also has been an increase in the ability of advertisers to track consumers on the Internet and elsewhere and collect personal information about them. JEFF CHESTER, DIGITAL DESTINY 128-38 (2007).

**97.** CPNI consists of personal customer information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier." 47 U.S.C. § 222(h)(1)(A). As the D.C. Circuit explains, CPNI "encompasses customers' particular calling plans and special features, the pricing and terms of their contracts for those services, and details about who they call and when." Nat'l Cable & Telecomms. Ass'n v. FCC, No. 07-0312, 2009 WL 348811, at *1 (D.C. Cir. Feb. 13, 2009). The D.C. Circuit has upheld the FCC's requirement that carriers obtain opt-in consent from a customer before sharing

restrictions on their use of similar customer data. CPNI regulations do not affect how Google uses customer information gathered through its search function, online calendar service, or e-mail service, Gmail. As explained below, however, the flip side of responding to convergence through an omnibus law is that this statute over time may itself become inflexible or ossified.

Finally, an omnibus federal privacy law might lessen the burden of the European regulatory hand on U.S. companies. Here, the Microsoft white paper notes, "[a] U.S. privacy law that is largely compatible with those of other countries would not only help reduce the complexity and cost of compliance, but also promote international business. Such legislation may help reduce barriers to data flowing into the United States."[98] The argument here is that a federal omnibus privacy law would do much, by its form alone, to smooth over differences concerning the critical issue—namely, the EU's regulation of personal data flows into the United States.

The EU Data Protection Directive requires that member states have equivalent data protection law. This requirement has exerted a force for harmonization around omnibus laws in the European Union. As a further requirement in the Directive, member states are only permitted to transfer personal data to nonmember states that have "an adequate level of protection."[99] As already noted, Senator Ervin wanted the United States to refuse to allow transfers of the personal information of U.S. citizens abroad without guarantees that the standards of S. 3418 would be met.[100] The idea of a data embargo on privacy grounds can be said, therefore, to have been first expressed in a U.S. Senate bill in 1974. Yet it was the EU that included a provision that required limits on data exports on privacy grounds in its information privacy laws.

It is hard to know whether the EU might conclude that an omnibus law in the United States adds something substantive to the current mix of information privacy safeguards in this country. Considering its ongoing scrutiny of substantive privacy practices in the United States, the EU may not reverse its "inadequacy" finding for U.S. law, or become more sympathetic to its privacy regime based simply on the form of American legislation. In 1999, the Working Party of EU Data Protection Commissioners found that U.S.

---

personal information with a carrier's joint venture partner or independent contractor in order to market communication-related services to that customer. *Id.* at *7.

**98.** Microsoft White Paper, *supra* note 1, at 5.

**99.** Data Protection Directive, *supra* note 19, art. 25(1), at 46.

**100.** *See supra* text accompanying note 29.

privacy law did not meet the adequacy standard.[101] Article 29 of the Data Protection Directive establishes this group; it is composed of a representative of the supervisory authorities in each Member State and a representative of the European Commission. Among the Working Party's tasks is providing the Commission with opinions on the level of data protection in third countries.[102] Pursuant to this authority, the Working Party stated that the "current patchwork of narrowly focused sectoral laws and voluntary self-regulation" in the United States is not adequate.[103]

Over time, the separate and collective responses by the U.S. government and the EU have provided U.S. businesses with myriad ways to comply with the adequacy requirement. These include (1) a negotiated "Safe Harbor" for companies that follow a set of preapproved regulations that meet the adequacy standard, (2) two sets of EU-approved model contractual clauses for use by American businesses, and (3) a newly streamlined process for approval of Binding Corporate Rules by European Data Protection Commissioners.[104] In addition, there has been an increasingly dense net of sectoral legal protection in the United States. Nonetheless, an omnibus law might add something and, thereby, help smooth the flow of personal information from the EU to the United States. In general, observers expect similar results from systems that share similar organizational forms.[105] Thus, if U.S. law adopted the same form as found throughout the EU, EU regulators might conclude that U.S. information privacy law provided as much protection as their own systems. On the other hand, the EU has already devoted significant resources to assessing information privacy in specific sectors in the United States and may continue with this mode of analysis.

Regarding the weight of the EU's regulatory hand, the United States might secure greater benefits through creation of a federal information privacy agency than adoption of a federal omnibus law. The Data Protection Directive requires

---

101. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, OPINION 1/99 at 2 (1999), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf [hereinafter WORKING PARTY].

102. Data Protection Directive, *supra* note 19, art. 30, at 48.

103. WORKING PARTY, *supra* note 101, at 2.

104. SOLOVE & SCHWARTZ, *supra* note 10, at 1079-80.

105. As a specific example of this phenomenon, the European Commission in 2003 formally found Argentina to have adequate data protection. Its decision was influenced by Argentina's omnibus law. *See* Press Release, European Union, Data Protection: Commission Recognises That Argentina Provides Adequate Protection for Personal Data (July 2, 2003), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/932.

such an independent organization in all EU member states.[106] The EU also has created a Data Protection Supervisor to ensure EU institutions process personal data lawfully, advise EU institutions on all issues with data protection dimensions, and cooperate with other data protection authorities.[107] Canada, Australia, Hong Kong, and Israel are only a few of the other countries that have a national data protection commission.[108] The lack of such an entity in the United States has harmed the continuity of its international privacy policy entrepreneurship. As Newman concludes, the lack of such a regulatory entity in the United States "has unintentionally undermined the power resources available to the United States to promote its interests globally."[109] In 2003, Robert Gellman made a similar point: "In essence, with the international critical mass of data protection agencies that now exists, a country without an agency is at an disadvantage."[110]

*2. Negative Results*

There are three potential problems with a federal omnibus law. These are (1) the costs of an extra layer of regulation, (2) the harms from disregard of the parsimony principle, and (3) the danger of ossification in the federal omnibus law itself. Under federal omnibus legislation, regulated entities would bear the cost of compliance with not only any sector regulation, federal or state, but also the federal omnibus law as it applies to their activities. To some extent FTC enforcement actions are already partial gap-fillers in regulatory coverage, and thereby increase the costs of compliance for private organizations that process personal information.[111] Yet the existing FTC privacy principles are far from comprehensive, and a federal omnibus law will, therefore, add in some fashion

---

**106.** Data Protection Directive, *supra* note 19, art. 28, at 47.

**107.** The EU Data Protection Supervisor was created in 2000. Regulation 45/2001, art. 41, 2001 O.J. (L 8/1) 1. For the home page of the European Data Protection Supervisor, see European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/15 (last visited Feb. 9, 2009).

**108.** For a listing of these agencies, see European Commission, National Data Protection Commissioners, http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited Feb. 9, 2009).

**109.** NEWMAN, *supra* note 6, at 155; *see* Schwartz, *supra* note 19, at 494 (arguing that the lack of an information privacy agency in the United States "handicaps its participation" in important international debates).

**110.** Robert Gellman, *A Better Way To Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1187 (2003).

**111.** *See supra* text accompanying note 95.

to the regulatory weight. At the same time, by leveling the privacy regulatory field, an omnibus law would also ameliorate inconsistencies that flow from convergence.

As for the parsimony principle, it warns against taking action—and especially broad action—under conditions of uncertainty. This principle was at work in 1974 during the debate about S. 3418 and then the Privacy Act. An analogy can also be drawn from environmental law. In this area, Congress has not enacted a federal gap-filling statute modeled on nuisance law. Instead, federal environmental law emerged in targeted areas—through sectoral regulations, as it were—as represented by the Clean Air Act, the Clean Water Act, the Endangered Species Act, and so on. Nuisance law is left as a gap-filler on the state level, where it is left to develop and be applied in a fashion that is attuned to local conditions, including aggregate local policy preferences.

Finally, a federal omnibus law might be difficult to amend. This flaw in a potential omnibus privacy law can be usefully compared to this flaw in the labor law context. Cynthia Estlund has demonstrated how an "ossification" of American labor law has taken place and contributed significantly to its ineffectuality.[112] By ossification, Estlund means a lack of meaningful changes over time within and without the National Labor Relations Act (NLRA) in response to new conditions. As part of her account, she describes the negative consequences of the federal labor statute's broad preemption of state and local law.

The risk of ossification following enactment of a federal omnibus privacy law is also great. Such an omnibus law, like the NLRA, would be difficult to amend—industry, privacy advocates, and other parties may be able to muster enough congressional support to block any significant changes to it.[113] Yet technological change will wreak havoc over time with such a statute's regulatory assumptions, both explicit and implicit. This example illustrates the negative side of the promise of an omnibus law in responding to telecommunications convergence.

In sum, with the issue of preemption off the table, the case for and against a federal omnibus law proves close. As a political reality, however, the issue of preemption cannot be bracketed from the discussion. Without strong preemptive language built around regulatory ceilings, an omnibus privacy bill would face considerable hurdles to enactment. The business coalition in favor

---

112. Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527, 1574 (2002) (offering an especially perceptive account of the way that labor law preemption doctrine has come "untethered from its statutory moorings").

113. *See generally* NEWMAN, *supra* note 6, at 60 (discussing "several institutional veto points" in the federal legislative system, which makes it easy to block legislation).

of the omnibus privacy bill has indicated its strong support for such preemption. As Meg Whitman, President and CEO of eBay, testified before Congress, "Legislation without preemption would make the current situation possibly worse, not better, by creating additional uncertainty and compliance burdens."[114] Indeed, the private sector alliance for privacy legislation is likely to prefer no federal privacy law to one that defers to stronger state privacy laws. Hence, I now turn to the critical issue of the merits of an omnibus privacy law that preempts stronger state privacy statutes.

### *B. Federal Omnibus Privacy Preemption of State Laws*

The standard federalism terminology presents three preemptive possibilities. These are express, field, or conflict preemption.[115] In the area of information privacy, a federal omnibus statute can be expected to involve only conflict preemption.

First, an omnibus privacy law is unlikely to contain an express clause that allows it to preempt *all* state sectoral privacy law. Regulatory chaos would result as hundreds, perhaps even thousands, of more specific state laws fell by the wayside, and courts were obliged to determine how to apply the general provisions of a federal omnibus law to specific situations.

Second, and as a related point, an omnibus privacy law is unlikely to occupy an entire subfield of privacy regulation. After all, such a statute is by definition a general one, and information privacy, moreover, is a subject that touches on many areas. Unlike classic areas for field preemption, such as nuclear safety or alien registration, the federal interest in the regulation of information privacy is not so compelling as to displace all state concerns and state laws on the subject.[116]

Under conflict preemption, a federal law blocks a state statute that frustrates its ends. One can imagine, for example, that a federal omnibus law might cap damages for statutory violations. It might forbid private rights of

---

**114.** *Privacy in the Commercial World II: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 12-13 (2006) (statement of Meg Whitman, President and CEO, eBay Inc.) [hereinafter *Whitman Statement at Commercial Privacy Hearing*].

**115.** *See* Richard A. Epstein & Michael S. Greve, *Introduction: Preemption in Context*, *in* FEDERAL PREEMPTION: STATES' POWERS, NATIONAL INTERESTS 1, 1-5 (Richard A. Epstein & Michael S. Greve eds., 2007).

**116.** *See* Pac. Gas & Elec. Co. v. State Energy Res. Conservation & Dev. Comm'n, 461 U.S. 190, 212-13 (1983); Hines v. Davidowitz, 312 U.S. 52, 67-68 (1941).

action in state law. More generally, an omnibus law might set a series of ceilings above which the states may not regulate.

An omnibus law with such conflict preemption would be a dubious proposition. The two problems with it are its effect on experimentation in federal and state sectoral laws and ossification of the omnibus law itself. The preemptive scope of an omnibus federal privacy law is likely to block new approaches to information privacy in federal and state sectoral laws. Regarding the importance of state law, Martha Derthick has noted, "[s]tate governments are usually first to act in response to new problems or issues, of which many arise in a time of rapid technological and cultural change. It is very rare . . . for the federal government to be the first mover on a domestic question."[117] Such first moves by the states have occurred in the health care area, with state experiments in universal health care insurance, and recently in the reduction of greenhouse gases and other areas of environmental law. This Essay has also examined privacy law innovations in Section I.C.

Note, as well, the healthy choice that both Germany and Canada made to incorporate zones for both federal and state sectoral privacy regulation. In Germany, one such zone reserved for the states is for the protection of the data of insured citizens, including those who receive public support.[118] As Spiros Simitis observes of the shared authority of the federal and state governments in Germany, "[t]he regulation of the processing of personal information is a task that can only be performed by both, and that therefore has from the start demonstrated all the chances and risks of a genuinely federal regulation."[119]

Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), regulates the international collection, use, and transfer of personal information. It also regulates the use of personal information by federal organizations and data flows between Canadian provinces. The provinces are generally reserved the right to regulate other use of personal information. As a substantive safeguard, however, PIPEDA requires that a provincial privacy law displace it only when the provincial

---

**117.** Martha Derthick, *Federalism*, *in* UNDERSTANDING AMERICA: THE ANATOMY OF AN EXCEPTIONAL NATION 121, 140 (Peter H. Schuck & James Q. Wilson eds., 2008).

**118.** The general German terms for this area of regulation are *Sozialordnung* ("social order"), or *Sozialwesen* ("social welfare"). For examples of the data protection issues in this area, see the recent report of the Berlin Data Protection Commissioner. BERLINER BEAUFTRAGTER, BERICHT DES BERLINER BEAUFTRAGTEN FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT [REPORT OF THE BERLIN COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION] 123-56 (2007).

**119.** Spiros Simitis, *Zweck und Andwendungsbereich des Gesetzes* [*Goal and Scope of the Statute*], *in* NOMOS KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [COMMENTARY ON THE FEDERAL PRIVACY LAW], *supra* note 17, at 156 (commenting on Section 1 of the BDSG).

regulation is "substantially similar" to it.[120] PIPEDA does not contain an explicit benchmark regarding the meaning of "substantial similarity," but assigns an important task to the national Privacy Commissioner in making this evaluation. In a report to Parliament, Commissioner George Radwanski has stated that, in the view of his office, substantial similarity means "equal or superior to" PIPEDA "in the degree and quality of privacy protection provided."[121] Lest there be any confusion, the Canadian Commissioner added, "The federal law is the threshold or floor."[122] The Ministry of Industry generally appears to take the same approach.[123] In her contribution to this Feature, Bellia also suggests that states will be subject to a number of federal inputs regardless of the formal existence of a federal statute.[124] These influences include judicial decisions interpreting constitutional provisions. As noted earlier, this point is well taken, and I further develop this theme of regulatory experimentation under decentralization in this Essay's next Part, which concerns federal and state sectoral law.

A second problem with a federal omnibus law would be difficulties in amending it. Here, I return to the risk of ossification in any federal omnibus privacy law.[125] Gridlock can also exist, of course, at the federal and state level for sectoral laws, but these challenges are more likely to be overcome. The next Part addresses this issue.

## III. SECTORAL PRIVACY LAW: LIFE UNDER DEFENSIVE PREEMPTION

Thus far, this Essay has found a mixed case for a federal omnibus law without preemption, and expressed skepticism about such a statute with conflict preemption, which is the form that it is most likely to take. This Part turns to the issue of sectoral privacy law. In my view, there is a role for federal activity in this area, although one cannot state in advance that a federal sectoral law will necessarily be an improvement on the perhaps less tidy results from various state privacy statutes.

---

120. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 § 26(2)(b) (Can.); *see* STEPHANIE PERRIN ET AL., THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT: AN ANNOTATED GUIDE 119 (2001).

121. PRIVACY COMM'R OF CANADA, REPORT TO PARLIAMENT CONCERNING SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION 2 (2002).

122. *Id.*

123. *See infra* text accompanying notes 135-136.

124. *See* Bellia, *supra* note 65, at 875.

125. *See supra* note 112 and accompanying text.

### *A. Federal or State Sectoral Regulation*

Among its problems, a federal omnibus law with conflict preemption would block regulatory experiments in sectoral laws. Yet these disparate statutes often can be improved through a process of ongoing consolidation of their results. As an initial point, I wish to describe this process and explain why this Essay's earlier objections to a federal omnibus law do not apply to sectoral laws, whether state or federal. This Section concludes by discussing why a trend of enacting federal sectoral laws is likely to continue.

States can generate simultaneous experimentation among different policies, but as information is generated about the benefits and costs of these alternatives, the next step, ideally, is a coherent policy implementation of the knowledge gained. In a similar fashion, Feeley and Rubin point to the need to take experimentalism under decentralization seriously.[126] In their view, some degree of centralization is needed to implement the results of experimentalism in a "reasonably effective fashion."[127] It is also important to add that centralizing results from multiple state laboratories of regulation does not necessarily lead to advocacy or creation of federal law.

First, the consolidation process can also take place within states. For example, important California financial privacy regulations originated at the local level, with counties in the Bay Area taking the lead.[128] These laws were then used in drafting S.B. 1, the California financial privacy law. Second, states might organize their own interstate mechanisms for evaluating results of disparate legislation. Possible institutions for such consolidation include the American Law Institute (ALI), the National Conference of Commissioners on Uniform State Law (NCCUSL), and the National Association of Attorneys General (NAAG). The classic example of an ALI process for improving state law is the *Restatement (Second) of Torts*, which sets out Prosser's privacy torts and heavily influences state law.[129] In contrast, NCCUSL and NAAG have not yet been especially influential in privacy law.[130]

---

126. *See* FEELEY & RUBIN, *supra* note 62.

127. *Id.* at 28.

128. Contra Costa County, Cal., Ordinance 2002-30 (Sept. 24, 2002); San Mateo County, Cal., Ordinance 04126 (Aug. 6, 2002).

129. For a selection of cases and a sense of the heavy influence of privacy torts as articulated in the *Restatement (Second) of Torts*, see SOLOVE & SCHWARTZ, *supra* note 10, at 30-140.

130. NAAG PRIVACY SUBCOMMITTEE REPORT: PRIVACY PRINCIPLES AND BACKGROUND, *available at* http://web.archive.org/web/20041216174950/http://www.naag.org/naag/resolutions/subreport.php (last visited Feb. 23, 2009).

What about the consolidation of state legal experiments at the federal level and through sectoral statutes? To a large extent, the arguments *against* a federal omnibus law that includes conflict preemption do not apply to sectoral law. Regarding its impact on state experimentation, a federal sectoral law in the United States is likely to occur subsequently to state sectoral laws because of the slow and sometimes difficult process of enacting federal legislation.[131] Indeed, assuming a similar pace of lawmaking among Congress and the states, there would be a random distribution of final legislative results among all the entities. The consequence would be that one or more of the fifty states would be likely to act before the federal government.

Moreover, in areas in which federal privacy law does not shut the door on further state activity, the states are likely to continue lawmaking. It is not only that state sectoral laws often will precede federal sectoral law in the United States, but also that state lawmakers will act in reaction to federal activity when it occurs, and a process of experimentation, drawing on involvement by advocacy groups and other stakeholders, will continue.[132] In addition, state government involvement in lawmaking increases the number of independent observations and the likelihood of deviations from the mean.[133]

Recent developments in Canadian information privacy law provide an illustration of this point. Important forces behind the enactment of PIPEDA, the federal Canadian privacy law, include the EU Data Protection Directive's "adequacy" standard, Canadian industry's drafting of an information privacy code for itself that it was able to incorporate into PIPEDA, and industry's awareness that it was increasingly subject to a variety of sometimes differing sectoral privacy laws in the provinces.[134] In addition, and as noted above, PIPEDA allows itself to be displaced by provincial laws that are "substantially similar" to it.[135] PIPEDA assigns authority to make this finding to the Governor in Council, legal adjunct to the federal cabinet, with recommendations from

---

**131.** For one illustration, contrast the quick reaction in Vermont in 1992 to certain credit reporting mistakes in the state the year before, and the slower reaction in Washington, D.C., which ultimately led in 1996 to certain amendments to the Fair Credit Reporting Act. *See* Michael Epshteyn, Note, *The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers?*, 93 GEO. L.J. 1143, 1162-63 (2005).

**132.** *See* Michael W. McConnell, *Federalism: Evaluating the Founders' Design*, 54 U. CHI. L. REV. 1484, 1498 (1987) (book review) ("Lower levels of government are more likely to depart from established consensus simply because they are smaller and more numerous.").

**133.** *Id.*

**134.** PERRIN ET AL., *supra* note 120, at 2-11.

**135.** *See supra* text accompanying note 120.

the Ministry of Industry and the Privacy Commissioner of Canada.[136] Thus far, this process has led to exemptions for all three of the provinces with omnibus privacy laws for the private sector. These provinces are Quebec, British Columbia, and Alberta. The omnibus privacy law in Quebec was enacted before the PIPEDA, and those in British Columbia and Alberta subsequent to it.[137] A sectoral privacy law for health information in Ontario that came into force in 2004 has also been found to meet PIPEDA's standards, and thus "health information custodians" in that province are exempt from the application of PIPEDA.[138]

PIPEDA offers a path to harmonize different state laws while also leaving room for continuing state government inputs into information privacy lawmaking. By allowing exemptions for "substantially similar" provincial laws, PIPEDA provides incentives for the state to enact omnibus and sectoral laws that follow its approach. More subtly, it also permits a way for innovations at the state level to be incorporated into it. PIPEDA's section 29 calls for a parliamentary review of the Act every five years.[139] In May 2007, a committee of the Canadian House of Commons provided recommendations from the first such statutory review.[140] Perhaps the most striking aspect of this report is the broad consensus about drawing on lessons from provincial laws in considering amendments to and alterations in PIPEDA. As the committee stated, "[W]e heard from privacy advocates, academics, business and industry organizations, as well as from the Federal Privacy Commissioner, that reference should be made to these provincial laws when making changes to PIPEDA."[141] Special attention in the ensuing recommendations was paid to the private sector data protection laws of Alberta and British Columbia.[142] These were considered to

136. Personal Information Protection and Electronic Documents Act: Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, C. Gaz., pt. I, at 3618-22 (Sept. 22, 2001) (Can.); PRIVACY COMM'R OF CANADA, *supra* note 121, at 1-2.

137. BARBARA MCISAAC, RICK SHIELDS & KRIS KLEIN, THE LAW OF PRIVACY IN CANADA 4-27 (rev. ed. 2006); STANDING COMM. ON ACCESS TO INFO., PRIVACY AND ETHICS, STATUTORY REVIEW OF PIPEDA 3 (2007) [hereinafter STANDING COMM. REPORT].

138. MCISSAC ET AL., *supra* note 137, at 4-27 to 4-28.

139. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 § 29 (Can.).

140. STANDING COMM. REPORT, *supra* note 137.

141. *Id.* at 1.

142. *Id.* at 47-51.

be important as "second generation" statutes that had been enacted subsequently to PIPEDA as well as the Quebec statute.[143]

In the United States, interplay between federal and state governments as well as with other entities is already observable in environmental law. As scholars in this field have explored, this interplay can take a number of forms. For example, Ann Carlson talks about "iterative federalism," in which the federal government allows one state, in the role of a "super-regulator" to have special power.[144] I return to this idea below. More broadly, Jody Freeman and Daniel Farber have developed a "modular" conception of environmental regulation based on their examination of the CalFed Bay Delta program.[145] In modular environmental regulation, decisionmakers at the federal and state levels share power through a mix of formal and informal tools for implementation of policy goals.

Although rare for the federal government to be a first mover on a domestic privacy issue, as Bellia indicates, such behavior can occur.[146] As an example in the privacy area, the VPPA demonstrates Congress's quick action after the publication of information about Judge Robert Bork's video rental records. This example provides an interesting case study of a privacy horror story with a uniquely federal aspect as well as a historical moment when preemption was not on the radar of the concerned industry.

Immediately before the passage of the VPPA, Judge Bork had been mired in controversial congressional confirmation hearings regarding his ultimately unsuccessful nomination for the Supreme Court. Ironically enough, one of the issues during the confirmation hearings had been the extent of Judge Bork's view of the constitutional dimensions of privacy.[147] There was bipartisan

---

**143.** *Id.* at 1.

**144.** Ann E. Carlson, *Iterative Federalism and Climate Change*, 103 NW. U. L. REV. (forthcoming June 2009) (manuscript at 12, on file with author).

**145.** Jody Freeman & Daniel A. Farber, *Modular Environmental Regulation*, 54 DUKE L.J. 795 (2005).

**146.** Bellia, *supra* note 65, at 881-86.

**147.** Judge Bork did not think that the Constitution contained a right to privacy. The confirmation hearings did not, however, turn on whether Congress had a right to legislate in this area. *See Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the H. Comm. on the Judiciary and the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary*, 100th Cong. 133-34 (1988) (statement of Sen. Alan K. Simpson) [hereinafter *Video Privacy Hearings*] ("As Judge Bork so articulately pointed out during his hearings, the Congress of the United States does have the power to legislate privacy rights if it wishes."); *id.* at 67 (statement of Janlori Goldman, Staff Attorney, Am. Civil Liberties Union) ("[T]he

agreement, however, regarding the outrageous nature of the violation of Judge Bork's own privacy by a Washington weekly's article on his video rentals. Senator Patrick Leahy expressed this outrage in the hearings on the Act:

> I well remember when Senator Al Simpson came before the committee during the Bork hearings and announced what happened. That committee, as you know, was split between those supporting Judge Bork and those opposed to him. But it was unanimous—the feeling across the committee of outrage—when we learned of the disclosure.[148]

Congress's rapid enactment of the VPPA was an exercise in unanimity at a time when the Bork nomination was dividing it and the nation. As it entered new legislative territory with the VPPA, Congress wisely chose not to preempt future state sectoral laws that offer stronger protections.[149]

From today's perspective, it is interesting to revisit this legislative choice. The legislative history of the VPPA is almost entirely devoid of references to preemption, apart from perfunctory mentions that the law would not preempt stronger state statutes.[150] Most telling, the joint hearing on the statute included no discussion of preemption. To be sure, there were contentious issues aired that day. The joint hearing involved a vigorous discussion of whether or not the proposed statute should include protection for library records, and such coverage, initially included in the House and Senate bills, was dropped from the final Act.[151] Another heated discussion at the hearing concerned the extent to which the Act would change practices of the direct mailing industry.[152] The Act as enacted allows marketing directly to consumers based on general subject matter categories of videos rented, but also requires that consumers be given

majority of Senators who voted against his confirmation cited their concern about the Judge's limited view of the Constitutional right to privacy.").

148. *Id.* at 31 (statement of Sen. Patrick Leahy).

149. 18 U.S.C. § 2710(f) (2000).

150. For such a brief reference, see S. REP. NO. 100-599, at 15 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-12.

151. *See id.* at 8, *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-8 (noting that the Subcommittee "was unable to resolve questions regarding the application" of a provision on disclosure of "library borrower records"). For the discussion of the protection of library records at the hearing, see *Video Privacy Hearings*, *supra* note 147, at 34-53.

152. *See Video Privacy Hearings*, *supra* note 147, at 87-114 (statement of Richard A. Barton, Senior Vice President, Direct Mktg. Assoc.).

the chance to prohibit such marketing.[153] It was felt that this approach would be generally consistent with marketing practices at the time.[154]

The hearings also provide hints regarding the grounds for the lack of interest in preemption. As testimony at the hearing indicated, the majority of the video rental industry in 1988 consisted of "small, one-owner operations."[155] Blockbuster and other large chains did not yet exist, and Netflix was not yet even a gleam in the eye of some entrepreneur or venture capitalist. Thus, the then-existing video rental industry, based around mom-and-pop stores, did not view preemption as a significant issue because so many of its retail outlets were in a single location with customers in that same geographic entity.[156] In this regard, the nature of the most affected industry at that time made it easy for Congress to structure this privacy legislation without preemption.

As for ossification, federal sectoral law runs this risk to a considerably lesser extent than an omnibus law. As an example at the federal level, the credit reporting industry is large, but far smaller, of course, than the entire private sector. And the emergence of new factors, such as identity theft, a high public interest in the issue, and a strategic use of sunset provisions in previous legislation, led in 2003 to the enactment of FACTA, which amended the Fair Credit Reporting Act. Many new problems had arisen since the last major amendment of the Fair Credit Reporting Act, which was in 1996.

Two of the most important of these problems concerned the explosion in identity theft and an increase in "risk-based" pricing, which raises or lowers the cost of borrowing based on one's credit score.[157] To help prevent identity theft, FACTA granted consumers the ability to add fraud alerts to their files at national consumer reporting agencies.[158] It also simplified this process by allowing consumers to inform just one agency, which is then required by law

---

**153.** 18 U.S.C. § 2710(b)(2)(D)(i)-(ii); *see* S. REP. NO. 100-599, *supra* note 150, at 13-14.

**154.** *See Video Privacy Hearings*, *supra* note 147, at 88-89 (statement of Richard A. Barton, Senior Vice President, Direct Mktg. Assoc.).

**155.** *Id.* at 125.

**156.** Indeed, preemption was not even on the radar of the nation's then-largest video retailer, Erol's, which had some multi-state operations. A representative of Erol's testified before Congress strongly in favor of the Video Privacy Protection Act and did not raise the preemption issue. *Id.* at 76-86 (statement of Vans Stevenson, Dir. of Pub. Relations, Erol's, Inc.).

**157.** *See* Epshteyn, *supra* note 131, at 1154-55 (describing the rise of identity theft after the enactment of the original Fair Credit Reporting Act); Gail Hillebrand, *After the FACTA: State Power To Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. 53, 56-57 (2004) (discussing the use of "risk-based" pricing to determine the "nuances and gradations in price and terms" of consumer credit).

**158.** 15 U.S.C. § 1681c-1(a) (Supp. V 2005).

to inform the other credit reporting agencies.[159] As noted above, moreover, FACTA also requires the FTC and banking agencies to issue so-called "Red Flag" rules.[160] As a final example regarding identity theft, businesses are to truncate credit and debit card numbers on electronically printed receipts and are forbidden from printing the card's expiration date on a receipt.[161] A receipt with such information on it represented one stop shopping for an identity thief.

As for the "risk-based" provision of credit, FACTA requires notice to the consumer when material terms of credit are less favorable than the most favorable terms available to a "substantial proportion" of consumers.[162] This information allows the consumer to know that she is receiving terms that are less favorable than those offered to others. It will thereby motivate investigations of accuracy in credit scoring. And FACTA also permits consumers to receive a free credit report as well as their credit score "for a reasonable fee."[163] Here, too, the idea is to increase the transparency for consumers of the credit industry.

Overall, federal sectoral law can have the potential to build on the results of state law. The devil is in the details, however, and one cannot state at an abstract level that a federal sectoral law is necessarily preferable to the messier universe of different and unconsolidated state sectoral statutes. Whether one is a privacy advocate or skeptic, history teaches that the federal government and the states may switch back and forth in their concern for and level of attention to this issue. As Lynn Baker and Ernest Young warn concerning institutional aspects of federalism, it is risky to make structural decisions about allocating power "based on predictions that any particular group will continue to dominate a particular portion of the government for long."[164] One cannot be confident in a given policy result reached by reliance on a federal as opposed to state regulatory process, or vice versa.[165] Change will be a constant with ongoing shifts in alignments, whether among branches of the federal government, or between the federal and state levels. Amidst the change, one

---

159. *Id.* § 1681c-1(e).

160. *See supra* text accompanying note 84.

161. 15 U.S.C. § 1681c(g).

162. *Id.* § 1681m(h).

163. *Id.* §§ 1681j(a), 1681g(a); *see* Hillebrand, *supra* note 157, at 65-66.

164. Lynn A. Baker & Ernest A. Young, *Federalism and the Double Standard of Judicial Review*, 51 DUKE L.J. 75, 151-52 (2001).

165. Even though Baker and Young favor state lawmaking, they also concede that "increased diversity [in legislation] among the states is not always a good thing." *Id.* at 155.

contribution that scholars can nonetheless make is to identify at least general circumstances under which federal sectoral law is likely to bring benefits. The next and final Section takes up this task.

An additional point should be made about federal versus state sectoral privacy in the United States regarding a certain reality of regulatory life. Good, bad, or indifferent, sectoral privacy law at the federal level is not only here to stay, it constitutes a future growth field. In a classic paper from 1985, E. Donald Elliott, Bruce Ackerman, and John Millian proposed an evolutionary model of statutory law.[166] In their paradigm, an important middle period in the regulatory lifecycle involves the flight by regulated entities to Washington, D.C., in search of relief. These entities seek to counter organizational successes for advocacy groups at the state level by seeking preemptive lawmaking at the federal level. J.R. DeShazo and Jody Freeman later termed this phenomenon "defensive preemption."[167] As DeShazo and Freeman point out, state-level regulations can unnerve industry and prompt its demand for federal preemptive lawmaking.[168]

This description accurately captures the unfolding dynamic in the policy arena for information privacy. There has been a noticeable lack of gridlock at the state sectoral level. The website of the California Office of Information Security and Privacy Protection displays an impressive list of privacy legislation enacted in 2008 alone or currently pending.[169] Among the recent legislation are statutes that make it a misdemeanor to eavesdrop intentionally on Radio Frequent Identification devices, that increase penalties for hospital employees that snoop through medical records, and that simplify the procedures for consumers to place a security freeze on their credit files.[170] An interesting regulatory lever has been the public's strong interest in privacy. This interest has been reflected in countywide privacy regulations—such as northern California's financial privacy ordinances—and a successful use of a privacy

166. E. Donald Elliott, Bruce A. Ackerman & John C. Millian, *Toward a Theory of Statutory Evolution: The Federalization of Environmental Law*, 1 J.L. ECON. & ORG. 313 (1985).

167. J.R. DeShazo & Jody Freeman, *Timing and Form of Federal Regulation: The Case of Climate Change*, 155 U. PA. L. REV. 1499, 1500 (2007).

168. *See id.* at 1530.

169. California Office of Information Security and Privacy Protection, 2008 Privacy Legislation Enacted, http://www.oispp.ca.gov/consumer_privacy/privacy_leg/leg.asp (last visited Dec. 1, 2008).

170. *Id.*

referendum in North Dakota and the threat of such a referendum in California.[171]

Like environmental law, privacy is also an attractive area for politicians and private advocates seeking a field for policy entrepreneurship. Regarding politicians, Regan in 1995 identified a number of factors that affected the willingness of members of Congress to assume policy leadership in privacy issues. For our purposes, it is of greatest significance that any initial interest and attention is only sustained, in Regan's analysis, when there is continuing visibility for the privacy issue and continuing media interest in it.[172] These conditions are more than present today. Concerning private organizations, Colin Bennett has noted that "the number of groups engaged in privacy advocacy has increased dramatically during the last ten to fifteen years."[173] He also finds that privacy is also now "on the agendas of an increasing number of more established groups."[174] He attributes this increase in advocacy organizations for privacy to the rise of the Internet, the new variety and pervasiveness of technologies of surveillance, and the international nature of flows of personal information.[175]

Thus, gridlock has not kept states from enacting privacy statutes. States are also not competing for business with each other by failing to regulate privacy with sufficient rigor. There certainly has been no race to the bottom, which also has been termed the "race of laxity."[176] In the context of environmental law, there is a rich scholarly debate regarding whether or not states have competed to offer weaker regulatory regimes to curry favor with business.[177] In the area of information privacy, there is scant room for such a debate. Even if there is no indication of a race to the top, states are far from enacting successive waves of information privacy statutes with weaker protections for consumers and more favorable conditions for businesses. In other words, California

---

171. Adam Clymer, *North Dakota Tightens Law on Bank Data and Privacy*, N.Y. TIMES, June 13, 2002, at A28; Jennifer 8. Lee, *California Law Provides More Financial Privacy*, N.Y. TIMES, Aug. 28, 2008, at A24.

172. REGAN, *supra* note 40, at 202-09.

173. COLIN J. BENNETT, THE PRIVACY ADVOCATES 59 (2008).

174. *Id.*

175. *Id.*

176. ZYGMUNT J.B. PLATER ET AL., ENVIRONMENTAL LAW & POLICY 296 (3d ed. 2004).

177. *See, e.g.*, Kirsten H. Engel, *State Environmental Standard-Setting: Is There a "Race" and Is It "to the Bottom"?*, 48 HASTINGS L.J. 271 (1997); Richard L. Revesz, *The Race to the Bottom and Federal Environmental Regulation: A Response to Critics*, 82 MINN. L. REV. 535 (1997); Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210, 1211-12 (1992).

privacy initiatives have not encouraged Nevada or other states, neighboring or otherwise, to enact weaker regulations in the same area. At any rate, state legislative activities will continue and will drive a flight by businesses to Washington for federal solutions. Over the next decade and beyond, continuing waves of state privacy lawmaking will provoke industry activity to seek federal legislation.

### *B. A Dual Federal-State System for Information Privacy*

Due to the regulatory dynamic that this Essay has described, there will be both federal and state privacy legislation in the years to come. As a consequence, there is a need to think critically about life under defensive preemption. In taking such a step, this Essay assesses three aspects of regulatory life under a dual federal-state system for information privacy law. First, there is value in identifying circumstances in which federal consolidation of state law will likely be useful. Second, there is need to consider points beyond the usual debate about floors and ceilings. Third, Congress may prove more enthusiastic regarding broad federal preemption than this Essay generally favors, and in those cases, second-best legislative solutions should accompany preemption.

#### *1. Federal Consolidation*

I now consider two ways in which consolidation of different state laws in the area of information privacy would bring benefits: (1) through the avoidance of inconsistent regulations, especially in areas with high costs and little policy payoff, and (2) through the establishment of "field definitions" that can lower compliance costs.

As for avoiding inconsistent regulation, certain regulations entail costs with scant privacy benefits. For example, Massachusetts has a law that blocks breach notices from including information about the breach incident.[178] In their respective statutes, other states require disclosure of precisely such information.[179] In addition, the triggers for notification in different states

178. MASS. GEN. LAWS ch. 93H, § 3 (2007).

179. *Compare id.* ("The notice to be provided to the resident . . . shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use."), *with* N.Y. GEN. BUS. LAW § 899-aa(7) (McKinney 2005) ("[N]otice shall include . . . a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of

differ—and sometimes in idiosyncratic ways.[180] An obligation to inform a consumer can follow from the acquisition of information by an unauthorized person when there is a breach that poses a significant risk of identity theft, when there has been a reasonable likelihood of illegal use of the information, or when there has been a "material risk of identity theft or other fraud to the resident."[181] The universe of choices might easily be standardized into a menu of three categories with scant loss of substantive regulatory variety.

A second benefit of consolidation concerns basic statutory definitions that mark a given regulatory field. The preemptive power of such a "field definition" prevents states from redefining the scope of a fundamental legislative category. As an example, the Fair Credit Reporting Act contains a detailed definition of "consumer report."[182] Congress was wise to enact such basic subject matter definitions; terms that clearly bound the scope of a regulatory field reduce regulatory transaction costs. Note, however, that as technology and businesses evolve, entire new enterprises and modes of data processing may spring up. In that case, states are free to generate a new category or categories for regulation.

### 2. *Beyond Ceilings and Floors*

The debate in information privacy law frequently centers on the merits of ceilings versus floors in federal legislation. As an international example, the Canadian Privacy Commissioner indicated his view in 2002 that PIPEDA sets a floor that only permits certification of state laws that offer equivalent or greater privacy protection.[183] The Department of Industry, which also plays an important role in a certification of provincial law as "substantially similar," has issued a notice of its process that indicates a similar view. In particular, the Department requires provincial legislation to incorporate the ten privacy principles of PIPEDA, provide for independent and effective privacy oversight,

personal information and private information were, or are reasonably believed to have been, so acquired.").

180. *See, e.g.*, Schwartz & Janger, *supra* note 56, at 942-43.

181. For a table with a detailed comparison of different state security breach notification laws, see *id.* at 972-84.

182. 15 U.S.C. § 1681a(d) (2000 & Supp. V 2005).

183. *See supra* text accompanying note 121.

and restrict the use of personal information to purposes that are "appropriate or legitimate."[184]

Despite the useful Canadian example, in my view, the debate about ceilings and floors in information privacy law cannot be resolved in advance and at a general level. As William Buzbee notes with a focus on environmental law, "[p]reemption choice . . . must turn largely on the nature of the regulatory task involved."[185] This debate regarding information privacy law also cannot be resolved in advance of a specific regulatory context. Nonetheless, there are important subjects beyond ceiling and floors, and a scholarship of information privacy regulation can contribute to these areas. In this light, I wish to concentrate on two points: the benefits of narrowing ceilings to only the conduct regulated, and sharing of enforcement authority among federal and state regulators.

Even when there is a strong argument for uniformity of regulatory action, and, hence, a federal ceiling, there are merits to narrowing the ceiling to specific conduct rather than the entire subject matter. The benefit of such preemption for conduct is to create an element of certainty for regulators and regulated entities while also leaving open the possibility for future regulatory innovations by the state. FACTA leads the way in showing how to limit a ceiling preemption.

To be sure, FACTA contains numerous examples of subject matter preemption.[186] Yet it also involves some preemption limited to required conduct; this preemption restricts the assignment of federal power to the behavior mandated. For example, as noted above, FACTA requires consumer reporting agencies to place fraud alerts on consumer credit files under certain circumstances.[187] In so doing, FACTA streamlines one area of industry procedures; at the same time, it allows states to engage in further regulation regarding the larger subject area, which is identity theft.

As a further matter, there is a strong argument for sharing enforcement authority among federal and state regulators. As Roderick Hills suggests, "The benefits of federalism in the present and in the future will rest on how the federal and state governments interact, not in how they act in isolation from

---

**184.** Personal Information Protection and Electronic Documents Act: Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, C. Gaz., pt. I, at 3621-22 (Sept. 22, 2001) (Can.).

**185.** William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1602 (2007).

**186.** 15 U.S.C. § 1681t.

**187.** *Id.* § 1681c-1. The preemption narrowed to "the conduct required" is codified at 15 U.S.C. § 1681t(b)(5).

each other."[188] FIPs should also take into account such interactions, and hence, demand attention to the conditions of joint federal-state governance. Information privacy standards require contributions by different federal and state government agencies, the private sector, advocacy groups, individual citizens, and the judiciary in ongoing deliberations. FIPs should not end the question of how to regulate a specific area of information privacy, but instead should begin a process of debating privacy norms and negotiating regulatory content.[189]

The problem with a monopoly on enforcement given to federal agencies is that it would assign these organizations too large a role in the regulatory dialogue. Federal preemption of statutory regulatory authority would also burden a handful of federal agencies with an impossibly large regulatory role in light of their limited resources and myriad other responsibilities.[190] In contrast to this view, the industry coalition in favor of federal privacy legislation, in addition to its support for preemption, opposes private rights of action. In her congressional testimony, for example, Meg Whitman termed a private right of action "counterproductive" and warned against companies being "brought to their knees" by class-action lawsuits.[191]

In an absence of private rights of action, however, there is likely to be significant underenforcement of privacy interests. As an illustration, the Federal Trade Commission—which Meg Whitman in her testimony singles out for an enforcement role—includes privacy as only one of its regulatory tasks, along with antitrust, mergers, and consumer protection issues other than privacy. It has already taken on a significant privacy enforcement role under the Children's Online Privacy Protection Act of 1998 as well its own power to stop "unfair or deceptive acts or practices in or affecting commerce."[192] An exclusive statutory grant of additional privacy authority to the FTC is not likely to cause much, if any, additional enforcement.

---

**188.** Roderick M. Hills, Jr., *Against Preemption: How Federalism Can Improve the National Legislative Process: Cyberspace Filters, Privacy Controls, and Fair Information Practices*, 82 N.Y.U. L. REV. 1, 4 (2007).

**189.** *See* Schwartz, *Lessig's Code*, *supra* note 15, 781-86.

**190.** A range of other issues also arise in any division and sharing of power, including the question of choice of judicial fora for hearing claims.

**191.** *Whitman Statement at Commercial Privacy Hearing*, *supra* note 114, at 13, 37.

**192.** 15 U.S.C. § 45(a)(1). For a discussion of the FTC's enforcement powers under its enabling act and its use in the context of children's online privacy, see SOLOVE & SCHWARTZ, *supra* note 10, at 777-82, 803.

### 3. *Second-Best Solutions*

I wish to conclude by acknowledging that Congress may sometimes manifest a taste for broad sectoral preemption.[193] As a second-best solution, this Essay therefore advocates that Congress draw on two additional policy safeguards. First, Congress should consider the usefulness of a unitary sectoral preemption "plus one" strategy. This idea is inspired by the Clean Air Act's regulation of pollution from mobile sources; it sets a federal ceiling, but allows a single state, California, to exceed federal emission standards.[194] Other states are permitted to follow the California approach, but they may not enact customized standards. Carlson terms a state that federal law singles out in such a fashion as a "super-regulator."[195]

If a federal sectoral privacy law chooses the path of broad preemption, Congress should allow at least a single state to keep its higher standards or develop different standards. This state should have bureaucratic expertise in the area, represent a large market in the chosen sector of regulation, and have a citizenry and advocacy organizations involved in the issue. Instead of the "plus one" strategy, however, federal law sometimes simply grandfathers in states with sectoral privacy regulation. For example, FACTA provides exceptions to one of its preemptive ceilings for California and Massachusetts.[196] While the approach rewards the states that beat Congress to the regulatory punch, it cuts off the possibility that other states will be able to make choices in a marketplace of regulatory models.

As a second fallback proposal, preemption clauses in federal privacy legislation should be subject to a ten-year sunset to allow Congress to evaluate information about the successes and failures of federal regulation. There is already a past example of such a sunset in substantive information privacy law. Amendments in 1996 to the Fair Credit Reporting Act contained sunsets for a number of statutory provisions that affected billions of dollars in commercial transactions.[197] With the expiration of these statutory sections imminent, industry was forced to the congressional bargaining table, and at a time when

---

193. Regarding this trend in areas other than information privacy law, see Buzbee, *supra* note 185, at 1552–55.

194. 42 U.S.C. §§ 7507, 7543(e).

195. Carlson, *supra* note 144 (manuscript at 1).

196. 15 U.S.C. § 1681t(b)(1)(F).

197. EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS 307–08 (2d ed. 2005). For a skeptical view of the industry's assessment of the cost of letting the preemption of these provisions lapse, noting the historic absence of a single nationwide market for credit reporting, see Epshteyn, *supra* note 131, at 1161.

the public had a growing awareness of the shortcomings of existing regulations and new information about the harms from identity theft and risk-based credit. The result was the enactment of FACTA, which—although imperfect—added important new protections to the Fair Credit Reporting Act. Creating sunsets for preemptions has the additional merit of forcing Congress to reassess the wisdom of its assertion of regulatory primacy. It schedules a revisiting of regulatory choices and thereby creates a safeguard against regulatory ossification.

## CONCLUSION

A federal omnibus information privacy law with strong preemption provisions would be an unfortunate development. It would limit further experimentation in federal and state sectoral laws. Such a law also would be difficult to amend, and would, therefore, become outdated as technological changes undermine such a statute's regulatory assumptions.

In contrast, federal sectoral privacy law presents a more complicated situation. One cannot state in advance that a federal sectoral law will necessarily be an improvement on the results of various state privacy statutes. It is clear, nonetheless, that federal sectoral privacy law will be a growth field in the next decades. State innovations in the information privacy field are also likely to provoke industry lobbying for federal responses. There will likely be many attempts, including some successful ones, at defensive preemption in federal sectoral privacy law.

A dual system of federal and state sectoral regulation has both promise and peril. This Essay provides new categories for classifying and encouraging federal and state inputs into information privacy law. Federal consolidation of state privacy laws can provide benefits by avoiding inconsistent regulations, especially in areas with high costs and little positive policy results, and by establishing basic regulatory categories. It is also important to work with concepts beyond the classic preemptive categories of "floors" and "ceilings." One such concept concerns the possibility of limiting ceiling preemption only to certain specific conduct rather than an entire subject matter. In 2003, FACTA demonstrated the feasibility of such an approach to the jurisprudence of preemption.

Even when Congress manifests a preference for broad sectoral preemption, certain second-best solutions are available. The first of these is to adopt a "plus one" strategy. In this approach, states can choose either a federal standard or that of a single state with different standards. A second fallback proposal is to subject preemption clauses in federal information privacy statutes to a ten-year sunset to allow for feedback regarding the performance of federal regulation.

The ultimate task of a dual system for federal and state information privacy law is to develop mechanisms for weeding out policies that fail and for promoting the successes.

Forthcoming, Stanford Law Review, vol. 63 (2010)
Draft of 3/10/10

# PRIVACY ON THE BOOKS AND ON THE GROUND

Kenneth A. Bamberger* & Deirdre K. Mulligan**

*Abstract*

*U.S. privacy law is under attack. Scholars and advocates criticize it as weak, incomplete, and confusing, and argue that it fails to empower individuals to control the use of their personal information. The most recent detailed inquiry into corporate treatment of privacy, conducted in 1994, frames these critiques, finding that firms neglected the issue in their data management practices because of the ambiguity in privacy mandates and lax enforcement. As Congress and the Obama Administration consider privacy reform, they encounter a drumbeat of arguments favoring the elimination of legal ambiguity by adoption of omnibus privacy statutes, the EU's approach.*

*These critiques present a largely accurate description of privacy law "on the books." But the debate has strangely ignored privacy "on the ground"—since 1994, no one has conducted a sustained inquiry into how corporations actually manage privacy, and what motivates them. This omission is especially striking because the neglect of the 90s has been replaced by a massive dedication of corporate resources to privacy management, the inclusion of privacy officers at the c-suite level, and the employment of a 6,500-strong cadre of privacy professionals.*

*This Article presents findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with Chief Privacy Officers identified by their peers as industry leaders. Spurred by these findings, we present a descriptive account of privacy "on the ground" that upends the terms of the prevailing policy debate. Our alternative account identifies elements neglected by the traditional story—the emergence of the Federal Trade Commission as a privacy regulator, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—and traces the ways in which these players supplemented a privacy debate largely focused on processes (such as notice and consent mechanisms) with a growing corporate emphasis on substance: preventing violations of consumers' expectations of privacy.*

*Two alterations to the legal landscape contribute to this definitional shift. First, the substantive definition tracks the emergence of the FTC as a roving regulator with broad yet ambiguous power to evaluate privacy practices in the marketplace through its consumer protection lens. The FTC's mandate to protect consumers from "unfairness" and "deception" permits dynamic regulation that evolves with changing contexts, and forces corporate practices to develop accordingly. Second, state security breach notification laws raised the soft and hard costs of mismanaging personal information. Together these changes led companies to integrate substantive considerations of consumers' privacy expectations into their workflows, rather than leaving privacy to the lawyers and their process-based "click through if you 'consent' to the privacy policy" approach.*

*Our grounded account should inform privacy reforms. While we have no truck with efforts to expand procedural mechanisms to empower individuals to control their personal information, doing so in a way that eclipses robust substantive definitions of privacy and the protections they are beginning to produce, or constrains the regulatory flexibility that permits their evolution, would destroy important tools for limiting corporate over-reaching, curbing consumer manipulation, and protecting shared expectations about the personal sphere on the Internet, and in the marketplace.*

---

* Assistant Professor of Law, University of California, Berkeley, School of Law (Boalt Hall).
** Assistant Professor, University of California, Berkeley, School of Information.

# PRIVACY ON THE BOOKS AND ON THE GROUND

Kenneth A. Bamberger* & Deirdre K. Mulligan**

TABLE OF CONTENTS



* Assistant Professor of Law, University of California, Berkeley, School of Law (Boalt Hall).

** Assistant Professor, University of California, Berkeley, School of Information.

This project has been funded by the Rose Foundation for Communities and the Environment Consumer Privacy Rights Fund, and by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422). We are extremely appreciative for critical assistance from Jen King and David Thaw; for important feedback from Catherine Albiston, Anita Allen, Colin Bennett, Beckwith Burr, Mary Culnan, Lauren Edelman, Chris Hoofnagle, Bob Kagan, Colin Koopman, David Medine, Maryanne McCormick, Helen Nissenbaum, Richard Purcell, Ira Rubinstein, Pamela Samuelson, Jason Schultz, Ari Schwartz, Paul Schwartz, Jeff Sovern, Peter Swire, Eric Talley, and other participants in workshops at the 2009 Privacy Law Scholars Conference, the UC Berkeley Center for the Study of Law and Society, the University of San Diego Law School, and the NYU School of Law Information Law Institute; and for excellent research assistance by April Elliot and Andy Weiner.

# PRIVACY ON THE BOOKS AND ON THE GROUND

## INTRODUCTION

Fifteen years ago, management scholar H. Jeff Smith released a landmark study of corporate privacy practices,[1] and his conclusions were grim. In the seven corporations studied, the privacy arena was marked by systemic inattention, and lack of resources. "[P]olicies in important areas" were "non-existent," and those that existed were not followed in practice.[2] Executive neglect signaled to employees that privacy was not a strategic corporate issue. Privacy decisions were left to mid-level managers who lacked substantive expertise, played "particularly subservient roles in most privacy discussions"[3] and responded, piecemeal, to issues as they arose. Privacy considerations were particularly absent in decisions about technological or business developments; in the words of one mid-level manager, "[t]he top executives rarely ask for [privacy] policy implications of . . . new uses of information. If anybody worries about that, it's my [mid-level] colleagues and myself. And we don't usually know the right answer, we just try something."[4]

Smith attributed these failures to "ambiguity" regarding the legal meaning of privacy and the requirements governing its protection in the context of corporate data management.[5] In the face of this ambiguity corporate executives avoided action unless external parties demanded specific new policies and practices, a tendency exacerbated because privacy was viewed as a goal in tension with core operational aims—an organizational phenomena exacerbated by the inherent secrecy around corporate data management.

These findings led Smith to conclude that remedying the problem of corporate inattention to privacy concerns required a "systemic fix,"[6] reflecting an ongoing credible threat of either consumer backlash or government scrutiny. More concretely, he argued, the primary objective of regulatory intervention must be "the reduction of ambiguity in the U.S. privacy domain."[7] In light of these objectives—comprehensive, credible and unambiguous external mandates—Smith advocated a suite of reforms reflecting elements of the European approach to privacy protection.[8] He called for the adoption of a uniform

---

[1] H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA (1994).

[2] *Id.* at 4 (documenting "a persistent policy/practice gap").

[3] *Id.*

[4] *Id.* at 82.

[5] *See id.* at 139; ch. 5.

[6] *Id.* at 207.

[7] Id. at 213; *see id.* at ch. 6 (describing "Ambiguity All Around").

[8] Specifically Smith recommended a Data Protection Board with advisory powers to assist corporations in developing codes of acceptable practice, pursuant to a codified set of principles

set of principles and a framework of more individualized industry codes, based on "Fair Information Privacy" principles (FIPPS)—an approach that emphasizes vindication of individual rights through mechanisms like notice and consent in decisions about the use of personal information—and he advocated the creation of a dedicated government board to assist in their implementation.[9] These steps, he concluded, would be necessary to force corporations to devote effective attention to privacy, as had happened with environmental protection.[10]

Smith's concerns have been echoed loudly for fifteen years. The dominant critique by privacy scholars and advocates charges that the U.S. system fails to provide adequate privacy protection. It criticizes the existing patchwork of privacy statutes as weak, incomplete, and fractured, and argue that it fails to provide across-the-board procedures empowering individuals to control the use of their personal information. Moreover, they decry the lack of clear guidance, oversight and enforcement, in the absence of an agency dedicated to data protection. And, while they differ in detail, academic and advocate proposals for reform generally concur that the increased focus of corporate attention and resources on privacy for which Smith called requires the model of protection adopted throughout Europe: omnibus FIPPS-based privacy principles in law or binding codes interpreted and monitored by an independent privacy agency.

This dominant critique of privacy requirements "on the books," however, has largely failed to take account of a sea change in corporate practices "on the ground"—and thus ignored a curious paradox for normative assessment.

Between 1995 and 2010, corporate privacy management in the U.S. has undergone a profound transformation. Following the lead of the financial and health sectors, thousands of companies have created Chief Privacy Officer positions, a development often accompanied by prominent publicity campaigns. A professional association of privacy professionals boasts over 6,500 members, and offers information-privacy training and certification. A robust privacy law practice has arisen to service the growing group of professionals and assist them in assessing and managing privacy. Pricewaterhouse Coopers and others conduct privacy audits across multiple sectors. And robust privacy seal and certification programs have developed.

Hence the paradox. In contrast to the lack of managerial "time and attention" devoted to privacy concerns documented fifteen years ago, corporate practice has promoted direct privacy leadership, in many instances by c-level executives managing large and well-resourced staffs. Yet these changes cannot be attributed to the prescription born of the dominant critique. U.S. privacy regulation remains fragmented and ambiguous, having failed to shed its siloed and sectoral emphasis. It has largely eschewed a commitment to robust FIPPS principles. Congress has declined to follow the European model; the U.S. still has no dedicated privacy administrator.

---

developed through consultation with industry, and field complaints. *See id.* at 207-224.

[9] *See id.* at 207-224.

[10] *See id.* at 210-11.

This paper, presenting the initial findings of the first empirical research into corporate privacy practices in fifteen years, seeks to address this paradox. This paper draws on semistructured qualitative interviews with Chief Privacy Officers identified as industry leaders by their peers, government officials, and journalists, to consider the following: If corporate attention to privacy seems to have flourished despite the failure to achieve what many believed were policy prerequisites, what has prompted the change? What was the role played by law, as opposed to other forces? And how do firms understand the meaning of privacy, despite external prompts that might seem as, or more, ambiguous as those identified by Jeff Smith fifteen years ago?

As described in Section II, although the leading CPOs we interviewed were at heterogeneous firms, they nonetheless communicated a coherent account in responding to these inquiries.

First, they consistently identified a profound shift in the definition of privacy, and its treatment. Each of the corporate privacy leaders defined information privacy as more than "information self-determination," protected by formal notice and consent, introducing as well a substantive notion of privacy rooted in *consumer expectations*. They understood the meaning of "privacy" to depend on the beliefs and assumptions of consumers as to the appropriate treatment of individual information and personal identity. These expectations, they indicated, evolve constantly, and change by context. The success of privacy protection, then, would be measured not by the vindication of notice and consent rights, but in the actual prevention of substantive harms, such as preventing data breaches, or treating information in a way that violates the "trust" of those whose information was at stake. The identification of privacy with consumer expectations as reflected in malleable context-dependent norms, moreover, has moved privacy from a compliance-oriented activity to a risk-assessment process, requiring firms to embed privacy in decisions about product design and market entry, as well as policy development.

Second, the interviews uniformly pointed to the importance of law in this definitional shift. While individual sectoral statutes might be responsible for firms' initial commitment of resources for privacy personnel, the path these professionals would take was influenced by two other regulatory developments. Most notable was the development of the Federal Trade Commission's role (as well as that of the state Attorneys General) as an "activist privacy regulator." Using its broad consumer protection authority, including the ability to shape the law through the threat of enforcement actions, the FTC has advanced an evolving consumer-oriented understanding of privacy. Additionally, the CPOs interviewed pointed to the passage of state security breach notification (SBN) laws as a means for binding corporate performance on privacy to reputation capital. This, they report, has had a significant effect on how privacy is perceived in the upper echelons of corporations, and accorded CPOs greater leverage to implement measures conforming with their notions of privacy within corporations. Taken together, these factors move corporations away from the reactive management style identified by Smith and away from a purely compliance-driven approach.

Finally, the interviews indicated a variety of non-legal phenomena central to the formation and diffusion of the legal notion of privacy compliance as consumer-harm-prevention. They discussed the role of both technology changes and third-party advocates in making consumer privacy protection a market reputation issue. And they discussed the importance of the professionalization of privacy officers as a force for transmission of consumer-expectation notions of privacy, and related "best practices," between firms.

Prompted by these interviews, Section III offers a new account of U.S. privacy "on the ground." It documents the uniquely American way in which the largely-procedural and individual-focused language of privacy protection has been augmented with a substantive concern for preventing violations of consumers' expectations about the treatment of information about them. Taking seriously the our respondents' attribution of this understanding to FTC behavior and other related activity, this section documents an account of the way in which privacy has been "reframed" over the past fifteen years, and its implications for corporate practices. This account emphasizes how elements largely neglected in the dominant "on the books" narrative—the emergence of the Federal Trade Commission as a privacy regulator, the enactment of SBN laws, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals—took part in reconstructing privacy norms in consumer terms, and participated in the diffusion and institutionalization of those norms.

This grounded account, as Section IV argues, has profound implications for debates about both privacy law's substance, and its form.

Specifically, this account casts into relief the incompleteness of a reliance on formal notice, consent and information alone to protect privacy norms as rapid technology changes reduce the power of individuals to isolate and identify the use of data that concerns them. It suggests the frailty of a procedural understanding of privacy protection in guiding corporate decisionmakers, *ex ante*, in making choices about the technologies they employ in products or processes. And it identifies a substantive language for declaring that corporations should not engage in certain types of practices regardless of the formal procedures they have used—a robust, if still emerging, language that has helped frame criticisms of recent privacy invasions by Google Buzz, Sears, and Sony. Indeed, the consumer-protection lens reflects approaches that theorists suggest best vindicate individual and societal interests: those emphasizing objective expectations over subjective formalism, dynamism in the face of technological advance, and application by context.

Moreover, the account of privacy on the ground should inform debates over regulatory form. While the dominant account argues for greater uniformity and specificity in privacy law, the account on the ground suggests the value of governing privacy through flexible principles. Where Smith saw ambiguity as a "bug," we see it as a "feature." Our account describes how a regulator's entrepreneurial deployment of a broad and imprecise legal mandate centered a robust multi-player discourse about privacy that has focused market pressure and executive resources. The increase in

corporate time and attention, accordingly, arose because, rather than in spite, of regulatory ambiguity.

Our research, as this Article's conclusion describes, redirects the unidemensional debate over the adequacy of U.S. information privacy law "on the books"—including arguments over whether U.S. law should mimic the EU model—just at the time that Congress, the Obama Administration, and international organizations are revisiting national and global approaches to privacy approaches. While bolstered procedural mechanisms for enhancing individual choices might be needed, pursuing that goal in a way that eclipses robust substantive protections, or constrains the regulatory flexibility that permits their evolution, will destroy important tools for overcoming corporate over-reaching, consumer manipulation, and the collective action problems raised by ceding privacy protection to individual choice alone.

## I. THE DEBATE OVER U.S. PRIVACY POLICY ON THE BOOKS

The adequacy of U.S. information privacy law is the subject of heated debate. A majority of privacy scholars and advocates criticize existing regulation for its market-based and sectoral approach to privacy protection in the corporate sector, and contend that the existing patchwork of U.S. regulation fails to ensure across-the-board conformity with the standard measure of privacy protection: compliance with the Fair Information Practice Principles (FIPPS) first articulated in the early 1970s. Legal academics and privacy experts have labeled the U.S. approach "FIPPS-lite[11]," an unfavorable comparison to the European Union where FIPPS are reflected through omnibus laws designed to structure all facets of data processing in the private and public sector, and centralized data protection agencies established to enforce them. Thus, they argue for the passage of omnibus U.S. legislation protecting "informational self-determination"—and mandating specific procedures for giving individuals greater control over information about them.

These critiques' descriptive claims regarding the nature of U.S. law on the books are, we readily agree, generally accurate. U.S. privacy law, and its enforcement, are fragmented, and depart frequently from a "FIPPS" understanding of the meaning of privacy.

But their normative and predictive conclusions adopted by many scholars and advocates—that policymakers should act under the belief that U.S. firms will not adopt privacy-protective practices without the passage of across-the-board procedural requirements—have remained troublingly constant given the radical shifts in the landscape of U.S. privacy law. Focusing on a debate between legislative and market mechanisms to protect privacy, the dialogue about protecting privacy in the U.S. has often ignored changes in both the substantive definition of privacy and the mechanisms for its protection that have emerged in the U.S. since Jeff Smith's study, and the ways in

---

[11] Advocates Privacy-lite http://www.privacyrights.org/ar/Privacy-IssuesList.htm; http://judiciary.house.gov/Legacy/mierzwinski050102.htm

which those developments have shaped corporate practice. And they are worth reconsideration.

A. The Dominant Discourse

1. The Touchstone for Measurement: Comprehensive FIPPS-based Regulation and Enforcement

The foundation of information privacy protection throughout much of the world is "informational self-determination"[12] or "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."[13] This rights-based conception of information privacy is embodied a set of "Fair Information Privacy Practices" which provide the backbone of data protection laws in Europe and many other countries.

The Organization for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, finalized three decades ago, provides an influential statement of FIPPS.[14] It articulates eight principles to "harmonise national privacy legislation, while upholding such human rights . . . at the same time prevent interruptions in international flows of data."[15] These principles emphasize an individual's knowledge, participation and control over personal information. They embrace transparency about the types of information collected and the way the information will be used. They propose certain limits on data collection—namely that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[16] They require data collectors to maintain information securely, and emphasize the rights of data subjects to access, and ensure the accuracy of, personal information.[17] And they link the use and disclosure of information to principles of individual self-determination. Thus a FIPPS approach relies largely on procedural protections, such as providing notice to the "data subject," as well as notions of "consent" to informational use.

A full implementation of the FIPPS approach's conception of data protection as a means of protecting individual rights is reflected in comprehensive laws governing information collection and use regardless of type and sector. Moreover, privacy scholars

---

[12] The term "information self-determination" was set forth in a German court decision limiting the intrusiveness of the census. See Judgment of the First Senate [Bverfge, Karlsruhe],, Dec. 15, 1983], translated in 5 HUM. RTS. L. J. 94 (1984).

[13] Alan F. Westin, Privacy and Freedom (New York: Atheneum Press, 1967) p. 7.

[14] O.E.C.D. Doc. C 58 (final) (Oct. 1, 1980); *see* Colin Bennett, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101-111 (1992) (describing the OECD principles).

[15] O.E.C.D. Doc. C 58 (final) (Oct. 1, 1980).

[16] *Id.* (Guideline 1).

[17] Many FIPPS proponents consider such access rights to be "the most important privacy protection safeguard." BENNETT, *supra* note _, at 103.

committed to such a rights-based conception of information privacy protection have emphasized the importance of a strong single privacy enforcement authority that "knows exactly when to use the carrot and when to use the stick, and who is not concerned with balancing data protection with other administrative and political values."[18]

These elements of privacy governance—comprehensive, procedural protections enforced uniformly by a dedicated privacy agency—typify the European approach. And they have served as the dominant metric against which the adequacy of U.S. regulation has been assessed in the policy debate.

2. The Prevailing Critique of U.S. Privacy Statutes

In measuring the U.S. privacy framework against the metric of the European data protection approach, critics have found the former sorely lacking on all three dimensions.[19] "In contrast to the approach in many other nations," one scholar summarizes, "it is unusual in the United States to find any comprehensive privacy laws, which legal experts term 'omnibus laws' and that enumerate a complete set of rights and responsibilities for those who process personal data."[20] Rather, "regulation of the treatment of personal information in the United States occurs through attention to discrete areas of information use" targeting "specific, sectoral activities, such as credit reporting," health care, or electronic commerce.[21] Accordingly, informational privacy is governed by a variety of different laws, administered by different agencies—or sometimes by no agency at all[22]—setting forth divergent requirements governing the treatment of information by type, and business sector.[23]

---

[18] Bennett, *supra* note _, at 239 (describing the arguments of David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States (1989).

[19] See Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime Of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006) ("Privacy protection in the United States has often been criticized."); Ira S. Rubinstein, *Privacy, Self-Regulation and Statutory Safe Harbors, available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 ("According to its many critics, privacy self-regulation is a failure. It suffers from weak or incomplete realization of Fair Information Practice Principles, inadequate incentives to ensure wide scale industry participation, ineffective compliance and enforcement mechanisms, and an overall lack of transparency.")

[20] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1932 (1999).

[21] *Id.*

[22] *See*, *e.g.*, Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 (extending restrictions against wiretaps to include transmissions of electronic data by computer); Video Privacy Protection Act of 1988 (VPPA), 18 U.S.C. § 2710 (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material"); Right to Financial Privacy Act (RFPA), 12 U.S.C. §§ 3401-342 (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records).

[23] *See*, *e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No.

The formal regulations that result provide uneven protection for personal information, and unequal treatment even for similarly situated industry players. Privacy protections, for example, often turn on the entity collecting personal information. Doctors and pharmacies are clearly covered by both federal and state privacy statutes protecting health information,[24] while the developing "personal health portals" designed to create portable "patient-controlled" health records may fall completely outside the scope of such laws, depending upon their business models. Similarly, privacy protection for information about an individual's location generated through the use of location enabled services, a mapping service used on a personal digital assistant (PDA) such as an iPhone or Treo, or a car-based service such as GM Onstar, will vary depending upon whether or not it is provided by a "telecommunications carrier" who is covered by specific regulations, or by another type of service or application provider.

The policies animating different U.S. privacy statutes, moreover, vary considerably. Early privacy statutes, notably the Fair Credit Reporting Act of 1970 (FCRA),[25] which regulates credit reporting activities, and the Privacy Act of 1974,[26] which regulates collection and use of data by government agencies, reflect FIPPS' "informational-self determination" rubric, and include a full range of safeguards reflecting those principles' emphasis on notice, information, and consent.[27] Yet more recent privacy measures often stem not from a commitment to informational-self determination, but from more instrumental concerns arising from harms experienced by consumers, or perceived threats to other interests. Such concerns highlight privacy as a means of promoting social goals like the efficacy of doctor-patient relationship, or of commercial exchanges—the notion, for example, that "privacy laws might promote confidence in Internet commerce, with benefits both for surfers' privacy and companies' sales."[28] Such instrumental approaches, and the balance between privacy and other values they implicate, were reflected in formative decisions regarding the governance of

---

104-191, 110 Stat. 1936 (1996) (regulating the use and disclosure of "Protected Health Information"); Title V of Gramm–Leach–Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6827 (2006)), 15 U.S.C. §§ 6801, 6805 (empowering various agencies to promulgate data-security regulations for financial institutions).

[24] HIPAA's Privacy Rule, for example, regulates only the use and disclosure of certain information held by "covered entities." generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions, 45 C.F.R. 164.501.

[25] 15 U.S.C. § 1681.

[26] 5 U.S.C. § 552a.

[27] *See* Solove & Hoofnagle, *supra* note __, 359-361 (discussing those two laws); *see also id*. at 357 (explaining how "emerging companies known as 'commercial data brokers' have frequently slipped through the cracks" these laws).

[28] Peter P. Swire, Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy, 54 HASTINGS L. J. 847, 861-862 (2003).

privacy on the Internet, which was characterized by limited government mandates supplemented by significant reliance on "self-regulation" by industry players.[29]

These elements of U.S privacy regulation have left it ripe for critique. First, scholars, advocates, and politicians alike charge that the "patchwork,"[30] nature of U.S. privacy statutes renders them underinclusive in its coverage of data worthy of protection, makes arbitrary distinctions that create confusion among both those who are regulated and those who are intended to enjoy protection, and provides only static protections, unable to evolve as technologies and business practices change.[31] Thus in many realms, privacy is protected only by self-regulation by market actors themselves, which is bound to fail in the absence of external incentives for information protection. [32]

---

[29] *See*, *e.g.*, WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997) (promoting self-regulation as the preferred approach to protecting online privacy); Rubinstein, *supra* note _ at 5 ("Clinton officials generally favored the view that private sector leadership would cause electronic commerce to flourish, and specifically supported efforts to implement meaningful, consumer-friendly, self-regulatory privacy regimes in combination with technology solutions.")

[30] Center for Democracy & Technology, *Webpage*, "Consumer Privacy" ("While privacy faces threats from both private and government intrusions, the existing motley patchwork of privacy laws and practices fails to provide comprehensive protection. Instead, it causes confusion that fuels a sense of distrust and skepticism, limiting realization of the Internet's potential."); Beth Givens, Privacy Rights Clearinghouse, *Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act* (September 15, 2000) ("Our approach is characterized as a 'patchwork' of laws.); Priscilla M. Regan, Safe Harbors or Free Frontiers? *Privacy and Transborder Data Flows*, 59 J. SOC. ISSUES 263, 266 (2003) (discussing "[t]he patchwork of sectoral regulation that has long confused the Europeans"); Larry Dignan, *Senate, Web Ad Titans Joust Over Behavioral Targeting*, Between the Lines Blog (posted July 9, 2008), available at http://blogs.zdnet.com/BTL/?p=9280 (quoting U.S. Senator Daniel K. Inouye as saying that "I fear that our existing patchwork of sector-specific privacy laws provides American consumers with virtually no protection.").

[31] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 48 (2001) ("The coverage of U.S. law was uneven: Fair Information Practices were in force in some sectors and not others. There was inadequate enforcement and oversight. Technology continued to outpace the law. And the failure to adopt a comprehensive legal framework to safeguard privacy rights could jeopardize transborder data flows with Europe and other regions.")

[32] Chris Jay Hoofnagle, Electronic Privacy Information Center, *Privacy Self-Regulation: A Decade of Disappointment*, (March 4, 2005), *available at* http://epic.org/reports/decadedisappoint.pdf ("[T]en years of self regulation has led to serious failures in this field. The online privacy situation is getting worse, so bad that offline retailers are emulating the worst Internet practices . . . the market has been a driving force in eroding both practices and expectations."); Joel Reidenberg, "Restoring Americans' Privacy in Electronic Commerce," 14 BERKELEY TECH. L.J. 771 (1999) (responding in part to WILLIAM J. CLINTON & ALBERT GORE, JR., A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (July 1, 1997), critiquing U.S. reliance on self regulation, and proposing FIPPS-based regulation).

Second, critics reject protections that do exist as "FIPPS-lite,"[33] failing to embody the robust procedures embraced by Fair Information Principles.[34] They contend, moreover that the turn to market-oriented rationales for privacy protection diminish the moral weight of privacy—reducing it to another item to be bartered and traded on the market—and fails to recognize the relationship between privacy and democratic society.[35]

Finally, they argue that the failure of the U.S. to centralize oversight of privacy in a single agency able to provide guidance to industry, evolve privacy rules to address emerging issues, and advocate for privacy protection across the public and private sector.[36]

These criticisms, and the metric they use, have dominated the policy debate. Scholars and advocates have been joined by industry leaders and politicians in support of passage of omnibus legislation requiring the adoption of FIPPS generally, sometimes coupled with the creation of an independent agency to oversee and enforce implementation.[37] Thus much of the dominant debate involves a normative claim that the current approach (in particular as measured by the EU data protection model) has failed to provide meaningful corporate privacy practices, and must be replaced by an "enforcement model of regulation (which is also referred to as command-and-control regulation)," in which "Congress defines a set of privacy rules for commercial firms based on FIPPS and authorizes agency regulation, which is then supplemented over time by court decisions interpreting the rules."[38]

B. Reevaluating the Dominant Debate—Indications from Privacy on the Ground

As a descriptive matter, the dominant critiques present a largely accurate picture of statutes and regulations governing U.S. privacy law on the books. Statutes provide

---

[33] Edmund Mierzwinski, Testimony of the U.S. Public Interest Research Group Concerning Affiliate Sharing Practices and the Fair Credit Reporting Act Before the Senate Banking Committee (June 26, 2003) (criticizing the Gramm-Leach-Bliley Act's provisions regarding treatment of personal financial information as "at best, based on FIPPS-Lite").

[34] Solove & Hoofnagle, *supra* note _ at 358 ("Privacy experts have long suggested that information collection be consistent with Fair Information Practices.").

[35] See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987).

[36] *See* sources cited in *supra*, note _.

[37] See, *Consumer Privacy Legislative Forum Statement of Support in Principle for Comprehensive Consumer Privacy Legislation*, June 20, 2006 (signatories Eastman Kodak Co., eBay Inc., Eli Lilly and Co., Google, Inc., Hewitt and Associates, Hewlett-Packard Co., Intel Corp., Microsoft Corp., Oracle Corp., Procter & Gamble Co., Sun Microsystems, Inc., Symantec Corp.).

[38] Rubinstein, *supra* note _ at 2.

inconsistent treatment of similar information and similar business activities leading to an uneven playing field for business and an unpredictable set of protections for individuals. Historically the absence of leadership and coordination on privacy has resulted in inconsistent adherence to existing law and a generally reactive stance to privacy within and by federal agencies. Finally promoting consumer trust, rather than protecting individual privacy, motivates many recent privacy interventions.

As accurate as this debate over the approach to privacy *on the books* may be, it gives short shrift—and therefore provides limited insight into—the ways in which individual privacy is protected "*on the ground*," by both regulators and corporate actors. This cursory treatment was unfortunate but understandable given the relative paucity of attention to privacy in the U.S. commercial sector between formulation of FIPPS as the crux of data protection in the 1970s and the mid-1990s. However, it bespeaks an inexplicable lack of engagement with the U.S. privacy framework that has emerged over the last ten years. In some ways, it therefore puts the cart before the horse, by proceeding to prescriptions about how to improve privacy protection without taking stock of the privacy practices in place within corporations, and how regulatory changes might affect those practices, for better or worse.

This Article begins from the position that the debate about how to move forward on privacy would benefit from a description of the working definition of privacy adopted by corporations, how that definition drives corporate practice on the ground, and how it is influenced by actual regulatory practice.

Since Smith's 1994 study, we have little information about how changes in the U.S. privacy framework—including the panoply of obligations on U.S. companies introduced incrementally by Congress, the FTC and state Attorneys Generals, and changes in the institutional structure of privacy oversight such as the increasing array of individuals in the public and private sector specifically tasked with protecting privacy and the growth of informal and formal tools developed to assist them in this work—have affected corporate practice.

Yet if the critiques of U.S. privacy law demonstrate constancy, corporate privacy practices on the ground evidence a sea change. In the nearly fifteen years since Smith's indictment regarding the lack of "time and attention" devoted to privacy by corporate managers, external signs of a shift in corporate privacy management abound. Smith determined that corporate privacy was mired in a cycle of ongoing policy drift, received only episodic and reactive attention from upper level managers; and was comprised of "non-existent policies in important areas and a persistent policy/practice gap." Yet today, corporate structures frequently include direct privacy leadership, in many instances by c-level executives. The individuals managing corporate privacy have an applicant pool of trained professionals to draw from. There is ongoing training, certification, and networking. A community of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy.

1. Indications of a Sea Change: The Rise of the Chief Privacy Officer

The development of the corporate Chief Privacy Officer offers the most ready evidence of sea change in privacy management In the late 1990's, companies in the financial and health sectors began creating chief privacy officer positions.[39] By 2000, companies in other sectors created CPO positions as well[40]—often to great fanfare, as evidenced by numerous press releases announcing the appointments.[41] Companies' motivations for creating CPO positions were glibly summarized by Richard Purcell, Microsoft's Chief Privacy Officer, in remarks at a large security conference, "How do we get to that vocabulary, that purpose and that channel of communication," he asked, "that assures consumers that we aren't a lot of evil-headed monsters?"[42]

With somewhat amazing alacrity, the informational, training and networking needs of these newly appointed CPOs was met by a new trade association, the Association of Corporate Privacy Officers. Formed in 2001 by Alan Westin, the association—which later developed into the "International Association of Privacy Professionals" (IAPP)—quickly went about formalizing educational programs and undertaking studies to understand the needs and activities of this new profession.[43] About the same time, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA5) created a Privacy Task Force that eventually developed the Generally Accepted Privacy Principles (GAPP), which provide the basis for privacy audits. Privacy seal and certification programs originated during this time as well. TRUSTe, the first online privacy seal program was founded in 1997 and currently has seals at 3,440 web sites. The Better Business Bureau

---

[39] Christopher Brown, *Survey Finds Increasing Number of Firms Appointing Officers with institutional Clout*, 1 PRIV. & SECURITY LAW REPT. 78 (Jan. 28, 2002). It appears that first US privacy officer was Jennifer Barrett of Acxiom, an information services company. Barrett joined the company in 1974, working in many departments of Acxiom, and became a vice president of the company in 1981. Since 1991, she has been responsible for managing privacy issues at Acxiom. ACXIOM CORPORATE LEADERSHIP, available at http://www.acxiom.com/default.aspx?ID=1667&DisplayID=18.

[40] For example, Ray Everett-Church (who claims to be the first CPO) was appointed to such a position by AllAdvantage.com in 2000. Ray Everett-Church, available at http://www.everett.org/about.shtml.

[41] *See, e.g.*, Linda Rosencrance, *IBM Joins Chief Privacy Officer Trend*, Computerworld, Nov. 30, 2000, available at http://www.computerworld.com.au/index.php?id=574929492 (announcing IBM's appointment of Harriet Pearson to a newly created executive-level CPO position); Earthlink, *Earthlink Names Chief Privacy Officer*, available at http://www.earthlink.net/about/press/pr_cpo_announce/ (announcing the appointment of Les Seagraves as CPO); Yukika Awazua and Kevin C. Desouzab, "The Knowledge Chiefs: CKOs, CLOs and CPOs," EUROP. MANAG. J. Vol. 22, No. 3, pp. 339–344, 341 2004 (CPO positions publicly announced on PR Wire and Business Wire covered financial services, banking and insurance (8), marketing and advertising(7), Healthcare (6), Computer Hardware (3), Computer Software (5), Communication Services (4), Consulting (4), and other (including information services and consumer electronics) (3)).

[42] John Schwartz, *Conference Seeks to Balance Web Security and Privacy*, N.Y. TIMES, Dec. 8, 2000, at C4.

[43] Email from the Center for Social & Legal Research to subscribers, P&AB/CSLR Closing, Sept. 14, 2006 (on file with authors).

launched a privacy seal program shortly thereafter and its Children's Advertising Review Unit is the primary self-regulatory program for web sites directed at children.

By 2002, the number of corporate CPOs had reached 500, while in 2003, the IAPP claimed 1000 overall members.[44] In 2004, the association debuted a certification program in corporate privacy compliance, which certified 350 professionals within a year.[45] And today, the IAPP boasts 6,000 members from businesses, governments and academic institutions across 47 countries.[46] IAPP runs a credentialing program in information privacy, the Certified Information Privacy Professional (CIPP) and provides educational materials and runs a wide range of educational and professional conference.[47]

Survey data, moreover, shows that Chief Privacy Officers (CPOs) continue to become more common, and more powerful, features within corporate structures. Within many Fortune 500 companies CPOs are directors or c-level executives,[48] evidencing a perception of privacy as a strategic matter. And corporate privacy resources expand outside firm structures as well. Pricewaterhouse Coopers and others conduct privacy audits across multiple sectors. A robust privacy law practice has arisen to service "in house" professionals and assist them in assessing and managing privacy. Several self-regulatory organizations provide oversight and enforcement of voluntarily adopted privacy policies, advice and support to businesses on privacy issues, handle consumer complaints and monitor members' privacy commitments.[49]

One additional measure, qualitative but perhaps more substantive, of the changes in corporate privacy management deserves mention here. In 1995, Smith referred to his study as the "study that almost wasn't."[50] He details the difficulties he faced in securing institutional participation. Despite his faculty position at a leading business school, strong entrée to high-level executives made possible through faculty and colleagues with existing institutional contacts, and iron-clad promises of anonymity, Smith experienced repeated rejections. Many of the rejections followed an initial positive response, and appeared to be driven by corporate lawyers and a overall sense that the topic of privacy was too sensitive and volatile to discuss publicly.[51] Furthermore, while Smith eventually secured seven participants, even they remained

---

[44] Privacy Officers Association Changes Name, 2 Priv. & Security L. Rept. 39 (Jan. 13, 2003).

[45] http://www.marketwire.com/press-release/Iapp-735905.html.

[46] https://www.privacyassociation.org/index.php.

[47] https://www.privacyassociation.org/index.php?option=com_content&task=view&id=2&Itemid=148 .

[48] *See* Ponemon Institute, *Privacy Professional's Role, Function and Salary Survey* (2005) ("50 percent of privacy professionals are at a director or higher level within their firms; 84 percent report their position is a full-time role within their organization; 42 percent said their department has a direct line of report to a C-level executive within the organization, while 25 percent have a direct line of report to General Counsel");.

[49] Truste, Better Business Bureau Program Privacy Seal, Children's Advertising Reivew Unit

[50] SMITH, *supra* note __, at 52.

[51] *Id.* at 54.

uneasy about such scrutiny. For example, Smith quotes one executive as saying, "I feel somewhat like we are standing nude before you . . . . It will probably be a healthy experience for us to see ourselves thorough the eyes of an outsider, but I imagine it will ultimately be painful."[52]

By contrast, the high-level corporate officials we contacted for the study discussed below were willing, and some quite eager, to participate in the study, to see our findings and conclusions, and to share them with others. While top news headlines affirm that privacy remains a high-profile, hot button topic, the companies we contacted welcomed the chance to share information about how they handle personal information. The marked change in corporate response to similar requests to participate in studies of corporate privacy management are, we believe, a strong indication that privacy is out of the closet and has become a topic corporate executives are willing to discuss candidly.

Taking seriously these external indicia of a massive increase in privacy resources, the remainder of the Article digs deeper. Rooted in qualitative research into corporate privacy management, it presents a new account of "privacy on the ground," an account which should inform, and transform, the policy debate moving forward.

## II. INVESTIGATING PRIVACY ON THE GROUND- EMPIRICAL EVIDENCE FROM CPO INTERVIEWS

To that end, we have embarked on a wide-ranging project to collect empirical information—both qualitative and quantitative—documenting privacy's operationalization "on the ground."[53] The earliest evidence from this project—derived from semi-structured qualitative interviews with nine Chief Privacy Officers identified as field leaders, is presented below. This subset of privacy professionals was identified by domain experts—leading privacy thinkers (both lawyers and non-lawyers) drawn from academia, legal practice (in house and firms), trade groups, advocacy groups, a consultancy, a federal government agency, and journalists focusing on privacy issues—using a snowball-sampling technique.

The structure and purpose of the interviews, sought to minimize the effects of the bias inherent in these selection methods. Snowball samples tends to include participants with thick social networks in a field, and our sample focused on domain leaders with interests in the way discussions of privacy were constructed. The interviews accordingly sought to capture the way in which players with these very characteristics—those "key informants" at the center of the privacy field—framed the privacy discourse. This framing, in turn, is contextualized in Section III, by explication of the privacy regulation and advocacy discourse more broadly.

---

[52] SMITH, *supra* note __, at 54.

[53] Other elements of this empirical project include parallel interviews of European Chief Privacy Officers, surveys of U.S. and European privacy officers more generally, and comparative empirical assessments of enforcement techniques.

The privacy leaders interviewed came from firms that were heterogeneous on every metric except size—all but one was a Fortune 1000 company. The firms hailed both from industries governed by sector-specific privacy statutes, and from unregulated sectors. Some claim global presence; others' only domestic scope. Some include highly diversified business lines, while others are focused within a single industry sector. Many focused on technology-intensive products and services, while others engaged in more traditional lines of business. Moreover, those interviewed had varied personal characteristics. Some were lawyers, others had operational or technical expertise. Some worked under the auspices of the corporate legal department; others as free-standing officers. A number had worked in government, while most had exclusively private-sector careers.

Yet despite this diversity, the interviewees conveyed a high degree of coherence regarding the constellation of issues about which we asked—the way privacy is defined and its protection is operationalized within corporations, as well as the extra- and intra-firm forces that shape these understandings. Specifically, they presented important consistency as to (1) the relevance of a legal "compliance" approach—FIPPS or otherwise—to corporate privacy practices; (2) the way in which privacy concerns are framed and measured within corporations; and (3) the role of external forces—specifically law, markets, advocates and professions—in shaping that framing.

### A. The Limited Import of the "Rules-Compliance" approach to Privacy

In response to open-ended questions about the "external factors" shaping their corporations' privacy practices, respondents articulated a consistent view of the role of compliance with specific legal requirements—both those arising from the EU and those originating in the U.S. sectoral-based regime. By their description, specific legal rules were important in shaping certain "compliance-oriented" measures but played only a limited role in animating corporate policy and principles more broadly.

#### 1. The Role of Legal Rules

Thus, when asked about the external or environmental forces that shaped particular practices in their firms, each respondent identified particular U.S. sectoral statutes, and, for those conducting business abroad, the E.U. Privacy Directive. They pointed, however, to the limited role of legal compliance with codified requirements played in constituting their understanding of what "privacy" demanded of corporate actors.

"[O]bviously," stated one respondent, specific "statutes and regulations" shape particular privacy practices.[54] In the words of others, they constitute the "starting point," "the backing" of an approach to privacy, or the "bottom" of the "privacy triangle."

---

[54] To protect respondent confidentiality, we have removed the interview citations, which are on file with the authors, from the version of this draft submitted to law reviews. Before publication, we will work with Law Review editors to develop a citation system that conforms to privacy practices.

Thus central to the attention accorded privacy is the reality that "[p]rivacy has parts of that, which is you have to comply with some of these laws that are out there." Compliance, then, "has driven the issue to some extent," in that companies must "always meet the legal compliance."

Moreover, several cited compliance with high-profile, and highly-specified, regulatory regimes as a means for signaling privacy leadership to consumers, businesses, and foreign regulators. As to the first, one respondent explained,

> I think that there is some benefit . . . from the consumer perspective, even though they don't understand HIPAA, to know that there is some federal law that makes it criminal if they misuse data. . . . [O]ne thing I think that HIPAA does well is it helps, in whatever fashion, tell the consumer, look, you're protected in this sphere. I don't think they understand it but I think it helps.

Compliance with the Department of Commerce-negotiated "Safe Harbor" certification of corporate conformity with EU privacy law[55] plays a similar signaling function for business partners, explained a different respondent in the business-to-business sector. Discussing his firm's choice between attaining Safe Harbor certification and instead enforcing privacy safeguards through contracts with outsourcers, he described:

> Well for instance, whether we decided to go for Safe Harbor or for contracts was really driven to a large extent by customers who started asking us, "Are you members of the Safe Harbor?" So we actually had a customer push because, for them, it was a checkbox, and the contract for them was much harder to manage than saying, I'm dealing with a Safe Harbor company so I have an adequacy. So we had a customer push and that helped us make the decision, because we were kind of on the fence.

2. The Shortcomings of Rules for Privacy Decisionmaking

Yet at the same time, every respondent—whether in highly regulated industries or those less burdened by sectoral regulation—spoke about the limited role that specific legal rules played in directly shaping their actual understanding of privacy's meaning. Those mandates, remarked one CPO, "enforce the minimum;" another continued: "then we build from there."

More respondents emphasized that specific procedural rules lack relevance to many privacy-impacting decisions that must be made by corporate managers. Specifically, they described the failure of such rules to offer a touchstone for guiding privacy decisionmaking in new contexts, as new types of products, technologies and business models evolve. As the boundaries between firms and the consumers and businesses with which they deal blur, and part of the value of products and services arises specifically from the purposeful sharing of information between business and consumer, the privacy threat model shifts from issues of "security," "access," "notice" and "consent"—dominant in U.S. FIPPS discourse—to questions of the reuse and

[55] *See infra* text at nn.__-__.

repurposing of information, and what notice and consent mean when companies can, while still in formal compliance with the law, manipulate huge amounts of data willingly supplied to them by consumers.

While each respondent spoke about potential privacy issues arising out of evolving product or service offerings or innovative organizational structures in the contexts of their particular firms, several examples illustrate the shortcomings of such static laws in providing a helpful guide in dynamic business contexts.

The most wide-reaching example arises from the societal shift towards "ubiquitous computing."[56] As companies root consumer or customer interactions in increased connectivity—ongoing relationships in place of one-off transactions—the use and transfer of data is constant. Indeed, respondents explained that the very fact of a communication itself may reflect information revealing that a recipient falls in a certain category: that they are an account holder, or use particular information products or services, or that they have a disease and are involved in ongoing medical treatment, , or are in a specific location—with all that might reveal. Data flows coming in and out of a home on a "smart" energy grid—data that may be readily shared for the purpose of enabling energy management—is an example of an environment that might also reveal significant information the activities on the inhabitant.[57] Moreover, explained another, previously nonproblemmatic policies such as monitoring communication to audit the quality of customer service take on new meaning, as personal information is revealed to third parties uninvolved with the service provision itself. In each case a customer might have been made aware of the privacy practices consistent with FIPPS policies, and the firm involved might have complied with all legal requirements, yet reasonable concerns about the integrity of privacy protections might nonetheless be triggered. In such new and changing contexts these regulatory approaches to privacy frequently fail to provide a metric for arriving at the appropriate balance between "value information flows and being technology-enabled" on the one hand, and "privacy-centric" or "trust-generating" concerns on the other.

Indeed, many new business services explicitly involve open-ended and ongoing corporate use and reuse of information in ways that develop over time. These services focus on the continuing manipulation of data to provide a "value proposition" to the "person who is giving us the information so they see some value coming back."

One sector operating in this manner identified by a number of respondents was healthcare, in which those other than traditional medical providers—such as pharmaceutical companies and medical technology firms—play an increasing role in ongoing oversight and monitoring of health practices and outcomes. Thus one

---

[56] Ubiquitous computing environments are those in "which each person is continually interacting with hundreds of nearby wirelessly interconnected computers. The point is to achieve the most effective kind of technology, that which is essentially invisible to the user," *See* M. Weiser, *Some Computer Science Issues in Ubiquitous Computing*, 36 ACM 75 (1993).

[57] *See* Mikhail A. Lisovich & Deirdre K. Mulligan, *Inferring Personal Information from Demand-Response Systems*, 8 IEEE Security and Privacy 11-20 (2010).

respondent described these shifts in their own company which now both "provid[es] IT systems for hospitals," and "make[s] all sorts of machines that you would see in a hospital" such as "diagnostic and interventional medical devices" that "go into the body." While these lines of business certainly require "thinking about HIPAA," they require deeper assessments ungoverned by either rights-based or process/access notions of privacy: "when you obviously get into the body," this respondent noted, "you've got all sorts of different healthcare privacy issues."

Another privacy officer spoke about the challenge of personalizing medicine, as research has demonstrated that there are "different tumor types," "different types of diabetics" and the fact that patients have "different kinds of diseases so they need different types of interventions." "[A]s you start to personalize," the respondent noted, "this requires more interaction with consumers." Moreover,

> we may need to try and figure out how to work or partner with another entity that has a tissue bank or we may need to figure out how to get access to a significant database that will allow our research to go forward. And the figuring out has to take into consideration, you know, what are the ethics? You know, what are the privacy issues around doing that?

While consumers, fully informed about the privacy practices and legal compliance regime governing the relevant company, might be truly interested in reaping the value resulting from the exchange of sensitive personal information, these trends, another CPO explained, reflect "fits and starts in the healthcare industry about its adoption of IT and the true connection of the different elements of that ecosystem," that raise potential new privacy issues.

Respondents thus identified the shortcomings of a "compliance-based" approach in a variety of contexts where technology supports the growing business trend towards ongoing remote communications with a product or service provider. Such technologies include, for example, means for remote transmission of data and information regarding software updates, and sensor technologies that convey usage and performance information back to manufacturers—information that consumers would, for some purposes, very much want corporations to have. In discussing this issue, one respondent noted their commitment to FIPPS: "We are an informed consent company. That's been my mantra. Informed consent is something a hundred years old. We can draw our little common-law hooks around it." Yet, she noted, this is an area in which FIPPS's rights-based notion of privacy fails to provide guidance:

> Opt in and opt out drives me crazy, especially when you talk about peripheral devices. How do you "opt in" to a [product] telling [the manufacturer] that it burned out? And do you want to? Probably not."

Finally, respondents spoke about the challenges arising from the potential privacy issues arising when two types of third parties—outsourcers and the government, under its subpoena power—are accorded, or seek, access to personal data. In both cases the original firm might justify sharing information by its compliance with governing legal rules; they can rely in the fact that they ensured that data transfers complied with the Safe Harbor or other regulatory requirements, or that they faced no legal obligation that

would hinder their release of data to a government agency. Yet both of these instances clearly implicate deeper privacy questions about the potential compromise of personal information—questions regarding which existing legal rules provide no answers.

Accordingly, respondents uniformly rejected an understanding of privacy as a compliance function. "[T]he law in privacy," one respondent summarized, "will only get you so far." Regarding many things that "privacy" requires, said another, "there's no law that says 'you have to do this.'" In sum, explained a third, broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts—privacy must be "strategic, part of the technical strategy and the business strategy."

B. The Articulation of an Alternative Framing of Privacy

While our interviewees attributed a more "reactive" approach to specific legal rules governing privacy, they nonetheless described significant changes in the approach to corporate privacy since Smith's 1994 study. Specifically, they described the adoption of an approach to privacy issues in varying and dynamic contexts, wherever they arose in the firm—an approach, moreover, that was strikingly consistent across firms. This approach reflected an understanding that privacy is defined by consumer expectations regarding the appropriate treatment of personally-identifiable information. Such expectations evolved with changes in both technology, and consumers' methods of interaction with it, and therefore required the implementation of privacy practices that were dynamic and forward looking. This approach, moreover, stressed the importance of integrating practices into corporate decisionmaking that would prevent the violation of consumer expectations—a harm-avoidance approach—rather than any formal notion of informational self-determination rooted in formal notice or consent.

1. Company Law

For both operational and strategy reasons, then, respondents stressed the importance of developing "Company Law"—consistent and coordinated firm-specific global privacy policies intended to ensure that a firm is both in compliance with the requirements of all relevant jurisdictions, and at the same time acts concordantly when dealing with additional business issues not governed by any particular regulation.

Critically, these policies extend beyond compliance with specific legal mandates to broader privacy policies focused on outcomes: that, even if technically legal, corporate practices are "consistent with our global corporate values, and consistent with employing customer expectations."

2. Privacy Measured by "Consumer Expectations"

This last remark, identifying consumer expectations as a touchstone for developing corporate privacy practices, is reflected in every one of our respondents' description of their understanding as the "company" definition of privacy. Privacy, in respondents' language, has evolved over the last several years to be defined in large part by respect for what consumers expectat regarding the treatment of their personal sphere.

Such "customer or the individual expectations," guide behavior that exceeds the demands of legal compliance. In the words of one CPO, "your customers will hold you to a higher standard than laws will, and the question is, do you pay attention to your customers? Do you care about your customers?" The expectations approach was framed in relational terms, sounding in a normative language of "values," "ethical tone," "moral tone," and "integrity"; in experiential terms such as "secure, private, reliable,", and "consistent," and, most frequently, in fiduciary terms, such as "respect[ ]", " responsibility," stewardship, , and "protect[ion]." On a fundamental level, respondents repeated, privacy "equates to trust," "correlates to trust," is "a core value associated with trust," and, in the words of one: "Trust, trust, trust, trust."

Privacy leaders varied in their articulations of "consumer expectations," but sounded several consonant themes. Each emphasized the customer's experience, including "think[ing] about how this feels from the customer perspective, not what *we* think the customer needs to know." In so doing, one respondent described,

> you run it by your friends, you run it by your family; ask your mom, ask your granddad, ask somebody who doesn't live in this world or doesn't live in technology or the leading technology companies. What's the reaction? Do they laugh? That's one set of problems. Do they get the heebie jeebies, you know? Is it kind of creepy? So, the creepy factor, for lack of a better description is good.

Yet such expectations arise as well, they described, from the representations and actions of firms themselves: the "discrete behaviors that are going to be objectively put out there, subjectively put out there and then met," and the ability to "deliver those consistent experiences, compliant experiences, you know, that's trust."

Finally a consumer expectations approach was described with regards to outcomes, rather than particular rules or practices: "the end objective in my mind is always what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us, which is probably pretty much any constituency." "[H]ow likely," for example, "is that customer going to be comfortable using online banking in the future or any other new online service that the bank offers, and how many friends is he likely to tell?" Or will "they start wanting to shut down the relationship, in other words shut off the information, complain to the FTC, send nasty letters and threatening lawsuits about email and that kind of stuff."

The fundamental implication of this definition of privacy, one respondent explained candidly, is that "it's not necessarily beginning from a privacy-as fundamental-right point of view," but rather reflects the notion of "privacy as important to what we do for a living."(VI:3)

3. Implications of a "Consumer Expectations" Framing: From Compliance to Risk Management

Defining privacy through a "consumer expectations" metric, the interviewees explained further, has important implications for both how firms need to think about

privacy protection, and, accordingly, how privacy protection is operationalized within the corporate structure.

The interviewed privacy officers sounded a consistent theme: that the definitional ambiguity inherent in privacy regulation required companies to embrace a dynamic, forward-looking outlook towards privacy. "[I]t's more than just statutory and regulatory," said one, "it's such an evolving area." "We're really defining [privacy as] 'Looking around corners . . . looking forward to things that are a few years out."

"We are all still learning," described another, "because the rules change:"

> Customer expectation changes and the employee expectations change. The world changes periodically too on top of that and I look at what we're doing as something that's really important from any kind of a personal and values perspective and from a business perspective.

In the words of a third: "[b]est in class is comparative, and it's also subjective. . . . [T]hat bar changes and it's different by industry and it's different by moment in time." A fourth echoed the contextual nature of the the "external environment" shaping privacy, including "how the regulations or even the perception of the public changes." Accordingly, explained a fifth, corporate leaders must focus on "What's the next thing that's coming down the pike, because if you get caught unawares, you're behind the ball and you're spending a lot of money."

This conceptualization of privacy issues, other respondents described, have shaped the way their companies have understood, and operationalized, the corporate privacy function. As rules-compliance provides an increasingly inapt mindset for privacy management, privacy is increasingly framed as part of the evolving practice of risk management. "[W]e're all talking about risk," said one interviewee, "And how do we mitigate risk at the same time we're . . . protecting information." Privacy, then, must be approached with the questions, "What do I need to be worrying about today? What am I missing?" Accordingly:

> I want to keep changing the way we're doing business so it is dynamic, so we are, you know, trying to mitigate the risk of the day while keeping our core program in place. And so we're changing . . . I don't keep [processes the same] the same. Because, if by chance it gets, you know, somebody figures a way to beat it, they won't be able to if I'm constantly changing it or adding something here or subtracting there. So my view is is it's a journey, not a destination, and we should always, we try to get everybody together to say, how do we mitigate risk; what's the latest, you know, what do we need to be-every time there is a breach I look at what happened and think, are we protected? So it's a constant, what's the next thing on the horizon?

Accordingly, as we discuss elsewhere,[58] privacy officers are incorporated into risk-management structures at the highest management level, and privacy discussions

---

[58] *See* Kenneth A. Bamberger and Deirdre K. Mulligan, *Operationalizing Privacy: Structures Within the Firm* (draft in progress).

have been moved out of compliance offices into the processes by which new products and services are developed.

C. External Influences on Privacy's Conception

Finally, respondents located the notion of privacy as a function of consumer expectations in particular developments over the last decade. As one respondent described, while a number of years ago "we talked to customers and said, 'How high on the radar is [privacy] for you?' And most of them at the beginning of this said, 'Not at all,'

> now we're seeing it pop up in RFPs in almost every selling instance. . . . And so these go on and on and that's something you never would have seen back in 2000, at least I never saw.

As another described,

> if you go back six, seven years ago, there was a change in the marketplace. Pre that time, no customer was demanding security in their solutions. They were demanding product features, and the more that you can ship me and the more that you can give me the capability to use, the better, and security just didn't matter at that point in time. I'm maybe going back just slightly pre seven years ago, but that changed with-- the market started to demand more security because security events started to become more common. And, we're a product company product companies produce what the market wants. The market doesn't want security, then you don't spend a lot of time thinking about security.(III)

This new emphasis on consumers and markets, they described, arose in the context of three intertwined phenomena central to development of a new privacy definition: (1) two regulatory developments—the Federal Trade Commission's expanded application of its consumer-protection enforcement authority pursuant to Section 5 of the FTC Act in the privacy context and the passage of state data breach notification statutes; (2) societal and technological changes that strengthened the role of advocates and the media; and (3) the professionalization of privacy officers.

1. Legal Developments

At the same time that respondents indicated the limited role of compliance with legal rules in shaping corporate approaches to privacy, every single respondent interviewed mentioned two important regulatory developments they believed central to shaping the current "consumer expectations" approach to privacy: the behavior of the FTC, and the enactment of state data breach notification statutes.

*a. The Federal Trade Commission*

Respondents uniformly pointed to the FTC's role as an "activist privacy regulator." in promoting the consumer protection understanding of privacy. As described below,[59] since 1996 the Federal Trade Commission has actively used its broad

[59] *See infra* Section III.

authority under Section 5 of the FTC Act, which prohibits "unfair or deceptive practices," to take an active role in the governance of privacy protection, ranging from issuing guidance regarding appropriate practices for protecting personal consumer information, to bringing enforcement actions challenging information practices alleged to cause consumer injury.

For three of the privacy leaders included in our study, the FTC's enforcement power held particular salience, as their firms had previously been subject to privacy enforcement actions by, or were currently governed by consent decrees with, the Commission. Yet respondents from firms uninvolved with previous FTC proceedings joined those three in referencing the threat of enforcement under the agency's broad authority as critical to the shaping of consumer-protection, rather than compliance-oriented, approaches to privacy. As an initial matter, they described, state-of-the-art privacy practices must reflect both "established real black letter law," and "FTC cases and best practices," including "all the enforcement actions [and] what the FTC is saying."

Perhaps more importantly, several respondents stressed, a key to the effectiveness of FTC enforcement authority is the agency's ability to respond to harmful outcomes by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change—the very opposite of the rule-based compliance approach frequently embodied by regulation. In acting against unfair and deceptive consumer practices, one respondent explained, the FTC has

> moved the bar over the last couple of years away from the sense that we're not exclusively focusing on deception and into the land of unfair. And in the land of unfair it's pretty foggy. The land of deception has become fairly clear over the years. There's always new situations that require an interpretation but there's some pretty clear rules of the road. I think the rules around unfair that we really have a fogged in set of landscaping here because unfair is much more subjective and the FTC has been pretty clear that they will figure out what it means at the time.

The unpredictability of future enforcement by the FTC and parallel state consumer protection officials contribute, others describe, to more forward-thinking and dynamic approaches to privacy policies in firms, guided by consumer-protection metric. One of those respondents in a firm subject to FTC oversight explained the ways in which the enforcement action against that company transformed the understanding of privacy in their, and other, firms, from one centered on compliance with *ex ante* rules to one animated by the avoidance of consumer harm. As that respondent explained, at the time of the privacy-compromising incident leading to the enforcement action,

> [W]e had everything in place, from a website security perspective, you know? We had, you know, SSL security, you know, in certain areas and in where we were collecting the information and we had, you know, a privacy statement that explained things . . . . [A]ll these things that we had in place that was fairly standard in corporate America at the time. I mean, we were consistent with the best practices at the time. I have no doubt about that. Our privacy policy was very standard for the time. (IV)

Yet the regulator determined that these "best practices" failed to conform with what should be expected of firms holding themselves out as privacy-protective:

> what we didn't have was the comprehensive program and the FTC, with our case, for the first time, looked at the privacy statement and said, "You know what? You can't say that you respect privacy and then not have a full privacy program with training." And now, you know, looking back, with six years of history, you say, well, yeah, okay, that's fairly fundamental. They've established that already. But even . . . when the incident occurred, you know, it was still pretty rare for companies to have the comprehensive program behind the website statement.
>
> * * *
>
> And so we did our walk around with the FTC commissioners, I went with my general counsel, and it was a completely eye opening thing for her. And there were exchanges with the commissioners where, you know, they basically said that, you know, what we did was similar to, you know, a nuclear warhead being dropped. I mean, I'm not making it up. And so that, the significance of that statement from a regulator who had the power to really hammer us hard, you know, stunned my general counsel.

Even those respondents not involved in previous FTC actions cited incidents such as those involving Choicepoint, Microsoft, Tower Records, Geocities, and other "FTC governance-type issues," as instigators for their firms' decision to hire a privacy officer, or create or expand a privacy leadership function. One described the threat of FTC oversight as a motivating "Three-Mile Island" scenario. Several described, moreover, the way in which the prospect of an enforcement action enhanced their credibility within their firm. "You know," said one,

> you had to start with the fear aspect or with the risk aspect. You can't really go in and build I think solely from an appeal to the . . . greater good, because it's not as tangible. It's longer term, right, and it's hard to do things in corporate America that are purely longer term. So I think you start with, boy, if we don't protect this, we're going to lose trust, we're going to-- and we could get prosecuted, you know?

"I walked in [to the firm]," described another, saying, "Look at what happened to them. This could be you. Be lucky because it's not just because they're bad guys. . . . And it was the FTC oversight [of other firms] and the length of scrutiny and the cost of audit that they had to submit to that I think was the dollar lever that started to open that box for me."

The very unpredictability of future enforcement can lead, a different respondent described, to "good dialogue" with regulators. "I think," she said, that "companies are often reticent to expose what they're doing for risk that they will be, you know, investigated or somehow found lacking. I would rather have the conversation now than have it during an enforcement action." Indeed, another suggested: "take a look at the FTC enforcement actions" under a

> loose framework of section 5. . . . [T]hat extra layer of – I don't think any privacy officer wants to skirt with – unless there is a compelling need. You have to

> analyze that in terms of the strict compliance line versus what can we do above and beyond that that's appropriate.

Similarly, another respondent remarked on the way that respondent's interactions had revealed differences between the FTC and European privacy regulators, reflecting the effects on U.S. business of the threat of, yet uncertainty about, FTC enforcement:

> You know, it's kind of funny in Europe where they get all kooky about the Americans who want to dot every I and cross every T. And it's like, well I'm sorry, my enforcement agency which is the Federal Trade Commission, they enforce the, you know, the black letters, [but also] the spaces, the semicolons, the periods; all those things are things they enforce.

*b. Data Breach Notification Statutes*

In addition to the changing role of the FTC, every single respondent mentioned a second regulatory development, the enactment of state data breach notification statutes,[60] as an important driver of privacy in corporations. . These laws, the first of which took effect in California in 2003, require that companies disclose the existence of a data breach to affected customers, usually in writing.[61]

Such laws, respondents explained, have served as a critical attention mechanism, transforming the effects of media coverage, and heightening consumer consciousness. "[A]ll the news around security breaches" is "[a] large focus," reported one respondent. In the words of another, "the breach news in the states last year was so--the drumbeat was so loud--that it didn't take much to get the attention of our senior executive on data security, kind of as part of the privacy program."

This mechanism has called attention specifically to the effect of the treatment of personal information on consumers:

> "it sure has heightened more people's understanding of the stakes inherent in managing data in a very real way" by "shift[Ing] the thinking of thinking about risks inside the company from thinking about the risk of losing data of IP or financial information, never thinking about the rest of the poor individual--I just lost a credit card file, okay, I lost a credit card file, who gives a hoot, but you know, it's capped, so no big deal, now, holy moly, I lost somebody's social security number and now there's liability associated with it for the company and they have to worry about it."

---

[60] As of December 9, 2009, forty-five states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, *see* National Conference of State Legislatures Website, at http://www.ncsl.org/default.aspx?tabid=13489.

[61] *See e.g.*, Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82. State laws differ to some degree on issues such as permissible delay, penalties, the existence of private rights of action, and the existence of exemptions for breaches determined "immaterial."

The public attention triggered by notification requirements has been critical, several respondents reported, in strengthening the privacy function more generally. Notification legislation, reported one, "enriched my role; it's putting more of an emphasis on leadership internally in a very operational sense as opposed to just policy setting and management of that sort." Indeed, explained another,

> the external environment has helped that tremendously. And that's everything, you know, from what the CEO reads in the newspaper to the number of breach letters that our own employees and executives get from other companies saying, "Oh, my gosh, I don't want this happen to us. I don't want to see one of these with [our company's] logo on it," you know. So I think there has been a lot of pressure in the U.S. media, particularly on the data breach issue, but then that gave me the opportunity, internally, to say, "Well, it's not just data breaches, it's not just laptops, it's a responsible overall program about how we take in, and use, and process and secure data. . . . it's a tiny little, you know, the tip of the iceberg, really of, you know, what privacy challenges are, and the privacy program should be."

At the same time, however, a respondent who heads privacy at a global company discussed her perception that many European companies, despite their more rigorous FIPPS compliance requirements, are far less sensitive to the problems of compromised data when they outsource business functions. They "don't think about it very much," she said, because "[t]hey don't have security breach notification," which "changes behavior."

2. Legal Changes and the Court of Public Opinion

The high-profile activities of FTC and the disclosures mandates by breach notification law, our respondents explained, were particularly important because they dovetailed with already-occurring social and technological changes fueling privacy consciousness. This rise in consciousness both germinated, and was in turn facilitated, by the growth in media interest in privacy, and the development of what one called a "privacy community"—including advocates and journalists—that pressed privacy as an issue. Respondents thus described the way in which the "court of public opinion," as well as regulatory attention, is shaped by "a nice, close loop that is the media advocate," and stressed the importance of "what the CEO reads in the newspaper" to the "external environment."

"[R]ight now," explained one,

> you see the "P-word all over the place. You know, it used to be like once a week I'd cut out an article and say, "Look, they're talking about privacy in the paper on page twenty-two of the Wall Street Journal." And now it's pretty much every day. So I think we've won the battle of actually being noticed."

Indeed, said another, "I think seeing other big brand names take a hit on the issue certainly raised awareness." These developments, in turn reflect a what a third termed a "growing sensitivity by particularly senior executives to [privacy] things that are going on in the marketplace."

Thus,

> companies have seen that there is a lot of news about it and it can be a help to them in terms of figuring out PRM activity, avoid the bad and promote the good. Try to avoid the breaches and the problems and the brand tarnishment issues and promote the ability to use and flow data in a proper way and make it a competitive advantage for him.

### 3. The Role of Professionalization in Filling in Ambiguous Definitions of Privacy

The consequent empowerment of those responsible for privacy within firms was, in turn, amplified the role of the increasingly professionalized privacy-officer field in shaping the dynamic, consumer-protective approach to privacy. One CPO summed it up by stating,

> Part of the privacy office challenge is what I call demystifying privacy . . . typically your boss and your bosses boss don't have a good, you know, pre-established idea of exactly what the program will look like except that they want a good one. That's what my bosses said, we want to have a wonderful privacy program and you tell us what that means. I think that's not an unusual experience.

In defining what "a wonderful privacy program means" in the face of a quickly-moving regulatory target, an active advocacy community with effective public-relations skills, and shifting norms arising from changes in technology and its use by consumers, the interviewed privacy leaders revealed a deep reliance on peers.

Specifically, interview responses highlighted the role that professional associations and communities of practice play in "filling in the details" of a fluid consumer-expectations privacy mandate. The importance of the IAPP, the large privacy trade association described earlier in Section I, was made explicit. The association's publication and dissemination of information as to best-practices approaches, and its capacity to provide a space for "networking," and "getting to see the other privacy offers" one respondent said, is about getting "drenched in the culture." Respondents reported that a non-trivial component of their job duties involved collaboration with other members of the privacy sector, and information-sharing about accepted best practices, guidelines and policies among the CPOs we interviewed was rampant.

Information garnered from peers provides privacy officers both with leverage as they advocate for certain privacy practices within their own firms, and with an important cost-savings technique for allowing CPOs to draw on the information and insights generated by better financed peers. Information-sharing, one CPO stated, "is really helpful for very resource-strapped groups . . . . [I]f there's a change in privacy, it's so ill-understood outside of our little enclave that for me to say, 'I need five hundred thousand dollars to do a research project based on opt in'—it ain't happening." To fill the knowledge gap within the constraints of the corporate budget, CPOs report learning from those they perceive as leaders—"So, with other corporate leaders, you know, the Microsofts and the Axioms and the P&Gs and others who really have phenomenal programs, there's a lot of, I think, of sharing that goes on."

At times, the peers themselves were literally brought into an intra-firm conversation. Strikingly, one CPO reported,

> I've been on the phone with [other firms'] executive committees, telling them about [our company's] experience because it helps the other company, you know, privacy office to have me tell their people because they've told them and they don't believe them. So when they hear it directly from me, that has some advantage and I've done that with a number of different companies. And we just see that we have to go down this path together. It's very important.

Thus while doing privacy "well" was viewed by respondents as a strategic advantage in the marketplace, those respondents generally expressed the view that a peer's mistake risked tarnishing the entire sector or worse, by drawing regulatory or public attention. For this reason, CPOs reported that helping competitors to make better privacy decisions was in her interest. In the words of one:

> if I help my competitor at XYZ company do better I don't think that's about competitive advantage. That's about doing the right thing because if they screw up, you know what, it screws up all of us.

Similarly, another respondent attributed a willingness to share information about privacy policies and practices quite freely to that respondent's belief that privacy offered more value to an industry space than to an individual firm. This perceived lack of competitive value created tremendous latitude for information sharing:

> I think most companies have the belief that the best practice, the good privacy statement or the training materials, you know, a process for handling a security breach isn't going to give you a competitive advantage and—but, you know, so you share these things pretty freely. We are pretty much an open book. If I had created it, then I'm very happy to share it pretty much with anybody, regardless of what it is, for the most part.

## III. CONTEXTUALIZING THE INTERVIEWS—AN ACCOUNT OF PRIVACY ON THE GROUND

The accounts of interviewed privacy leaders strengthen the quantitative external evidence of a radical increase in corporate privacy management between Smith's study and ours. By their descriptions, privacy took on new meaning during this era; in response firms evolved new management practices. These practices, moreover, address many of the failings Smith identified, namely systemic inattention to privacy, reactive policy development, and gaps between policy and practice. Yet they emerge without the passage of comprehensive federal privacy laws or the creation of a U.S. data protection authority. And most notably, the new definition that they claim organizes privacy thinking is characterized by less, rather than more, legal specificity, directly counter to the reduction in ambiguity that Smith championed.

If the developments were not spurred by the introduction of an omnibus privacy law and data protection agency—for in fact the U.S. held fast to its piecemeal approach to federal privacy legislation during this period of change—what was the context in which they occurred?

The interviews suggest that changes in the logic and practice of corporate privacy management tracked other atmospheric, institutional and substantive developments—developments that play a minimal role in dominant critiques of the U.S. privacy framework. Specifically, they suggest that a constellation of regulatory phenomena—the emergence of new activist federal regulators, new information-forcing state laws, and the increased visibility and influence of privacy advocates in the regulatory landscape—fostered legal and market connections between privacy, trust and corporate brand, which combined with the professionalization of privacy officers to heighten attention to privacy management within corporate America.

In light of these suggestions, this Section explores those phenomena, and details the history of their development. This account reveals a history of purposeful interactions among regulators and other actors across the U.S. privacy field to shape the logic of privacy protection in ways reflected by the interview responses. While a language of "trust," and the connection between privacy and consumer protection, first arose on the global stage during the early days of the commercial internet, the emergence of the Federal Trade Commission as a site of privacy norm interpretation pursuant to its broad Section 5 authority built upon the broader conversation of privacy as a market enabler. The FTC's activities were neither driven nor limited by standard data protection rules, but took advantage of breadth and ambiguity in its statutory mandate, and the agency ultimately provided a forum for the expansion of privacy discourse. This forum, strengthened by privacy disclosures mandated by state security breach notification laws, enhanced the visibility of privacy debates, empowered a movement of privacy advocates, and strengthened the position of privacy professionals within corporate organizations. Leveraged by the agency's entrepreneurial use of its enforcement powers, and by increased market pressures for privacy performance these activities, these developments moved the privacy discourse from a focus on individual procedural mechanisms to an approach emphasizing the protection of substantive privacy norms, and shaped corporate privacy practice by creating a "realistic threat of retribution for inattention"[62]

A. The Roots of a Consumer-Focused Language Of Privacy

The privacy leaders we interviewed unanimously articulated a non-FIPPS-based definition of privacy as driving activity within their firms. Privacy was portrayed as an expansive concept: privacy "equates to trust," "is a strategic initiative," and "a core value associated with trust, primarily, and integrity and respect for people." Moreover the concept sounded in terms of broad principles: "apply[ing] information usage to new contexts" in a "very contextual" manner. And the implementation of these principles required ongoing expertise: "[T]he company . . . understands that trust plays a key part . . . but isn't able to kind of codify what . . . trust looks like," so "the idea that there's going to be a one-size-fits-all privacy practice is, I don't think, possible." Thus "you don't really have a practice that is uniformly developed on the back end because it's also a

[62] SMITH, *supra* note __ at 214.

judgment call." Finally, it was tied to consumer reputation: "the biggest value to privacy is it's a part of brand."

This way of framing privacy reflects a discourse that first arose in the mid-1990s, a transformative period for information and communication technology use and policy in the U.S. and globally. The birth of the internet as a commercial medium and the need to respond to privacy challenges created by its global and data-driven nature altered the political discourse about privacy protection. Specifically, in both the U.S. and in the European Union, arguments about the importance of privacy protection no longer sounded exclusively in the language of individual rights protection. Instead, they also reflected a desire to facilitate electronic commerce and the free flow of information by building consumer trust. While tension between the EU and the U.S. about how to instrument the protection of privacy was high, they increasingly advanced a similarly instrumental rhetoric about privacy's value, stating that electronic commerce "will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information."[63]

By 1996, the rhetoric of consumer trust as a reason for business to attend to consumer privacy had become "something of a mantra" internationally.[64] That year, the Organisation for Economic Co-operation and Development (OECD)[65] issued the first in a series of reports indicating that "privacy interests" needed bolstering, not only for human rights reasons, "but also [to ensure] that the right balance is found to provide confidence in the usage of the system so that it will be a commercial success."[66] In preparation for the EU ministerial conference on Global Information Networks in Bonn in July 1997,

---

[63] White House, *Framework for Global Electronic Commerce* 12-14 (July 1, 1997),

[64] Bennett & Raab, *supra* note 1 at 49.

[65] A consortium of 30 countries, including the United States and many European countries, united in their commitment to democracy and a market economy. Organisation for Economic Co-operation and Development (OECD), *Members and Partners*, http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html (last visited Aug. 1, 2008) (describing what OECD does and who its members are).

[66] OECD, *Report of the Ad Hoc Meeting of Experts on Information Infrastructures: Issues Related to Security of Information Systems and Protection of Personal Data and Privacy* 8 (1996), http://www.oecd.org/dataoecd/32/50/2094252.pdf. Later reports continue this theme, *see OECD Ministerial Conference "A Borderless World: Realising the Potential of Global Electronic Commerce," Conference Conclusions* 5 (Oct. 1998), http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/NT00000FEE/$FILE/12E81007.PDF. (stressing that "users must gain confidence in the digital marketplace" and "that the potential benefits [of global electronic commerce] will not be realized if consumer confidence. . . is eroded by the presence of fraudulent, misleading and unfair commercial conduct."); *Declaration on Consumer Protection* and *Conference Conclusions* OECD, *Ministerial Declaration on Consumer Protection in the Context of Electronic Commerce* 3 (Oct. 1998), http://www.olis.oecd.org/olis/1998doc.nsf/LinkTo/NT00000E12/$FILE/12E81004.PDF (mentioning "trust" and "confidence" a total of twenty times in 19 pages but mentioning privacy rights once to declare that member nations will "ensure the respect of important rights" without stating a consensus position on what those rights are, or how they function in the marketplace).

German Economics Minister Günter Rexrodt and EU Commissioner Martin Bangemann wrote, "building confidence by achieving efficient [privacy] protection is essential to allow the positive development of these networks."[67] The organization's report on *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*,[68] also issued that year, concludes that "consumer confidence is a key element in the development of electronic commerce," and that enforcement of privacy policies serves to bolster that confidence.[69] On the domestic front the Clinton Administration released its white paper, *Framework for Global Electronic Commerce*, which stated that e-commerce "will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information."[70]

Thus scholars in this period identified "an emerging international consensus" in the public and private sector "on the importance of trust and confidence in modern information and communication technologies and their application to online transactions."[71] The dominant reason advanced to protect privacy in high-level government statements on the global stage, was the promotion of electronic commerce rather than individual privacy rights.

B. The U.S.-E.U. divergence: The Timing of Institutionalization

While this instrumental expression of privacy's value in a networked world spanned the Atlantic, it encountered divergent regulatory climates in the U.S. and Europe. European countries were committed under the EU Data Protection Directive[72] to a rights-based implementing framework with local Data Protection Authorities (DPAs) to monitor its application.[73] The DPAs, some of whose existence dated from 1970's, were also organized around a rights-based framework.[74] Thus, in Europe the shift in privacy rhetoric occurred against a well-developed framework and growing set of institutional players committed to conceptualizing information privacy through a lens of "data protection."[75]

---

[67] Bennett & Raab, *supra* note 1 at 49.

[68] OECD, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet* 4 (May 22, 1998), http://www.oecd.org/dataoecd/33/43/2096272.pdf.

[69] *Id.*

[70] White House, *Framework*, *supra* note __ at 12-14 (describing privacy protection as essential, but that privacy should not inhibit the free flow of information; self regulation is the way). .

[71] Bennett & Raab, *supra* note 1 at 50.

[72] Available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[73] Directive, Article 28.1

[74] *See* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 74-98 (2008) (arguing that the adoption of the EU Directive itself is rooted in the "historical sequencing of national data privacy regulation and the role that the resulting independent regulatory authorities played in regional politics").

[75] For a discussion of EU member states' laws and the process leading up to the directive, see, Fred H.Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33

By contrast, the information privacy landscape in the United States was more of a *tabula rasa*. Its patchwork system reflected no deep commitment to a specific implementation framework, and no institutional authority vested in defending a specific approach. Against this backdrop, the expression of privacy's value in terms of promoting consumer trust proved influential in the U.S. in a way that rights-based arguments had not. Historically, successful legislative efforts, with a few notable exceptions, were mounted in response to specific and egregious harms or to protect highly sensitive information. Advancing privacy as a matter of individual rights, generically, across the corporate sector, had little legislative or regulatory traction. By contrast, legislators and regulators were relatively quick to join a conversation about addressing privacy risks to advance electronic commerce.

Consumer confidence and trust became a central theme of arguments both for and against new privacy regulations in the U.S. On the one hand, consumer advocates employed such arguments in promoting a regime of new privacy laws. Advocates claimed that in the absence of robust privacy protection individuals would be "more fearful to disclose information"[76] and would retreat from shopping or banking online.[77] Consumer groups warned that "the full economic and social potential of global electronic commerce will only be realized through its widespread use by consumers," and "such use will only occur if consumers become confident and comfortable with the online world."[78] Business groups, on the other hand, employed this new rhetoric to support a self-regulatory agenda, stating that "building consumer confidence is a key issue for the development of electronic commerce"[79] and claiming "There is a business advantage to be gained by companies that safeguard consumer interests."[80] When the Federal Trade Commission sought public comments in preparation for a consumer protection workshop in 1999, sixty-nine companies, nonprofits and individuals responded—some in

---

INDIANA L. REV. 33 (1999).

[76] John Schwartz, *Health Insurance Reform Bill May Undermine Privacy of Patients' Records*, WASH. POST, Aug. 4, 1996, at A23 (quoting Denise Nagel of the National Coalition for Patient Rights, who was responding to the recently-passed Kennedy-Kassebaum health insurance reform bill, which mandated the creation of a national computer network among health care providers, who were required to participate).

[77] Robert O'Harrow Jr., *White House Effort Addresses Privacy; Gore to Announce Initiative Today*, WASH. POST, May 14, 1998, at E1.

[78] Letter from Frank C. Torres, III, Legislative Counsel to Consumers Union, to the Federal Trade Commission (Mar. 26, 1999), http://www.ftc.gov/bcp/icpw/comments/conunion.htm (these folks favor further rules and standards with regard to privacy, and they, too, use consumer trust to bolster their arguments).

[79] Global Business Dialogue on Electronic Commerce, *The Paris Recommendations* 6 (Sept. 13, 1999), http://www.gbd-e.org/pubs/Paris_Recommendations_1999.pdf (further evidence that the business community embraced at least the rhetoric of consumer trust).

[80] Alliance for Global Business, *Global Action Plan for Electronic Commerce* 22 (Oct. 1999), http://www.iccwbo.org/policy/ebitt/display7/folder85/index.html

favor of self-regulation, and others arguing for new rules, but nearly unanimous in stressing the importance consumer trust.[81]

The link between privacy, trust and commerce, moreover, was underscored by repeated consumer pushback after corporate privacy blunders. "Consumer concern about privacy [had] the attention of Corporate America."[82] Companies announced information-sharing deals only to cancel them once masses of consumers made their objections known.[83] In July 1997, AOL scrapped a plan to sell subscribers' phone numbers to marketers.[84] Other high-profile reversals followed: in 1998, American Express pulled out of a partnership with KnowledgeBase Marketing that would have made the personal data of 175 million Americans available to any retailer that accepted the charge card.[85] In 1999, Intel reversed a plan to activate an identifying signature in its Pentium III chip faced with advocacy filings with the Federal Trade Commission, pressure from industry partners, and a boycott.[86] And in 2000, a plan by DoubleClick, the dominant network advertising service, to combine clickstream information with personally identifiable information in a massive customer database it had acquired for the purpose of delivering highly customized and targeted advertising was shelved. DoubleClick withdrew its plan due to public pressure.

While disputes over the optimal way to build trust waged on—consumer advocates favoring a regime of new privacy laws, the Administration and industry groups favoring industry self regulation—all players increasingly framed their arguments in favor of privacy protection in instrumental terms—the crucial role privacy played in enabling electronic commerce and e-government. This fit well with the Administration's predilection for market driven solutions, the regulatory powers of the Federal Trade Commission which was staking out its agenda in the privacy space, and the agenda of pragmatic advocates keen to promote reforms by utilizing available regulatory fora.

### C. Regulatory Developments and the Consumer-Oriented Privacy Frame

#### 1. The Federal Trade Commission and the Consumer-Protection Discourse

---

[81] List of Commenters in Preparation for a Federal Trade Commission Workshop on U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace (1999), http://www.ftc.gov/bcp/icpw/comments/ (listing all commenters and links to their comments; nearly every comment makes at least a passing mention of consumer trust before launching into their vision of privacy protection).

[82] Bruce Horovitz, *AmEx Kills Database Deal after Privacy Outrage*, USA TODAY, July 15, 1998, at 1B (describing the scrapped AmEx deal, and at the end of the article listing other companies "that recently changed course after consumers balked").

[83] *See, e.g., id.*

[84] *Id.*

[85] *Id.*

[86] Jeri Clausing, *The Privacy Group that Took on Intel*, N.Y. TIMES, Feb. 1, 1999, at C4 (describing a successful grassroots campaign to force Intel to reverse its plans to activate an identifying signature in the Pentium III chip).

It is in this context that the Federal Trade Commission emerged,[87] in the words of one of our respondents, as an "activist privacy regulator," engaging the broader privacy community in a conversation about privacy's meaning through its consumer-protection lens.[88] "We recognized," explained former FTC Chairman Robert Pitofsky, speaking about his time at the agency, "that the Internet was a vast new marketplace that could provide great benefits to consumers and to the competitive system. The idea was to protect consumers without undermining the growth of electronic commerce. A special dimension of commission activities related to concerns about on-line privacy."[89]

*a. Jurisdictional Entrepreneuship*

This development was not predetermined by the terms of the Commission's statutory mandate to police "unfair or deceptive acts or practices."[90] As Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection from 1995-2001, remarked, "It didn't quite fit into 'deception or unfairness' for us to say, 'Everybody out there ought to be required to protect people's privacy.'" [91] Thus, she explained, "I didn't go through any big deal process in terms of saying, 'Yes we're policing the Internet.'"[92] But the

---

[87] The FTC had developed expertise on privacy as the agency responsible for rulemaking and enforcement under several sectoral statutes including, Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (addressing the accuracy, dissemination, and integrity of consumer reports); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 et seq. (including the Telemarketing Sales Rule, 16 C.F.R. Part 310) (prohibiting telemarketers from calling at odd hours, engaging in harassing patterns of calls, and failing to disclose the identity of the seller and purpose of the call); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq. (prohibiting the collection of personally identifiable information from young children without their parents' consent); Identify Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (directing the FTC to collect identity theft complaints, refer them to the appropriate credit bureaus and law enforcement agencies, and provide victim assistance). For an overview of the FTC's power's under specific grants of authority, including several enacted during the late 1990s, *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW, 777-82 (2009) and RICHARD C. TURKINGTON AND ANITA ALLEN-CASTELLITTO, PRIVACY LAW: CASES AND MATERIALS, 428, 476-488, 492, 496-500 (2002).

[88] *See, e.g.*, Christine A. Varney, Commissioner, FTC, Prepared Remarks on *Privacy in the Electronic Age* at the Privacy & American Business National Conference (Nov. 1, 1995)http://www.ftc.gov/speeches/varney/varnprvy.sthm (making the point that the FTC is grappling with questions about how best to approach privacy in the information economy).

[89] Oral History of Robert Pitofsky Sixth Interview March 30, 2004 p. 155.

[90] 15 U.S.C. § 45.

[91] Oral History of Joan (Jodie) Z. Bernstein – Seventh Interview, May 1, 2000 p. 240. For an overview of the FTC's activities through 1996 see, Consumer Privacy on the Global Information Infrastructure, Staff Report, Federal Trade Commission (1996), for an overview of completed and planned work as of 1999 see Self-Regulation and Privacy Online, Prepared Statement of the Federal Trade Commission, presented by Chairman Robert Pitofsky before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate July 27, 1999.

[92] *Id.*

substantive imprecision and procedural breadth inherent in the FTC Act left the agency the space to play an increasingly important role in framing the debate. "There were internal discussions about how to handle it," Bernstein continued, "and from that came our concept of convening forums on privacy issues on the Internet very early and to articulate our program. Then we did the first survey of what was happening to the personal privacy on the web sites, encouraging self- regulation, [and learned that] the privacy issues are real hot right now."[93]

Thus, beginning in 1995 with a public workshop to identify the consumer protection and competition implications of the globalization and technological innovation at the core of the internet revolution, and continuing with similar programs over the following several years, the FTC began to chart its own privacy agenda.[94]

These initiatives were strengthened as the EU Data Protection Directive's effective date of 1998 loomed, and the issue of the "adequacy" of U.S. law became a pressing trade matter. In light of the Directive's prohibition on the transfer of data to companies in jurisdictions which failed the test of "adequacy"—which included as the United States—U.S.-based multi-nationals, and other firms with a global presence, or substantial foreign markets feared the economic consequences. These fears led to the initiation of negotiations to develop a "safe harbor" framework, by which individual U.S. firms could sign-on and thereby demonstrate privacy practices sufficient for trade with European partners.[95] These negotiations culminated with the EC approval of the "Safe Harbor Privacy Principles" (Safe Harbor) in July 2000.[96]

Throughout the extended and contentious process of negotiating the Safe Harbor agreement heavy pressure was on U.S. industry to evidence meaningful capacity to self-regulate and for the U.S. to provide evidence of meaningful oversight, enforcement and mechanisms for redress. Struggling with the need for credible oversight and enforcement structures for privacy, but unwilling to craft either omnibus regulations or to push for the creation of a data protection authority, and faced with limited industry support and participation in self-regulatory activities with credible enforcement, the Administration and industry turned to the Federal Trade Commission to fill this gap. A critical component of the Safe Harbor Agreement, then, was the commitment by the

---

[93] *Id.*.

[94] For an overview of the FTC's activities through 1996, see Federal Trade Commission, Staff Report, *Consumer Privacy on the Global Information Infrastructure* (1996); for an overview of completed and planned work as of 1999, see *Prepared Statement of the Federal Trade Commission: Self-Regulation and Privacy Online*, presented by Chairman Robert Pitofsky before the Subcommittee on Communications of the Committee on Commerce, Science, and Transportation, United States Senate (July 27, 1999).

[95] For an in depth discussion of the connection between the EU Directive and privacy developments in the U.S. and other countries see Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMP. L. & SECURITY REP. (2008).

[96] http://ec.europa.eu/dgs/internal_market/mission_en.htm (Last visited May 7, 2009)

Federal Trade Commission to enforce privacy statements and to prioritize complaints by EU citizens.[97]

With the Safe Harbor's signal, the FTC was now relatively insulated against suggestions that its nascent privacy activities were beyond its inherent authority. The Federal Trade Commission became a laboratory of privacy norm elaboration, seeking through its own and outside expertise, measurement, investigation, and sustained stakeholder engagement to define privacy's place in the new online market place, and its role as the leading consumer protection agency in shaping and enforcing practices to respect it.

The FTC was neither bound to, nor enabled by, traditional conceptions of data protection—for better and worse. However, it had substantial discretion to define what practices were unfair and deceptive.[98] As the Supreme Court observed as early as 1931, unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by . . . 'the gradual process of . . . inclusion and exclusion.'"[99] For "[n]either the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories."[100]

The agency, further, possesses wide latitude as to the institutional methods available for developing its perceptions of legal requirements. In the privacy arena, the FTC used convening and fact finding powers to facilitate a dialogue about corporate data practices, consumer understanding and expectations, and consumer harms. It convened Federal Advisory Committees[101] and workshops,[102] requested[103] and issued[104] reports,

---

[97] Article 1 ¶ 5 of the EC's Commission Deicison explicitly provides that " the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce, or that of another statutory body that will effectively ensure compliance with the Principles." (EC Commission, July 27, 2000). *See also* Priscilla M. Regan, *Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows*, 59 J. SOC. ISS., 263-282 (2003) (discussing national and international politics related to the adoption of the Safe Harbors).

[98] See Federal Trade Commission Act, 15 U.S.C. § 41 et seq. (prohibiting deceptive or unfair acts or practices), and Federal Trade Commission, *Statement on Unfairness* "The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time"); Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305 (2001) (discussing congressional delegation and court deference that results in FTC's ability to define deceptive practices); Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Rule Model*, 52 OHIO ST. L.J. 437, 440-45 (1991) (discussing FTC's broad interpretative authority).

[99] *FTC v. Raladam Co.*, 283 U.S. 643, 648 (1931).

[100] *FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 310 (1934).

[101] *See, e.g.*, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security, May 15, 2000.

worked with industry to develop self-regulatory codes of conduct,[105] and employed its enforcement powers to ratchet up demands on industry to be transparent about privacy practices, respect consumer understandings, and safeguard personal information.[106]

In contrast to the static requirements and prohibitions of U.S. sectoral statutes, FTC actions presented industry with an evolving set of privacy "norms," as the agency, in conjunction with the cadre of experts empowered by its activities, developed understandings of the meaning of privacy as a trade practice. The agency's broad statutory authority and its expansive institutional powers contributed to a growing imprecision about what it meant to satisfy the rhetorical measures of "privacy protection" and "consumer trust" in the online environment.[107] This, in turn, accorded the agency substantial capacity to shape the terms of the debate in a dynamic fashion.

*b. Developing a Consumer Expectations Metric*

i. Non-Enforcement Regulatory Tools

---

[102] The agency held fourteen public workshops on matters related to privacy between 1995 and 2004. Twelve related to unfairness and deception, one concerned financial privacy, and one credit reporting. *See* ftc.gov, Unfairness and Deception: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_wkshp.html; Financial Privacy: Financial Privacy Rule: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_wkshp.html (last visited Feb. 27, 2010); ftc.gov, Credit Reporting: Workshops, *available at* http://www.ftc.gov/privacy/privacyinitiatives/credit_wkshp.html

[103] *See, e.g.*, Report to the Federal Trade Commission by the Ad-Hoc Working Group on Unsolicited Commercial Email (1998).

[104] Since 1996 the agency has issued seventeen reports relating to privacy. The agency has issued seven staff reports and ten reports to Congress. *See* ftc.gov, Unfairness and Deception: Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/promises_reptest.html; ftc.gov, Financial Privacy: Pretexting Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/pretexting_reptest.html; ftc.gov, Children's Privacy: Reports and Testimony, *available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens_reptest.html.

[105] *See* FTC, *Individual Reference Services: A Report to Congress*, (1997); *Network Advertising Initiative: Self-Regulatory Principles For Online Preference Marketing By Network Advertisers* (2000).

[106] *See generally* Chris Jay Hoofnagle, *Privacy Practices Below the Lowest Common Denominator: The Federal Trade Commission's Initial Application of Unfair and Deceptive Trade Practices Authority to Protect Consumer Privacy (1997-2000)*, (January 1, 2001) (discussing the initial 5 cases brought by the FTC under their deceptive practices act jurisdiction).

[107] *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2053-54 (2001) ("The Agency has provided very little information, however, which would indicate the standards of fairness the Agency intends to apply," and therefore businesses have "little guidance as to how much is required of them in terms of providing notice, data security, data access, and determining what constitutes consent.").

Central to the FTC's emerging role as privacy regulator was its employment of regulatory tools outside the enforcement context, notably publicity, research, best-practice guidance, the encouragement of certification regimes, the enlistment of expert input, and other deliberative and participatory processes promoting dialogue with advocates and industry.[108] These tools furthered three types of regulatory goals.

First, they greatly increased the transparency of corporate privacy practices. Prior to these activities the invisibility of corporate practices, as noted by Smith's 1994 study, made them largely immune to regulatory and public pressure. FTC initiatives brought corporate practices into the light, and fueled a sustained debate about appropriate corporate norms of behavior on an issue that was previously addressed episodically, at best, by legislators in response to high profile privacy failures.

The agency conducted "sweeps" of both child-directed and general audience web sites to assess information practices. It encouraged stakeholders to engage in their own research to document privacy practices on the internet which led to additional surveys of business practices online and consumer expectations. This focus on fact finding about corporate practices provided pressure for continuous improvement on industry, as initial sweeps provided a baseline for measuring improvement, or at times the lack thereof. The emphasis on best-practice improvement in turn provided an important tool for trade associations and self-regulatory organizations to use in corralling the business community to join forces to stave off the threat of regulatory action. Through a variety of measures, the Commission thus focused on developing a detailed public record of factual data about privacy-impacting technologies and related business practices, and how these practices in turn related to consumers' expectations and privacy concerns.

Second, the Commission employed its bully pulpit power to motivate two important developments. Its calls for credible self-regulatory efforts that provided meaningful redress for consumers and oversight and enforcement of policies were largely responsible[109] for the creation of two self-regulatory privacy seal programs[110] as well as a technical standards designed to reduce the transaction costs associated with privacy decision making by standardizing and automating the process.[111] Furthermore, Commission persuasion was critical in encouraging companies operating online to post

---

[108] *See generally* Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 YALE L. J. 64, 99-100 (2008) (discussing the capacity of agencies to provide a site for norm elaboration through deliberative and participatory processes outside the APA rulemaking or adjudication processes).

[109] Ongoing negotiations with the European Union over the "adequacy" of U.S. companies' privacy practices and U.S. law led to the creation of the Safe Harbor Guidelines. Companies that subscribed to the Guidelines would be considered to have adequate privacy protection for the sake of EU law and therefore would be able to receive data on EU citizens. In this context too, proving that remedies were available and that industry would be regularly policed through some oversight body was an important component of the agreement. Thus, the Commission's work was not the sole contributor to the creation of the seal programs.

[110] Truste, BBBonline.

[111] P3P, Tim Berners Lee & Deirdre K. Mulligan FTC presentation; Lorrie Cranor; Lessig.

privacy policies. The Commission's workshops and presentations, combined with publicity about privacy invasions occurring online, fueled this pressure. As discussed below, the publication of policies making representations about companies' practices with respect to personal information became central to the Commission's initial exercise of its Section 5 enforcement jurisdiction, because the least controversial manner for the FTC to exercise authority in the privacy area was to address factually misleading claims.[112] In addition to fueling the FTC's assessments, the visibility into corporate practices these policies provided facilitated a measurement of corporate privacy practices by legislators, advocates, and the press.

Finally, the FTC's participatory fora provided a space for a sustained conversation about privacy outside the bright lights of the congressional hearing rooms that empowered privacy advocates. Never before had privacy claimed a domestic institutional home as well resourced as the FTC, and the advocacy community quickly took advantage of the FTC's heft, filing numerous complaints about business practices[113], participating in Federal Advisory Committees[114] and workshops, and engaging in agenda-setting through the production of independent research[115] as well as interactions with FTC staff and Commissioners. The agency's policy fora provided low-cost, and relatively high profile, opportunities for advocates to shape the discourse about corporate data practices. Indeed, several privacy organizations and advocates appeared on the scene in the mid- and late-1990's focusing much, if not all, of their energy on FTC engagement.[116] Workshops accorded an opportunity for advocacy organizations to convey their views to

---

[112] *See* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046 (arguing based on public choice theory the FTC's promotion of privacy policies should be viewed as a means for "the Agency to sink its jurisdictional hooks more firmly into the Internet privacy debate, and therefore the Internet").

[113] *See, e.g.*, *Website*, ftc.gov (including press releases discussing five agency enforcement actions—against CVS Caremark, UMG Recordings, Microsoft, Eli Lilly, and Lisa Frank—initiated after privacy advocates or the media brought the matter to the FTC's attention) http://www.ftc.gov/opa/2009/02/cvs.shtm; BENNETT, THE PRIVACY ADVOCATES, *supra* note __, at 124-25, 152, 155, 160-61 (discussing four other actions triggered by complaints from advocacy groups.).

[114] *See, e.g.*, FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY-REPORT TO THE COMMISSION (May 15, 2000) (report of committee discussing mechanisms to afford consumers access to personal information collected and maintained by commercial Web sites, including representatives from Consumers Union, the Electronic Privacy Information Center, the Center for Democracy and Technology, the Electronic Frontier Foundation, as well as several privacy academics).

[115] *See, e.g.*, Center for Media Education, Report, WEB OF DECEPTION: Threats to Children from Online Marketing (1996); *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* (1998).

[116] For example, Junkbusters, a for-profit, privately held privacy advocacy firm founded in 1996, focused much of its activity on the FTC, *see* Amy Borrus, *The Privacy War of Richard Smith*, BUSINESSWEEK (Feb. 14, 2000) (containing FTC comments on the importance of Junkbuster founder Richard Smith's work).

a DC audience of reporters, hill staff, trade associations, lobbyists and industry executives. These contexts provided a formidable stage for advocates to serve as a mouthpiece for concerns about privacy risks faced by the diffuse and broad-based population of consumers nationwide.[117]

Advocates filed a steady stream of complaints with the FTC requesting investigations of corporate privacy practices testing and advancing the FTC's use of its deceptive and unfairness jurisdiction. [118] This level of activity contrasts starkly with advocates' pursuits in the far-more-costly realm of litigation; indeed, privacy organizations have rarely led court challenges to remedy privacy wrongs in the corporate sector.[119] Through a compelling FTC complaint an advocacy organization could leverage the resources, expertise, and investigative and enforcement capacity of a formidable agency. The publicity surrounding the filing of an FTC complaint could generate substantial scrutiny of corporate practices and might yield a related benefit by increasing the influence of the advocacy organization on the hill.[120] These complaints thus accelerated the dynamic the framing of privacy obligations, advancing from straightforward allegations of deceptive statements and unfair data practices[121] to novel complaints, such as those alleging that the assignment of unique identifiers to consumers' computers violated their expectations by putting them at unavoidable risk of

---

[117] *See generally* MANCUR OLSON THE LOGIC OF COLLECTIVE ACTION (1965) (articulating the public choice insight that concentrated groups enjoy a comparative advantage with respect to their ability to organize to advance group interests compared to groups facing diffuse, individually small benefits); George Stigler, *The Theory of Economic Regulation*, 2 Bell J. of Econ. & Mgmt. Sci. 3, 3 ((1971) (setting forth a model of interest groups and regulatory agencies by which "regulation is acquired by the industry and is designed and operated primarily for its benefit").

[118] The Center for Media Education (CME) filed the first internet related petition in May 1996, requesting that the FTC investigate Kidscom.com. While the FTC did not to file an enforcement action, its published letter evaluating Kidscom.com provided early notice of the agency's views on corporate data collection of children's information. *See* Letter from Jodie Bernstein, Director, FTC Bureau of Consumer Protection, to Kathryn C. Montgomery, President, Center for Media Education (Jul. 15, 1997) (concluding that collecting personally identifiable information from a child for a particular purpose when the information also will be used for another purpose that parents would find material, is a deceptive practice in the absence of a clear and prominent notice to a parent regarding the practice; and finding that parental consent must be obtained before a Web site that has collected identifiable information about children can release it to third parties) *available at* http://www.ftc.gov/os/1997/07/cenmed.htm *See also* BENNETT, THE PRIVACY ADVOCATES, *supra* note __, at 124-132 (discussing complaints in context of "naming and shaming" strategies); *id.* at 150-159 (discussing complaints against Intel, PSN, Doubleclick, and Microsoft Passport).

[119] *See id.* at 119-121.

[120]

[121] *See, e.g.*, *ACLU Complaint* (contending that Eli Lilly's disclosure of the email addresses of individuals receiving updates about Prozac constitute unfair trade practices in violation of section 5 of the FTC Act), *available at* http://www.aclu.org/technology-and-liberty/aclu-letter-ftc-re-eli-lilly.

privacy harms,[122] or targeting spyware and adware distributors, leading to enforcement actions discussed below.

In these fora, the FTC built support for its work and gained an ongoing awareness of the concerns of consumer advocates, and the ways in which consumer harms can arise from the breach of expectations wrought by the increased capacity and regularity of data collection—and a means publicizing them. Simultaneously advocates had a singular opportunity to shape an ongoing stakeholder dialogue in which the link between privacy, trust, and consumer expectation were nurtured—giving evolving content to imprecise rubric of privacy as consumer protection.

ii. Bringing Investigation and Enforcement Powers to Bear

These evolving consumer-oriented notions of privacy protection, in turn, were ultimately given force through the FTC's enforcement authority. As discussed above, the Commission's early cases focused on the accuracy of notices, targeting claims that were actively misleading. Then-Chairmen Pitofsky took a conservative view of the FTC's authority distinguishing the FTC's authority under section 5 from federal privacy statutes that "apply whether or not a privacy policy is posted" stating that "[o]nce posted, the privacy policy falls under the jurisdiction of the FTC, which uses existing laws to hold companies to the promises they make to consumers. In short, if a private sector web site does not post a privacy policy, there is no ready legal recourse available to an individual whose privacy has been violated."[123] Early enforcement actions followed suit, focusing on adherence to public statements related to a limited set of FIPPS principles tied directly into the creation of a functioning market for privacy that would limit the need for additional regulatory intervention—notably requirements of notice and consent.

This approach accorded with industry's expectation of the agencies exercise of authority. However, many in the privacy community pointed out the perverse disincentive this created for corporations to post privacy policies as it directed the FTC's action to what many believed would be the relatively good actors. As Joel Reidenberg wrote, "In an ironic twist, this public enforcement also provides a disincentive for greater

---

[122] *See* See In the Matter of Intel Pentium III Processor Serial Number: Complaint and Request for Injunction, Request for Investigation, and for Other Relief filed by the Center for Democracy and Technology, Consumer Action, and Privacy Rights Clearinghouse, *available at* http://netdemocracyguide.net/privacy/issues/pentium3/990226intelcomplaint.shtml.

[123] Remarks of FTC Chairman Robert Pitofsky, Hearing On Recent Developments In Privacy Protections For Consumers, House Subcommittee On Telecommunications, Trade And Consumer Protection (Oct. 11, 2000). Thus while two early investigations, one involving children, *see* FTC Guidance Letter in kids.com, *available at* http://www.ftc.gov/os/1997/07/cenmed.htm, and the other an anti-competitive practice that used personal information harvested from a competitors site in contravention of terms of service, s*ee* FTC Complaint in reverseauction.com inc, *available at* http://www.ftc.gov/os/2000/01/reversecmp.htm, included unfairness claims based on the inability of consumers to avoid substantial injury, the majority of early claims focused on affirmative misstatements of companies' data collection, use and disclosure practices.

transparency. A company risks liability by making a disclosure, but does not risk accountability by remaining silent."[124] The inability to police practices in the absence of a posted policy, accordingly, was perceived by advocates as an unacceptable gap in privacy protection.

As political support for improved privacy practices grew, resistance from industry waned—perhaps due to the FTC's central role in reducing tensions with the EU over cross-border data flows— and the perceived inequity of "extra policing for the good guys", the FTC approach broadened. The agency increasingly directed its enforcement focus on practices deemed "unfair"[125] and transactions that were on the whole misleading despite legal disclosures. This change in regulatory approach unraveled settled understandings of the agency's requirements regarding corporate privacy practices. If earlier enforcement actions aimed at holding companies to their word provided some precision as to rules of conduct, the new legal standards employed by the agency to protect privacy in the face of new technologies, new corporate behaviors, and new threats, were far more ambiguous, evolving, and context-dependent. This development is seen strikingly in the agency's actions to address two phenomena: spyware, and data breaches.

Spyware—a type of software that is typically installed on a computer without the user's knowledge, and collects information about that user—presented an important conceptual challenge to the FTC's policing of privacy, and to industry intent on distinguishing the good actors from the bad through adherence to procedural regularity. Companies distributing spyware often relied on the same fine-print legal disclosures as other companies to inform consumers of their data practices. The difference was that their practices diverged even further from consumers' expectations of the bargain they were striking than those of other market participants, and therefore put consumers at risk. No longer did it make sense that providing a legal disclaimer and click-through "consent" screen should suffice to evade FTC scrutiny.

In a series of actions against companies that downloaded software without appropriate notice and consent procedures[126] the Commission began to breathe substance into the process of consent. The majority of these cases involved "bundled software,"[127] where formal disclosures in end user licensing agreements (ELUAS) were

---

[124] Joal R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L. J. 886, 886 (2003).

[125] *See, e.g.*, FTC v. GM Funding, Inc., et al. (C.D. Cal. 2002).

[126] FTC v. Seismic Entm't, Inc., 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (holding FTC was likely to succeed on the merits because it is an unfair practice to exploit a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge and enjoining this method of software distribution); Analysis of Proposed Consent Order to Aid Public Comment, *In re* Advertising.com, USFTC File No. 042-3196 (Aug. 3, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (alleging that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

[127] In "bundled" software offerings, the user understands that they are installing one program, but because they fail to read the EULA, and the software attempts to hide itself in other

found insufficient to provide notice of hidden software that eroded consumers' privacy in an unexpected manner, typically serving pop-up advertisements, collecting information about consumer's on-line "clicks", or engaging in another insidious data collection technique. Through its spyware work, the Commission broadened the range of practices that trigger privacy concerns to include software that collects and transmits information about users, their computers, or their use of the content in addition to information that is narrowly considered personally identifiable, and signaled that the existence of formalities that might establish consent in contract law[128] would not preclude the Commission's inquiry into the sufficiency of notice and consent where consumer privacy is concerned.[129] The spyware cases also established the principle that some practices were so at odds with consumer expectations that regardless of the consent experience, they were actionable.

FTC actions against companies failing to prevent the breach of personal information similarly abandoned a legalistic, notice-bound analysis. In these actions, the Commission brought unfairness claims against companies that had not made representations regarding data security.[130] While these cases have settled quickly, the resulting consent decrees have established that the failure to employ certain security processes and practices, such as addressing commonly known and well-understood security vulnerabilities and identifying and preventing security vulnerabilities that put customer information at risk, constitutes unfairness. Specifically, firms feel compelled to employ practices and procedures that provide a "reasonable" level of security to protect

---

ways, they fail to understand that they are in fact installing several different software programs and often creating relationships with several different companies. Typically these programs engage in invasive activities (pop-up or other forms of push advertising) or extractive activities (monitoring and data collection) which users presumably would avoid if given appropriate notice. *In re* Advertising.com, USFTC File No. 042-3196 (Sept. 12, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *See also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (holding that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

[128] See Deirdre K. Mulligan and Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERK. TECH. L. J. 1157, 1205-1211 (2007).

[129] For example, the order in the Sony BMG matter requires that the installation of software from a CD, and the transfer of information by such software, requires heightened "clear and prominent" notice and consent, Sony BMG Consent Decree (prohibiting downloads unless a consumer "dictates his/her assent to install such software by clicking on a button or link that is clearly labeled or otherwise clearly represented to convey that it will activate the installation, or by taking a substantially similar action").

[130] For example see, In re BJ's Wholesale Club, Docket No. C-4148, Decision and Order § I, available at http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf; In re DSW, Inc., Docket No. C-4157, Decision and Order, available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSCDecisionandOrder.pdf; and In re CardSystems Solutions, Inc., Docket No. C-4168, Complaint (Sept. 8, 2006), available at http://www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf.

users' personal information,[131] employing a legal standard that is notoriously fluid, responsive to market context (in terms of threats and mitigations), and open to change, evolution, and reinterpretation.

The ambiguity as to what privacy protection requires of corporations developed through FTC practice mirrors the sense the ambiguity articulated by the interviewed privacy leaders. It is easy to understand why these leaders believe that "privacy" requires "looking around corners" to anticipate ways in which new technologies, and new practices comport with consumer expectations regarding information usage. The agency's move to flexible standards, and away from data protection rules, has let loose a renewed conversation about privacy issues –whether unique identifiers and IP addresses warrant protection as personal information, whether behavioral tracking raises novel privacy questions, what security practices firms must have in place—and what firms must do to treat consumers fairly—meet their expectations—in the electronic marketplace.

2. State Data Breach Notification Laws and the Harnessing of Market Reputation

If the FTC sought, through a variety of "soft" and "hard" regulatory approaches, to publicize the risks posed by emergent technologies and market practices on the one hand, and link legal standards to the vindication of consumer expectations on the other, the passage of state data breach notification laws provided a single concrete mechanism for strengthening the link between privacy protection and consumer trust. As discussed earlier,[132] these laws—of which 45 have been enacted since 2002—require corporations to notify individuals whose personal information has been breached, in an effort to tie corporate privacy performance directly to reputation capital.

The breach notification laws embody a governance approach that emphasizes "informational regulation," or "regulation by disclosure."[133] Such tools require the disclosure of information about harms or risks as a means of "fortify[ing]" either "political checks on private behavior" or "market mechanisms."[134] In this case, disclosure requirements seek to prompt both—and while disclosures have provided important

---

[131] *See* MTS Inc., 69 Fed. Reg. 23,205 (Fed. Trade Comm'n Apr. 28, 2004) (proposed consent order) (failure to implement procedures that were reasonable and appropriate to detect and prevent "broken account and session management" vulnerabilities was unfair or deceptive given Tower Records's statements about attention to security and privacy); Eli Lilly & Co., 67 Fed. Reg. 4,963 (Fed. Trade Comm'n Feb. 1, 2002) (proposed consent order) (lack of proper controls to avoid disclosure of email addresses was unfair or deceptive given statements to the contrary).

[132] *See infra*, text at notes __-__.

[133] Cass R. Sunstein, *Informational Regulation and Informational Standing:* Akins *and Beyond*, 147 U. PA. L. REV. 613, 613 (1999) (describing the shift to such an approach as "one of the most striking developments in the last generation of American law").

[134] *Id.* at 614.

factual predicates for FTC enforcement, they have also subjected privacy outcomes to market and consumer discipline in important ways.

The breach notification laws transformed previously unnoticeable corporate lapses into press events with deep implications for brand. While the extent to which companies notified affected individuals of a security breach that exposed personal information prior to the advent of the security breach laws is unclear, and difficult to assess systematically, very few press stories predating their enactment mention customer notification of breaches,[135] and both survey and anecdotal evidence (along with the fact that industry groups strongly objected to notification requirements on cost grounds)[136], support the conclusion that the security breach laws drove consumer notification well beyond prior practice in industry.

The notices moreover, have permitted privacy advocates to exploit media coverage in ways that keep public conversations about privacy and data protection on the front burner. Thus the Privacy Rights Clearinghouse maintains a chronology of data breaches, [137] while U.S. PIRG and Consumers Union have leveraged the steady drumbeat of security breaches to build momentum for the proliferation of model laws across states.[138]

By these mechanisms, in the words of one respondent, notification laws lead corporations to "[t]ry to avoid the breaches and the problems and the brand tarnishment issues and promote the ability to use and flow data in a proper way and make it a competitive advantage . . . ." While reported security breaches involving personal information result in both an immediate short-term impact on firms' stock price,[139] and direct remediation and litigation costs[140]—recently calculated at $197 per record breached[141]—the bulk of the penalty to firms arises from lost business, a phenomena that has nearly doubled between 2005 and 2007.[142] Lost business represents the costs related to customer "churn," or turnover, as well as increased costs of customer acquisition. These costs directly reflect consumer pushback arising from perceived failures in the

---

[135] *But see, e.g.*, *Travel Web Site Admits To Security Breach*, USA TODAY (Jan. 24, 2001) (describing Travelocity's email notification sent to 45,000 affected customers); Sarah Left, *Web Security Breach Forces Users To Cancel Cards*, THE GUARDIAN (June 22, 2001) (describing notice to 27,000 customers of exposure of credit card and other personal details).

[136] Jaikumar Vijayan, *Consumer Groups Rail Against Proposed Data-Breach Notification Law*, COMPUTERWORLD (March, 16, 2006) (discussing industry efforts to pass less stringent laws).

[137] http://www.privacyrights.org/ar/ChronDataBreaches.htm

[138] http://www.uspirg.org/financial-privacy-security/identity-theft-protection

[139] *See* Alessandro Acquisti, *et al.*, *Is There a Cost to Privacy Breaches? An Event Study*, Proceedings of the International Conference of Information Systems (ICIS) (2006) (discussing an impact of short duration, a 0.6% reduction in stock price on the day the breach is reported).

[140] *See* Joris Evers, *Break-in Costs Choicepoint Millions*, CNET NEWS (July 20, 2005).

[141] Larry Ponemon, 2007 Annual Study: U.S. Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventative Solutions (2007)

[142] See id.

protection of personal information, and directly affect the way in which privacy failures undermine trust and brand. But for the notification requirements of the law, it is highly unlikely that customers would have knowledge of the breach and place market pressure on companies to improve security practices. The consumer expectation rubric revealed in our interviews thus reflects an increasing reality prompted by the security breach disclosure laws and which in turn resonates with an evolving conversation linking trust, brand image and privacy.

Finally, the SBN laws created an incentive structure that drove companies to develop internal processes to manage risk.[143] The laws provided CPOs with a powerful performance metric, both internally and with respect to peer institutions. The CPOs we interviewed reported summarizing news reports from breaches at other organizations and circulating them to staff with "lessons learned" from each incident, and explained that that breaches at other organizations help justify expenditures for implementing new protocols within their own organizations. In the words of one respondent, "the breach news . . . was so loud that it didn't take much to get the attention of our senior executive on data security, kind of as part of the privacy program." Another reported, "[the security breach laws] enriched my role; it's putting more of an emphasis on leadership internally in a very operational sense." The visibility of privacy failures thus enhanced internal resources; as one CPO described, "we're now in the process of rolling encryption across all of our laptops. It's the right thing to do and I'm very glad we're doing it but, if it wasn't for the security breach laws in the U.S., we wouldn't be doing it. I don't think any company would be. It's what drove it."

D. The Turn to Professionals

While the rhetoric of privacy as trust was no doubt appealing to corporate privacy officers trying to gain traction within their organizations—as it was for regulators attempting to motivate industry to take privacy seriously or face a barrier to electronic commerce—the combination of uncertainty as to the FTC's evolution of privacy requirements, and as to market responses spurred by data breach notifications was central to the striking trend towards corporate reliance on professional privacy management described in Section 2.B.

Professionalism has long served as an important institution for mediating uncertainty in the face of environmental ambiguity,[144] And in the privacy context,

---

[143] *See also* Deirdre K. Mulligan & Joseph Simitian, "Security Breach Notification Laws: A Race to the Top?" (unpublished manuscript on file with the authors) (identifying similar impact of SBN laws in areas such as asset management, portable media encryption and the development of best pratices).

[144] *See generally*, Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*. 53 AM. ECON. REV. 941, 947 (1963) (describing how physician professionalism was an intermediating "nonmarket social institution" that compensated for uncertainty in the context of the severe information asymmetry between market actors); Lauren B. Edelman, *Legal Ambiguity and Symbolic Strustures: Organizational Mediation of Civil Rights Law*, 97 AM. J. SOCIOL. 1531 (1992) (discussing the importance of professionals in mediating legal ambiguity within organizations).

increasing ambiguity as to the future behavior of both regulators and market forces prompted a parallel escalation in the reliance on internal corporate experts, grounded in knowledge and experience of privacy regulation's trajectory, to guide corporate practices and manage privacy risk.

Our interviews reflect this risk-management orientation by their forward-looking focus on identifying future challenges, rather than on compliance with existing mandates. They also underscore the potential for environmental ambiguity, combined with credible threats of meaningful sanction, in affecting the scope of the privacy function within corporate organizations; our respondents described a broad reach throughout the corporation, authority to participate in strategic decisions about the firm business, and a relatively wide latitude to establish corporate practices and define their jobs. In words attributed to one corporate employer: "we want to have a wonderful privacy program and you tell us what that means."

## IV. THE IMPLICATIONS FOR POLICY DEBATES

By this account of privacy "on the ground," the dramatic rise in corporate resources and attention accorded privacy management since 1998, and its development of privacy frameworks to guide decisionmaking in new contexts, tracks a transformation of the privacy field more generally. While the dominant account of U.S. privacy regulation—of privacy "on the books"—correctly argues that U.S. law fails to provide the robust FIPPS protections and comprehensive rule- and enforcement- structures developed in Europe, the alternative account illuminates the concurrent entry of a new force into the regulatory space—the Federal Trade Commission—and the way in which its activities, together with the involvement of advocates, professionals, and market forces, framed a new discourse regarding privacy protection. Far from reducing uncertainty in the legal field, that agency's "soft" regulatory tools and "roving" exercise of enforcement power increased legal ambiguity. But in doing so, they contributed to the augmentation of the discourse around privacy from one focused on procedural mandates to one that includes a substantive measure: the vindication of consumer expectations regarding the treatment of personal information.

Grounding the debate over the U.S. privacy-protection framework has deep implications for public policy, at a time that the Obama Administration and Congress are considering an overhaul of federal privacy statutes, and the OECD reconsiders global privacy approaches on the occasion of the thirtieth anniversary of its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[145].

These implications, first, touch debates over how privacy is framed. We have no truck with those who argue for strengthening procedural methods of protecting personal information. Yet the grounded account of privacy casts into relief the incompleteness of

---

[145] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*', *Organisation for Economic Cooperation and Development*, (1980).

a reliance on formal notice, consent and information alone to protect against real harms as rapid technology changes reduce the power of individuals to isolate and identify the use of data that concerns them. It suggests the frailty of a procedural understanding of privacy protection in guiding corporate decisionmakers, *ex ante*, in making choices about the technologies they employ in products or processes. And it indicates that a combination of field participants have refocused on a substantive approach of privacy protection that important theorists suggest best vindicate individual and societal interests: one that emphasizes objective expectations over subjective formalism, dynamism in the face of technological and advance, and application by context.

Moreover, the account of privacy on the ground offers important lessons for debates over regulatory form. While traditional regulation eschewed uncertainty in favor of regulatory specificity, more recent governance approaches increasingly experiment with ambiguous mandates, "delegating" to regulated parties greater discretion in fulfilling legal goals.[146] Nonetheless, such regimes can produce merely "symbolic" or "cosmetic" self-regulation, as participants in the legal field shape understandings of conformity that undermine or contort the public goals they purport to advance. The account of privacy on the ground, however, describes a regulator's deployment of a broad legal mandate by means of a suite of "New Governance" approaches—measurement, publicity, learning, dialogue, and process, as well as credible, yet indeterminate and evolving, threats of enforcement—in a way that centered the public voice in shaping both the law's framing and the "compliance-plus" mindset reflected by the interviewed privacy leaders. In this context, the account suggests, a substantive approach to privacy, increased executive attention, and the corporate privacy management's move from the legal compliance office into product and business decisions arose because, rather than in spite, of regulatory ambiguity.

### A. Implications for the Substantive Debate Over Privacy Regulation

The emergence of consumer expectations as a measure with which to judge privacy protection introduces an independent overlay to a legal framework that otherwise relied on the formal satisfaction procedural indicia of consent. In framing privacy's meaning and what values it serves, this new measure adds a rubric rooted in substantive norms, social values, and evolving community practice, to existing approaches emphasizing procedural tools, individual autonomy, and personal choice.

This overlay does not deny the value of formal notice, information, and consent protections; rather, it eliminates the presumption that the existence of procedural mechanisms are conclusive of an interaction's fairness. Thus while the FTC's early actions focused on enforcing the bargains between individuals and corporations—regardless of their content—later actions found certain practices to be unreasonable regardless of individual "consent" by means of the standard click-wrap processes generally upheld by courts. Unfairness and deception concern whether a practice,

---

[146] See Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 377 (2006).

including the notice that accompanies it, falls outside some acceptable level of deviation from, past consumer experience. Those inquiries rely on understandings that consumers bring to an transaction—the "mental model" they have of information "flows?"—and whether a practice is unexpected in light of those understandings, and therefore violative of public policy. As a conceptual matter, a notion of privacy as a public policy or social value is superimposed over existing notions of its link to individual autonomy. As a practical matter, new or unanticipated information flows will trigger legal scrutiny.[147]

By diversifying legal understandings of privacy,[148] then, the development of the consumer expectations rubric provides an additional protection framework that scholars from diverse fields suggest can provide a more robust conception of privacy values deserving of defense; a framework that offers a means to identify privacy problems *ex ante* in contexts that procedural protections cannot; a framework that is not reflected FIPPS principles.

As these scholars explore, defining privacy as "informational self-determination" at once claims too much, and protects too little. By its emphasis on choice, this definition recognizes that privacy's requirements can vary by context; for example, information will be appropriate to share in some contexts, with some recipients, and for some purposes—but not others. Yet the notion that law should provide individuals with a common set of mechanisms for vindicating privacy, the animating principle behind the push for "omnibus" regulations, requires that "information privacy policy [be] based inevitably . . . on procedural, rather than substantive, tenets," by which "individuals can assert their own privacy interests and claims if they so wish," and "the content of privacy rights and interests have to be defined by individuals themselves."[149] As such, the substantive interest in the protection of privacy values is transformed into a "right" to procedure.

Even on its own terms, this procedural definition places prohibitive costs, and unrealistic expectations, on privacy's actualization. One recent study demonstrated that an average person would expend between 91 to 293 hours per year were they to skim the privacy policy at each website visited, and 181 to 304 hours if they actually read them.[150] . In real terms, then, even the procedural right is often an empty one.

---

[147] This formulation of privacy bears some semblance to the two-part test used in Fourth Amendment cases. *See* Katz v. United States, 389 U.S. 347 (1967). However, unlike that jurisprudence's "reasonable expectations" test, under which the very existence of new surveillance and data-collection technologies generally eroded the sphere of reasonable expectations, the FTC's formulation is protective in its bias—the expansion of surveillance and information-collection capacity in new ways is understood to signal unanticipated information flows and the loss of privacy that may flow from them.

[148] *See* DANIEL SOLOVE UNDERSTANDING PRIVACY 187 (2008) (discussing the "Benefits of a Pluralistic Understanding of Privacy").

[149] COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 9 (2006).

[150] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. OF L. & P. FOR THE INFO. SOC., (2008) (the ranges reflect the low, point and high estimates they arrived at through study for skimming and reading policies). The study ultimately concludes that reading

More generally, the mindset of data-protection through procedural mechanisms is mismatched to paradigm changes in the technology landscape; it is "not quite able to conform to the ebb and flow of anxieties that these systems and practices provoke."[151] Framing privacy protection as mechanisms facilitating discrete decisions regarding access to or acquisition of data places the substantiation of privacy's meaning in an individual's hands at one particular time, without knowledge or foresight about the changes in information treatment that future technologies and practices will bring.

This framing, moreover often provides no "decision heuristic,"[152] no substantive touchstone, to guide the choices of those with far greater power to shape privacy's treatment: corporate actors shaping the systemic decisions about design choices that impact information usage. Most simply, decisions at the corporate level might provide the best way to avoid privacy harms.[153] But perhaps more pervasively, providing a substantive metric to guide such systemic decisions recognizes the fact that the values embedded in technology systems and practices shape the range of privacy-protective choices individuals can, and do, make regarding interactions with those systems and practices.[154] Technology can both be shaped and shaped by, social context.[155] An abdication of the opportunity to provide a substantive decision heuristic for technology shapers, therefore, permits other interests to limit the very choices that a "self-determination" emphasis suggests must be accorded to individuals.

The failure of "information self-determination" as a heuristic for corporate decisionmaking was emphasized in the comments from those chief privacy officers considering contexts characterized by the greatest technological change.[156] When

---

privacy policies costs approximately 201 hours a year at a vlue of $3,534 annually per American Internet user, or about $781 billion annually for the nation).

[151] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE 148 (2010). This is reflected the fears of scholars and advocates who find that data protection can lead to a reductive construction of privacy and therefore resist working "within any fixed and guiding definition of what privacy means," COLIN BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 18 (2008).

[152] NISSENBAUM, *supra* note __ at 148.

[153] *See generally*, GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970). (adopting Coasean insights regarding assigning liability to promote decisionmaking by the "cheapest cost avoider," and therefore the party best able to avoid harms).

[154] *See* Martin Heidegger, *The Question Concerning Technology*, *in* TECHNOLOGY AND VALUES: ESSENTIAL READINGS 99, 106–08 (Craig Hanks ed., 2010) (describing the way technology shapes a *Gestell*, or world view, that alters the perceptions of the decisionmakers it informs); *see generally* LAWRENCE LESSIG, CODE VERSION 2.0, at 5 (2006) (describing the regulatory power of "code"); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553, 554 (1998) (discussing the regulatory power of technological capabilities and system design choices).

[155] *See* Patrick Feng, *Rethinking Technology, Revitalizing Ethics: Overcoming Barriers to Ethical Design*, 6 SCI. & ENGINEERING ETHICS 207, 211–12 (2000) (describing the Science and Technology Studies insight that "technology both shapes and is shaped by its social context" (emphasis omitted)).

[156] *See supra*, text at nn. __-__.

dealing with business practices involving constant connectivity such as ubiquitous computing, in which information is sensed and exchanged as part of the product offering, or health technologies whose value derives explicitly from "get[ting] in the body," privacy must inform contextual, changing, and nuanced decisions about the very structure of the service provided, and procedural mechanisms are of limited use. In these contexts they have sought normative guidance from the evolving metric of consumer expectations.[157]

Philosopher and theorist Helen Nissenbaum describes the ways in which norms informed by social expectations can provide a far more robustly-protective frame for privacy than its definition as a set of one-off individual choices. The latter, she describes, encourages the mistakes of "moral mathematics" described by philosopher Derek Parfit.[158] A focus on informational "self-determination" limits the balance involved in privacy choices to the costs and benefits accruing to an individual decisionmaker. It thus precludes inquiry as to whether "my act [will] be one of a set of acts that will *together* harm other people,"[159]—and therefore ignores privacy's importance as a social good.

Nissenbaum explores the socially-situated nature of privacy, arising from the reality that "we act and transact not simply as individuals in an undifferentiated social world, but as individuals acting and transacting in certain capacities as we move through, in, and out of a plurality of distinct social contexts." [160] Each of these social contexts is governed by a set of norms derived from history, culture, law and practice. Such norms "govern key aspects such as roles, expectations, behaviors, and limits" in any given situation. They also provide two types of informational norms important to understandings of privacy: norms of information appropriateness and distribution. Norms of "appropriateness,"

> dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed.[161]

---

[157] Privacy scholar Priscilla Regan has documented, moreover, the ways in which internal corporate debates on privacy are more responsive to an available language of privacy as an enabler of some other collective social good, as opposed to as an individual right, *see* REGAN, LEGISLATING PRIVACY (1995).

[158] *See* NISSENBAUM, *supra* note _ at 242 (quoting DEREK PARFITT, REASONS AND PERSONS 86 (1986)).

[159] *Id.*; *see also generally*, Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 959 (1989) (offering a normative account of privacy that does not focus just on the protection of individuals, but also on protection of the community, and finding that privacy torts in the common law uphold social norms, which in turn contribute to both community and individual identity).

[160] *See* NISSENBAUM, *supra* note _ at 129.

[161] *Id.* at 140.

Norms of distribution, by extension, examine "whether [the information's] distribution, or *flow*" is consistent with context specific norms ranging from expectations of confidentiality and discretion to entitlement and obligation to reuse or re-disseminate.[162] Thus, as Robert Post has described, privacy norms "rest not upon a perceived opposition between persons and social life, but rather upon their interdependence."[163]

These norms vary by context and evolve over time, but at any one point embody the situational clues and understandings that inform individual cognition,[164] permitting efficient decisionmaking by precluding the need for individuals to engage in the impossible task of collecting and assessing all information anew.[165] From here derives the social value of expectations: when these understandings are upended, each of the participants in a social context will be deprived of accurate inputs for their decisions, resulting in unintended and unexpected, breaches in "contextual integrity,"[166] and therefore their privacy.[167]

The privacy-protective power of a substantive consumer expectations overlay onto procedural protections is reflected by a host of recent incidents in the privacy domain.

In some, expectations have provided a basis for fortifying notice and consent procedures themselves. The FTC's recent consent order with Sears Holding

---

[162] *Id*.

[163] Post, *supra* note __ at 959.

[164] *See generally* Mark C. Suchman, *On Beyond Interest: Rational, Normative and Cognitive Perspectives in the Social Scientific Study of Law*, 1997 WIS. L. REV. 475, 483 (describing the normative perspective on decisionmaking, which emphasize the selection of the norm that applies by first identifying the context as one in which the norm should prevail).

[165] "The capacity of the human mind for formulating and solving complex problems is very small compared with the size of the problems whose solution is required for objectively rational behavior in the real world," HERBERT A. SIMON, MODELS OF MAN 198 (1957) (emphasis omitted). "The human mind adapts to these shortcomings by developing unconscious cognitive shortcuts that generally make it easier to make sense of new situations even in the absence of complete information," Bamberger, *Regulation as Delegation*, *supra* note __ at 411. Thus rather than "maximizing," their choices, humans consider only a few possible courses of action and "satisfice[]," HERBERT A. SIMON, ADMINISTRATIVE BEHAVIOR xxix (3d ed. 1976), choosing to settle for a solution that is adequate.

[166] See Nissenbaum, supra note __ at 158-185.

[167] This focus on privacy as a social good finds resonance in the privacy advocacy community as well. While many advocates frame privacy in the context of protecting individual rights, others emphasize its value to society in limiting abuses by those with power, *see* COLIN BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE, 20-23 (2008). For these advocates the focus on data protection distracts from conversations about the responsibility of corporations to consider the privacy and human rights impacts of the technology they build, and services they offer, *see generally* John G. Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, GLOBAL INFO. TECH. REP., 69 (2006); *Website*, Global Network Initiative http://www.globalnetworkinitiative.org/

Management Corporation,[168] for example, targets the company's use of an email invitation to join their "MY SHC Community" and download a program that ran in the background on users' computers and transmitted information on virtually all of the users' Internet use to Sears, including web browsing, business transactions during secure sessions, completing online application forms, checking online accounts, and use of web-based email and instant messaging services—pushing against Nissenbaum's "appropriateness" norm. Specifically, it challenges the company's communications with users, which explained that "[t]his research software will confidentially track your online browsing," and only disclosed all the details about the function of its tracking software in a separate scrollbox. The scrollbox and standard click-through agreement used were of the kind generally upheld by courts. But the FTC decided that a detailed understanding of these unexpected practices reached such a level of materiality for consumers that it must be made "unavoidable" in consumer transactions.

Similar notions animate the response to practices surrounding the launch of Google's new social networking service, Buzz. That service's default options led, for many consumers, to the unexpected public disclosure—implicating Nissenbaum's distribution norm[169]—of the list of the people they email and chat with most frequently (including journalists' sources and therapists' patients). Rejecting outright the claims that formalities had satisfied privacy mandates, advocates and critics have both framed the nature of the violations, and rooted solutions, squarely in the language of expectations. Thus CNET's Molly Wood critiques,

> But I *do* have an expectation of privacy when it comes to my e-mail, and I think that even in this age of social-networking TMI, most people still think of e-mail as a safe place for speaking privately with friends and family. And for Google to come along and broadcast that network to the world without asking first—and force you to turn it off after the fact—is, I think, both shocking and unacceptable.[170]

In turn, writes Kurt Opsahl of the Electronic Frontier Foundation, the problem is that Google "failed to provide users with the setting users had reasonably expected."[171] Thus the appropriate privacy-protective behavior: "mak[ing] secondary uses of information

---

[168] In the Matter of Sears Holdings Management, File No. 082 3099 (FTC), *available at* http://www.ftc.gov/os/caselist/0823099/index.shtm

[169] *See e.g.*, Complaint of the Electronic Privacy Information Center, In the Matter of Google, Inc., ¶ 8, *available at* http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf ("While email senders and recipients always have an opportunity to disclose email-related information to third parties, email service providers have a particular responsibility to safeguard the personal information that subscribers provide.")

[170] Molly Wood, *Google Buzz: Privacy Nightmare*, CNET NEWS (Feb. 10, 2010), *available at* http://news.cnet.com/8301-31322_3-10451428-256.html.

[171] Kurt Opsahl, *Google's "Buzz" Should Have Required Consent For Secondary Use Of Private Information*, JURIST (Feb. 24, 2010) (commentary by Electronic Frontier Foundation senior staff attorney).

only with clear, unequivocal user consent and control, and test these controls to ensure that the default settings match with the expectations of the user."[172]

In other contexts, a consumer expectations framework has been used to protect privacy where technological changes render traditional reliance on consent inoperative. In light of advances in capacity permitting data storage for far longer periods than ever expected, for example, a recently released FTC staff report on behavioral advertising stated that, companies may "retain data only as long as is necessary to fulfill a legitimate business or law enforcement need"[173]—thereby removing data retention time frames from the private bargaining between individuals and corporations in the marketplace.

Finally, expectations provide a measure for privacy protection even in circumstances in which procedural protections are inapposite. An early example involves Intel's decision to attach a unique serial number to each Pentium chip. Considered against a background of a proliferation of device and application identifiers, the FIPPS principles had offered no indication that a serial number on a chip would raise a privacy uproar, or would trigger the need for procedural requirements. The Pentium serial number was not tied in any way to the type of personally identifiable information that at that time was typically the trigger for FIPPS requirements. Yet advocates singled the PSN out for the ease with which the number could be remotely and invisibly requested, and the possibility that the unique identifier would be used to track the actions of a computer across the internet. Because of Intel's market penetration and position in the internet ecosystem, and the ease with which even anonymized behavioral data can be used to detect individual identity,[174] the company had essentially embedded a tracking device in each computer—or in the colorful words of one advocate "branded (it) with an identifier."[175] If procedural protections could not address this concern, substantive encroachment on consumers' normative understandings did, leading to an FTC complaint, a call for a boycott, and advocate-generated pressure from computer manufacturers.[176]

B. Implications for Debates over Regulatory Form

---

[172] *Id.*

[173] FTC, Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 47 (Feb. 2009).

[174] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. (forthcoming 2010) (manuscript at 42–43, on file at http://ssrn.com/abstract=1450006) (discussing anonymization's failure to preclude reidentification techniques).

[175] Declan McCullagh, *Intel Nixes Chip-Tracking ID*, WIRED (Apr. 27, 2000) (quoting David Sobel, General Counsel, Electronic Privacy Information Center).

[176] The Center for Democracy and Technology asked equipment manufacturers (OEMs) for information about how the PSN would be implemented in their devices. Several responded indicating that they would provide users with greater control. For the history see http://opt-out.cdt.org/privacy/issues/pentium3/ ; for the letter to OEMs see http://opt-out.cdt.org/privacy/issues/pentium3/990216oem.letter.shtml for OEM default settings see http://opt-out.cdt.org/privacy/issues/pentium3/990414OEM.shtml

As much as the account of privacy on the ground can inform disputes over regulation's content, it also offers profound implications for debates over its form. Specifically, it provides important perspectives on questions regarding the optimal specificity of regulatory mandates regarding privacy, and regarding the institutional structures of privacy governance.

1. Debates Over Regulatory Specificity and Ambiguity

Traditional command-and-control regulation seeks to achieve particular outcomes by articulating, *ex ante*, uniform rules requiring certain conduct. Such a rules-based approach reflects faith in regulatory entities to be able to determine, in a top-down manner, the best means for achieving regulatory goals. Its emphasis on regulatory specificity permits little compliance discretion; regulated parties can either comply with requirements, or fail to do so. Moreover, the more "complete" the codification of behaviors, the more it anticipates possible contingencies, and direct behaviors accordingly.[177]

The shortcomings of command-and-control governance, however, are well recognized.[178] Rules are notoriously both under-and over-inclusive, identifying certain relevant factors that can easily be codified, while ignoring others. Specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals, such as reducing the types of risk produced by a combination of factors.[179] And specific commands reflect, in a static manner, their authors' beliefs about the best way to achieve general principles at the time of promulgation; as a tool, codified rules lack the agility to adapt to changing circumstances and new understandings.

For these reasons, reliance on compliance with a set of detailed provisions may frustrate, rather than further, underlying regulatory ends. Rule systems are inevitably incomplete, failing to provide guidance in a host of contexts, especially as circumstances change. At the same time, they can have detrimental effects on decisions within the organizations they govern, leading to a process of bureaucratization that results in "goal displacement," by which compliance with partial but specific rules—originally promulgated as a means for achieving a regulatory goal—becomes the singular end.[180] In particular, a bureaucratic "compliance"-oriented approach, by which rules of action are communicated in a centralized top-down fashion and intended to be applied by others

---

[177] *See generally*, JEREMY BENTHAM, A GENERAL VIEW OF A COMPLETE CODE OF LAWS (1802) (presenting the ideal of a "complete code").

[178] *See, e.g.*, Cass Sunstein, *Administrative Substance*, 40 DUKE L.J. 607, 627 (1991) (citing failures in using "rigid, highly bureaucratized 'command-and-control' regulation" to govern "hundreds, thousands, or even millions of companies and individuals in an exceptionally diverse nation").

[179] *See, e.g.*, Susan Sturm, *Second Generation Employment Discrimination: A Structural Approach*, 101 COLUM. L. REV. 458, 461 (2001) (discussing the problems with regulating the "complex and dynamic problems inherent" in workplace bias with "specific, across-the-board rules").

[180] *See generally* ROBERT K. MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 195-206 (1957) (discussing the process of "goal displacement," whereby "an instrumental value becomes a terminal value").

with little contextual knowledge, can disempower those within organizations who are charged with carrying out policies,[181] constraining internal pressures for greater resources and attention. It can alienate them from the goals behind the rules in favor of a focus on formalism, which in turn leads to a routinization of decision processes[182] that results in a greater number of human error events when implementing external regulation.[183]

The extensive literature on the economics of contracts identifies such problems with "complete" contracting—attempting to fully articulate terms *ex ante*—in situations of complexity and uncertainty.[184] In such circumstances, an instrument's terms should be left vague or unspecified, while assigning future decisions about how to resolve imprecision to parties that will, at the appropriate time, have best access to relevant information.[185]

These insights have shaped choices about regulatory design. Indeed, the past two decades have seen widespread experimentation with regulatory requirements framed in terms of broad principles rather than precise rules, and therefore that create greater ambiguity regarding appropriate methods of compliance.[186] In contexts as diverse as securities regulation, employment discrimination, and domestic terror protection,[187] policymakers have turned increasingly to general mandates rather than specific requirements in an attempt to deal with the complexity of the public goals at issue.[188]

---

[181] See Alfred A. Marcus, Implementing Externally Induced Innovations: A Comparison of Rule-Bound and Autonomous Approaches, 31 ACAD. OF MGM'T J. 235 (1988).

[182] *See* Bamberger, *Regulation as Delegation*, *supra* note __, at 445 (discussing studies indicating that making monitoring criteria well-specified and known to decisionmakers "exacerbates the substitution of cognitive shortcuts for reasoned judgment, and promotes routinized 'check the box' compliance").

[183] See Marcus, supra note __ at 235.

[184] *See generally* Robert E. Scott & George G. Triantis, *Incomplete Contracts and the Theory of Contract Design*, 56 CASE W. L. REV. 187, 191 (2005) ("In contract theory, incompleteness is due to the fact that information is costly and sometimes unavailable to (a) the parties at the time of contracting or (b) the parties or the enforcing court at the time of enforcement.").

[185] *See generally* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM: FIRMS, MARKETS, RELATIONAL CONTRACTING 34 (1985) (discussing "governance structures" put into place to resolve future contractual uncertainty).

[186] *See* Cristie L. Ford, *New Governance, Compliance, and Principles-Based Securities Regulation*, 45 AM. BUS. L. J. 1, 5 (2008) (contrasting principles-based regulation with "the more prescriptive and inflexible mechanisms associated with classical regulation"); Bamberger, *Regulation as Delegation*, *supra* note __ at 390-392 (discussing the increased reliance on regulation that "articulates general goals," yet "make[s] few *ex ante* decisions about substantive detail").

[187] *See* Ford, *supra* note __ at 1; Sturm, *supra* note __ at 461; Kenneth A. Bamberger, *Global Terror, Private Infrastructure, and Domestic Governance*, in 2 THE IMPACT OF GLOBALIZATION ON THE UNITED STATES: LAW AND GOVERNANCE 204 (2008).

[188] *See* Bamberger, *Regulation as Delegation*, *supra* note __ at 386-392 (discussing "The Trend Towards Regulatory Delegation").

This development has provided regulators with important tools for overcoming the challenges they face in identifying either threats on the ground or private information about firm organization necessary for developing uniform top-down requirements for risk-mitigating behavior.[189] Framing legal mandates broadly leaves space for discretion in implementation. By permitting heterogeneous and flexible methods of compliance in individual firm contexts, such framing provides a means for enlisting the judgment of firm decisionmakers, drawing on their superior knowledge both about the ways risks manifest themselves in individual firm behaviors and business lines, and about available risk-management capacities and processes.[190] It further accords regulators continuing flexibility in the face of uncertainty as to how public goals should be furthered in diverse and heterogeneous contexts, and quickly shifting landscapes over time.[191]

Yet scholars have also questioned the reliance on ambiguity as to the meaning of legal mandates as a regulatory tactic, pointing to numerous contexts suggesting this method's failure in achieving public goals. Most simply, eschewing specific top-down commands can render regulation hollow; regulated firms are freed from compliance with concrete measures, while resource constraints, industry pressure, and the complexity of the task, can derail regulators' efforts to give meaning to the broad language they are charged with enforcing. In these contexts firms are unrestrained both from incentives to expend effort in furthering public goals, and from the "external shocks" wrought by regulatory action and the credible threat of enforcement, the type of events that are frequently necessary to spur meaningful internal organizational change.[192]

Even when firms take compliance measures, scholars have argued, legal ambiguity can permit a form of evasive self-regulation. Specifically, the absence of specified requirements allows regulated firms to adopt practices that might appear to further the broad regulatory mandate, but are merely "cosmetic," in that they "do not deter prohibited conduct within firms and may largely serve a window-dressing function that provides both market legitimacy and reduced legal liability."[193]

---

[189] *See* Edward L. Rubin, *Images of Organizations and Consequences of Regulation*, 6 THEORETICAL INQUIRIES L. 347, 386 (2005) (describing fact that regulators often impose counterproductive measures because they lack knowledge of particular firms' internal operations).

190. *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 110–13 (1992) (describing the public and private benefits of an enforced self-regulation model, which takes advantage of the greater expertise and information of firm insiders).

[191] *See* generally, Vince Fon & Francisco Parisi, *On the Optimal Specificity of Legal Rules*, 3 J. INSTITUTIONAL ECON. 147, 147 (presenting a model of optimal specificity of laws suggesting the use of standards instead of rules in areas undergoing rapid change).

[192] See generally, Neil Fligstein, The Structural Transformation Of American Industry: An Institutional Account Of The Causes Of Diversification In The Largest Firms, 1919–1979, in THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS (W. Powell and P. DiMaggio, eds), 311 (1991) (discussing how 'external shocks' provided by legal institutions, macroeconomic conditions, or other organizations can provoke change in an otherwise stable field).

[193] Kimberly D. Krawiec, Cosmetic Compliance and the Failure of Negotiated Governance, 81 WASH. U. L.Q. 487 (2003); see also generally Kenneth A. Bamberger, Technologies of Compliance: Risk and Regulation in a Digital Age, 88 TEX. L. REV. __ (2010) (discussing the ways in which

These critiques are deepened by the contributions of socio-legal scholars exploring the way that legal and organizational "fields"[194]—the constellation of organizational actors participating in a particular domain—construct legal meaning in the face of ambiguity. Faced with an unclear mandate, firms have strong incentives to adopt "ceremonial"[195] compliance measures, procedures sufficient to signal "legal legitimacy" while simultaneously limiting law's impact on managerial power," or otherwise disrupting central firm structures.[196] Such practices, in turn, spread to other firms, which mimic what are perceived to be "successful" compliance models.[197] In such a fashion, compliance responses are institutionalized and ambiguous law is given contours.

In the employment context, for example, Lauren Edelman and others have traced the construction of compliance with equal opportunity laws such as Title VII's instruction that "[i]t shall be an unlawful employment practice for an employer . . . otherwise to discriminate against any individual . . . because of such individual's race, color, religion, sex, or national origin"[198]—language that "is ambiguous both in a legal sense and with respect to organizational policy."[199] In concert with "weak enforcement

---

technology systems that firms use to comply with broad risk-management mandates can "permit individual actors motivated by organizational incentives and individual greed to manipulate their behavior in ways that mask [risk]"); Kimberly D. Krawiec, Organizational Misconduct: Beyond the Principal-Agent Model, 32 FLA. ST. U. L. REV. 571 (2005) (arguing that organizations have perverse incentives to implement ineffective compliance programs); Lawrence A. Cunningham, The Appeal And Limits Of Internal Controls To Fight Fraud, Terrorism, and Other Ills, 29 J. CORP. L. 267, 335 (explaining that an emphasis on corporate internal control systems put into place to signal regulatory compliance with broad mandates "can lead controls to take on the character of ends in themselves, rather than means of achieving ultimate goals").

[194] *See* Lauren B. Edelman, *Overlapping Fields and Constructed Legalities: The Endogeneity of Law*, IN JUSTIN O'BRIEN, ED., PRIVATE EQUITY, CORPORATE GOVERNANCE AND THE DYNAMICS OF CAPITAL MARKET REGULATION 58 (2007) (defining a legal field as "the environment within which legal institutions and legal actors interact and in which conceptions of legality and compliance evolve"); Paul J. DiMaggio & Walter W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, 48 AM. SOC. REV. 147, 150 (1983) (defining an organizational field as "[t]hose organizations that, in the aggregate, constitute a recognized area of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products.").

[195] John W. Meyer & Brian Rowan, *Institutionalized Organizations: Formal Structure as Myth and Ceremony*, 83 AM. J. SOC. 340, 340–41 (1977).

[196] Shauhin A. Talesh, The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law, 43 L. & SOC. REV. 527, 533-34 (2009).

[197] New-institutionalist sociologists identify the process of three varieties of "isomorphism," by which understandings are diffused through an organizational field. "Mimetic" isomorphism, describes the process by which organizations respond to contexts in which goals are ambiguous and success difficult to measure by imitating others in the field who appear to be successful or legitimate, DiMaggio & Powell, *supra* note __ at 151-52.

[198] Title VII of the 1964 Civil Rights Act, section 703(a), 42 U.S.C. 2000e–2.

[199] Lauren B. Edelman, Legal Ambiguity and Symbolic Structures: Organizational Mediation

mechanisms" that provide "inadequate and inconsistent feedback on what organizational practices are legal," such laws thus leave regulated parties "wide latitude to construct the meaning of compliance."[200] In response, regulated organizations have focused compliance efforts on creating formal processes, including legalistic procedures for handling discrimination complaints. Such procedures appeal to legal norms by signaling an organization's "legality" but, because they are distinct from other firm structures, they can arise without the existence of fundamental alterations to existing workplace culture. These organizational responses to antidiscrimination law, in turn, spread throughout corporate practice, and were ultimately accorded deference by courts struggling for a metric to determine whether corporate practice satisfied the substance of the statute.[201]

By this process, the "right to a nondiscriminatory workplace in effect becomes a 'right' to complaint resolution."[202] Yet the right to complaint resolution "is far more superficial and entails fewer disruptions of routines than would a right to a nondiscriminatory workplace."[203] Legal meaning is resolved, but in a way that substitutes substance for process, and constrains law's effect. This phenomenon, moreover, track developments in a host of other contexts.[204]

2. Ambiguity in the Privacy Sphere

Debates over privacy regulation track these broader contests over regulatory form. Jeff Smith's study of privacy practices in 1994 concluded that the absence of clearly articulated legal aims and implementation strategies led to corporate inaction as CEOs avoided murky areas with unclear obligations and uncertain pay-off. "[T]he ambiguous corporate privacy domain," he concluded, was a primary driver of the "poor policy-making dynamic—the drift-external threat-reaction cycle"[205] in which firms avoided proactive privacy management, and executives only confronted privacy issues in face of specific, and limited, external threats. Ambiguity, moreover, was the condition "from which the other problems originate."[206] The trickle-down effect of a narrow focus only on compliance with specific mandates left employees charged with promoting privacy powerless to raise normative claims in tension with other organizational goals, leading to

---

of Civil Rights Law, 97 Am. J. Sociol. 1531, 1532 (1992).

[200] *Id*.

[201] Lauren B. Edelman, et al. Diversity Rhetoric and the Managerialization of Law, 106 AM. J. SOCIOL. 1589 (2001).

[202] Lauren B. Edelman et al., *Internal Dispute Resolution: The Transformation of Civil Rights in the Workplace*, 27 LAW & SOC'Y REV. 497, 529 (1993).

[203] Carol A. Heimer, *Explaining Variation in the Impact of Law: Organizations, Institutions, and Professions*, *in* 15 STUDIES IN LAW, POLITICS, AND SOCIETY 29, 41 (Austin Sarat & Susan S. Silbey eds., 1995).

[204] *See also*, *e.g.*, Talesh, *supra* note __ at 527 (describing a similar way in which "the content and meaning of California's consumer protection laws were shaped by automobile manufacturers, the very group these laws were designed to regulate.").

[205] SMITH, *supra* note __ at 167; *see generally id*. at ch. 6.

[206] *Id*.

an "emotional dissonance" that resulted in "redefining privacy"[207] in a manner that uniformly mitigated conflicts in favor of business profit. Contemporary critiques of privacy on the books echo these concerns, calling for greater specification of "command and control" privacy requirements across sector and practice.[208]

An account of privacy "on the ground," however, indicates otherwise. While in 1994 Smith viewed ambiguity as a "bug," this current account sees it as a "feature"—as a means for providing a space within which regulators could play an active role in catalyzing the privacy field's development of legal meaning that involved a variety of important institutional players, supplemented procedure with substantive heft, and has entailed far more robust, and more dynamic, corporate attention to privacy management.

A grounded account justifies the worries attendant to a singular reliance on highly-specified and proceduralized regulatory mandates. A recently–released multidisciplinary report reviewing the EU's Data Protection Directive, for example, finds that its focus on specific process rather than substantive outcomes "risks creating an organisational culture that focuses on meeting formalities to create paper regulatory compliance (via check boxes, policies, notifications, contracts . . . ), rather than promoting effective good data protection practices."[209] These findings track earlier research about the impact of the Privacy Act—the law governing the treatment of personal information by government agencies and the fullest embodiment of FIPPS in the United States context—by privacy law pioneer Ron Plesser. Plesser found that "agencies by and large find the Privacy Act, in short, to be an annoyance. There is usually a person or two on the General Counsel's staff of most agencies whose job it is to see that the agency or Government department complies with the technical requirements of the Act of in other words, stays out of trouble."[210] He reported that the one individual responsible for the Privacy Act in the Department of Health and Human Services spent, "most of his time guiding his 'clients' through the maze of the Privacy Act so that they can obtain their goals rather than as a voice for privacy in that massive agency, which deals with millions of privacy-related files every day."[211] In sum, he found the tendencies towards bureaucratization that rules can promote.

---

[207] *Id.* at 88

[208] *See supra* text at nn. __-__.

[209] Rand Europe, *Review of the European Data Protection Directive* 39 (2009) (commissioned by UK Information Commissioner's Office).

[210] David Flaherty, Protecting Privacy in Surveillance Societies quoting from *Who cares about privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Committee on Government Operations (Subcommittee on Government Information, Justice, and Agriculture) (Washington D.C., 1983) p. 237-238.

[211] David Flaherty, Protecting Privacy in Surveillance Societies quoting from *Who cares about privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress*, House Committee on Government Operations (Subcommittee on Government Information, Justice, and Agriculture) (Washington D.C., 1983) p. 237-238.

By comparison, the account of privacy on the ground has reveals a set of interactions that have amplified the "voice[s] for privacy" external to, and inside of, regulated corporations. Indeed, this account adds to an increasing number of studies that reveal the importance of purposive agency and "collective action" in shaping discourse in an organizational field to facilitate the construction of meaningful substantive regulatory norms.[212]

Central the construction of such norms were the activities of the Federal Trade Commission. The FTC's activity diverges from command-and-control governance, but also contrasts sharply with the "reticent regulator" approach that studies have found permits the subversion of public norms in organizational fields.[213] Specifically, its behavior adopts many of the methods that scholarship on "New Governance" models of regulation suggest will best leverage the strengths of legal ambiguity.[214] Such approaches emphasize dynamism and collaboration. They emphasize the regulator's ability to draws recurrently from "experience at the relatively local level" and changing challenges as they arise, in order "continually to update the standards all must meet,"[215] and its capacity to "harness the power of new technologies, market innovation, and civic engagement to enable different stakeholders to contribute to the project of governance."[216] As such, new governance is "both top-down and bottom-up."[217]

The Commission's emphasis on making privacy management practices and failures transparent, bolstered by the disclosures forced by state security breach legislation, surfaced metrics for assessing corporate activity over time,[218] and benchmarks

---

[212] Hayagreeva Rao, et al., *Power Plays: How Social Movements and Collective Action Create New Organizational Forms*, 22 RES. IN ORG. BEH. 239, 242 (2000) (studying "the construction of new organizational forms as a political project involving collective action").

[213] Bamberger, *Technologies of Compliance*, *supra* note __ at 35 (discussing failures in oversight of implementation of broad risk-management mandates).

[214] *See See* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 342–50 (2004) (describing the recent shift from the traditional "New Deal" regulatory era to a "Renew Deal" governance paradigm in which government, industry, and society "share responsibility for achieving policy goals").

[215] Michael C. Dorf, *The Domain of Reflexive Law*, 103 COLUM. L. REV. 384, 384 (2003) (reviewing JEAN L. COHEN, REGULATING INTIMACY: A NEW LEGAL PARADIGM (2002)).

[216] *Id*. at 264.

[217] Dorf, *supra* note __, at 384.

[218] *See* Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 314–23 (1998) (discussing how agencies can take advantage of their vantage point on the behavior of multiple firms to develop "rolling best practices" by collecting data from regulated entities about what works and what does not, and then disseminating that information back, through education and capacity building); *see also* Bradley C. Karkkainen et al., *After Backyard Environmentalism: Toward a Performance-Based Regime of Environmental Regulation*, 44 AM. BEHAV. SCIENTIST 692, 692–709 (2000) (providing, in the environmental context, a model in which administrative agencies develop the architecture for gathering and analyzing information across local contexts as a part of the regulatory and education process).

for improvement[219]—the type of measures that both permit external accountability, and spur changes in organizational management. By publicizing the debates over privacy policy, such transparency further coupled privacy performance with dynamic pressure from evolving market perceptions, and especially to consumer protection.

Moreover both the availability of detailed information, and the wide range of participatory procedures the FTC provided has empowered privacy advocacy, and enabled the tremendous rise of a movement of advocates central to developing "frames that justify, dignify, and animate collective action,"[220] around "privacy"—a "concept that leaves a lot to be desired" as "a clear organizational principle to frame political struggle."[221] Indeed, as one advocate explained, "[i]n the United States it's the agency debates that are really important."[222]

This contrasts with the EU context, in that U.S. advocates are, a recent study documented, "far more likely to use the provisions within their relatively fragmented patchwork of laws, than (have) their European counterparts"[223] to advance privacy protection. In comparison, "[t]he privacy advocacy community has generally not made extensive use of the complaints investigation and resolution process under data protection law." Indeed, the study explains, "[i]t is indeed striking how few complaints have been lodged by European advocacy groups under their stronger and more comprehensive data protection laws" despite the fact that doing so "cost no money and very little time."[224] This paradox is attributed to the fact that European Data Protection Agencies are relatively "under-resourced," legally "constrained," and that some " do not have enforcement powers." Accordingly, advocates recognize that DPAs often "have to adopt a more pragmatic approach."[225]

The role of such advocates in shaping the discourse of an increasingly professionalized corps of corporate privacy officers—marked by some level of fluidity between the members of the two groups—has moreover introduced an element of advocacy within regulated organizations themselves, and within the professional associations whose members participate in the diffusion of privacy management practices across corporate boundaries.

The way in which these developments in publicity and participation can act as a "social license" constraining corporate activity "[r]esonate[s] with theories that

---

[219] *See* Sturm, *supra* note __, at 492–519 (discussing the importance of benchmarks in fostering meaningful organizational change and improvement).

[220] Colin J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 1 (2008) (quoting Sydney Tarrow, Power in Movement: Social Movements and Contentious Politics 21 (1998))

[221] *Id.* at 2.

[222] *Id.* at 100 (quoting Chris Hoofnagle, formerly of the Electronic Privacy Information Center).

[223] *Id.* at 122.

[224] *Id.*

[225] *Id.* at 118.

emphasize the importance of a firm's social standing and in particular its economic stake in maintaining its reputation for . . . good citizenship."[226] In particular, they have aggregated otherwise dispersed market, consumer, and advocacy pressures to reproduce the types of forces that scholars of corporate regulation flag as important in producing "compliance-plus" behavior: visibility, community concern and threat to economic investment. In these contexts behavior can be "shaped by a far broader range of stakeholders within the 'organizational field' than regulators alone."[227]

Finally, at the core of this legal environment sits the FTC's entrepreneurial use of its enforcement power. To be sure, the ambiguous legal standards grounding the Commission's most powerful exercise of its regulatory power makes enforcement unpredictable, and incomplete. Yet in contrast to the "weak enforcement authority" described by Edelman in the employment context, the ambiguity of the FTC's legal directive provides its strength, and serves as a means to leverage the capacity of its entire regulatory approach.

The response to the FTC's roving enforcement authority described by every one of the privacy officers we interviewed—the way in which it spurred them to "look around corners" to consider the way in which an ambiguous consumer protection mandate could be applied to new practices, technologies and contexts—reflects dominant research on meaningful accountability in decisionmaking. Specifically, that research indicates that when decisionmakers face review by entities whose monitoring criteria are both well-specified and well-known, they behave as "cognitive miser[s]," "avoid[ing] mental calculations that require sustained attention, effort or computing power."[228] Yet that same research identifies other contexts in which the threat of review can force decisions to be more dynamic, thorough and thoughtful—when decisionmakers do not know the socially "acceptable" response—or more precisely, when those decisionmakers need to explain themselves to others.[229]

If, by socio-legal insights, regulated parties will adapt to a static set of external rules with a minimum of change, which, in turn, results only in cosmetic trappings of compliance, a dynamic model of regulation complicates the certainty of the threat, empowers those managers within organizations tasked with minimizing the threat in the competition for corporate resources, and creates a continuous external stimulus that must be translated into meaningful internal practice.[230] "Rather than perceiving the government demand as a single cost, the corporation's process of self-understanding may lead it" instead "to develop a relationship based on genuine compliance."[231]

---

[226] NEIL GUNNINGHAM, *ET AL.*, SHADES OF GREEN: BUSINESS, REGULATION, AND ENVIRONMENT 147 (2003)

[227] *Id.*

[228] Philip E. Tetlock, *Accountability: The Neglected Social Context of Judgment and Choice*, *in* 7 RES. IN ORG. BEH. 297, 311 (Barry M. Staw & L.L. Cummings eds., 1985).

[229] *Id.* at 314–21 (reviewing research evidence).

[230] Rubin, *supra* note __, at 387.

[231] Id.

## CONCLUSIONS: PRIVACY UNDER THE MICROSCOPE

The privacy and data protection community is entering a two year period of reflection and introspection. 2010 marks the thirtieth anniversary of the Organization for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the first international statement of fair information practice principles, and the OECD will kick off a review of the guidelines to identify areas for revision in early March.[232] A recent report reviewing the EU Data Protection Directive commissioned by UK Information Commissioner has proposed an alternative regulatory model oriented around outcomes.[233] And momentum has built for reconsidering the U.S. privacy framework. Both Congress and the Federal Trade Commission have signaled a commitment to deep reexamination of the current regulatory structure, and a desire for new models. Representative Rick Boucher (D-VA), chairman of the Communications, Technology and the Internet subcommittee of the House Energy and Commerce Committee, and Rep. Bobby Rush (D-Ill.), chairman of the House Energy and Commerce subcommittee on consumer protection, are reportedly in the final stages of drafting a bill to address internet and other technology-related privacy issues.[234] FTC Chairman Jon Liebowitz, and the Director of the agency's Bureau of Consumer Protection, David Vladeck, have both indicated a strong inclination to revisit the dominant privacy paradigm of notice and consent.[235] Vladeck has opined that, "[t]he frameworks that we've been using historically for privacy are no longer sufficient"[236] yet signaled uncertainty about how to move forward in protecting privacy's "dignitary"[237] interests in the commercial marketplace.[238]

---

[232] This groundwork will build a record for the review of the Guidelines in 2011 called for in the OECD's SEOUL DECLARATION FOR THE FUTURE OF THE INTERNET ECONOMY (2008). The aim is to determine whether the Guidelines should be revised or updated to address the current privacy environment, *see* SEOUL DECLARATION, at 10. The review process will begin in early March with an OECD Roundtable on the impact of the Privacy Guidelines, followed by a conference on privacy, technology and global data flows in October coinciding with the 32nd International Conference of Data Protection and Privacy Commissioners, and conclude on December 1, 2010 with a focus on the economic dimensions of privacy. http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html

[233] *See* Robinson, *et al.*, *supra* note__, at xi-xii.

[234] Tony Romm, *House Lawmakers Preparing Key Cell-Phone Location Privacy Legislation*, THE HILL Feb. 24, 2010.

[235] Stephanie Clifford, *F.T.C.: Has Internet Gone Beyond Privacy Policies?*, N.Y. TIMES, January 11, 2010.

[236] Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, August 5, 2009

[237] *Id.*

[238] *An Interview With David Vladeck of the F.T.C.*, N.Y. TIMES Media Decoder, August 5, 2009 (discussing difficulty of identifying harm in context of behavioral advertising and how to frame dignitary interests).

Our account of privacy on the ground provides several important insights[239] for what we consider to be the "third wave" of privacy initiatives—tort laws being the first, data protection the second, and security breach notification and consumer protection analysis marking the beginning of the third.

First, our account supports the argument that calls for federal regulation structured exclusively around fair information practice principles are ill-advised. Our interviews indicated ways that FIPPS was insufficient to guide corporate behavior—particularly in times of profound technical or market change—and could create stumbling blocks for CPOs by positioning them once again as the "no" person. Thus many of our interviewees discussed efforts to transform internal perceptions about privacy from a compliance oriented, rule dominated, legal hurdle to be addressed at the end stage of product design, to a consultation and dialogue about how technical designs, business strategies, and policies can respect consumers' expectations and support trust in their companies. Our interviewees further suggested that, without a substantive touchstone, a data-protection regime can focus resources on developing a host of often meaningless consent processes,[240] which must be designed and redesigned in an effort to do better—where the meaning of "better" is unclear. They further predicted that the limitations of consent as the dominant fall-back for protecting consumer privacy would be exacerbated by the increasing trend toward networks, embedded devices, and increasingly personalized services.

While FIPPS remain an important touchstone for information privacy in the U.S., they should not be the exclusive touchstone for regulatory reforms. FTC enforcement aimed at protecting consumers' reliance on conventional information flows have brought greater substance and meaning to an area routinely critiqued for its formalism. In adopting a contextual analysis of privacy issues, the FTC's approach is responsive to the criticism of scholars and advocates who find that data protection can lead to a reductive construction of privacy and therefore resist working "within any fixed and guiding definition of what privacy means."[241] Viewing privacy as context-dependent protects against corporate and bureaucratic desires to reduce it to a set of *a priori* process-oriented rules, and the legalization and regularization that critics and proponents alike claim plague data protection. And protecting existing social norms about information use, rather than leaving each individual to the mercy of the marketplace, is key to addressing both collective and individual interests, for while

---

[239] There are certainly other core issues, such as those involving the preemption of state law, to which this paper does not specifically speak, and regarding which debate persists, *compare* Paul M.Schwartz, *Preemption and Privacy*, 118 YALE L.J. (2009) *with* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009). For the time being we note that the debate over preemption largely brackets discussion of the issue of technical and scientific expertise issues, an "on the ground" issue which remains to be engaged.

[240] *See generally* Fred H. Cate, *The Failure Of Fair Information Practice Principles*, in CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' (2008) (discussing the failure of the notice and consent model to protect privacy meaningfully).

[241] BENNETT, THE PRIVACY ADVOCATES, *supra* note __ at 18.

"[p]rivacy self-defense operates at the individual level . . . surveillance operates at the collective level;" thus "the logics of surveillance require a considered, collective response."[242]

Second, our account identifies the important role that FTC plays in providing a forum for structuring and advancing a collective understanding of privacy among advocates, industry, academics and regulators. While the FTC's function as roving enforcement agency has been especially significant, its threat of coercive authority leverages an even deeper role in developing a cross-field understanding of privacy through workshops, fact-finding investigations, and other soft-law techniques to flesh out the meaning of its ambiguous privacy mandate. The collective engagement prompted through these regulatory choices has yielded both substantively groundbreaking outcomes—a divergence from *caveat emptor* with respect to privacy disclosures—as well as unique changes in corporate privacy management. The FTC's combination of enforcement threats with its centrality in fostering a social network of entrepreneurial privacy advocates offers a model for avoiding both the shortcomings of static top-down command-and-control regulatory approaches and the ways in which reliance on bottom-up self-regulation alone can subvert public goals by private interests.

This model should guide the choice and design of whatever regulatory institutions take the lead on information privacy in the corporate sector moving forward. They must both possess and use regulatory tools that exploit market, corporate and advocacy capacity to develop collective understanding of risks and solutions to future privacy problems.

Third, our account begins to illuminate the ways in which corporate privacy professionals impart meaning and structure to societal privacy concerns within corporations.

Debates about the establishment of a dedicated privacy agency in the United States emphasize the importance of governmental privacy expertise in shaping the rules governing corporate behavior.[243] Veteran privacy expert Robert Gellman contends that regardless of whether the U.S. chooses a highly regulated path forward or continues with on its current path, an expert federal privacy board would help achieve privacy objectives "more quickly, more efficiently, and consistently."[244] David Flaherty in his comparative study of the implementation of data protection and privacy laws in five countries, concluded that data protection must be entrusted to a "cadre of specialists" in a data protection authority [245] and attributed what he believed was the United States' poor privacy performance in large part to "the lack of an oversight agency."[246] Yet while

---

[242] Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*. 75 U. CHI L. REV. 1 (2008).

[243] For a thorough discussion of debates and various proposals to establish federal data privacy protection agencies see, Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L. J. 1183, 1192-97 (2003).

[244] Gellman, supra *note* __, at 1218.

[245] DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 389 (1992).

[246] *Id*. at 305

numerous proposals for a U.S. privacy agency have been proffered—some giving it regulatory authority, some merely advisory—none have garnered public or political support.[247] Indeed, recent legislative proposals to address privacy in the corporate sector seem to have abandoned the notion.

Yet if the vision of privacy expertise centralized within a free-standing government agency seems unlikely to be realized, a broad, vibrant and entrepreneurial "cadre of specialists" has developed in the private sector—within companies, advocacy organizations and academia. In the absence of a DPA staffed with data protection experts, and faced with increasing ambiguity as to what privacy requires, corporations depend on these new professionals to guide them through the challenges wrought by evolutions in technology and business practice. These professionals do not view themselves as compliance officers, but as norm entrepreneurs. Empowered by external threats that support their entrepreneurial efforts, they offer a unique capacity to embed privacy—as trust and consumer expectations—into the corporate psyche as well as business operations.

Choices about regulatory form will affect the ability to leverage these professionals—to empower them within their own organizations in ways that pushes privacy further into corporate culture. A decision to redirect privacy regulation towards more rule-bound governance, for example, might diminish the need for corporations to rely on high-level internal advocates of privacy concerns. As society becomes more pervasively networked, and privacy protection requires ongoing and on-the-ground attention to dynamic privacy interests that manifest in very different ways within different firms, then, institutional reforms should be attentive to preserving the benefits flowing from this embedded class of professionals, and seek to empower rather than displace them.

Finally, as the privacy community reflects upon the key global instruments of data protection, our account underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy is to be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today's frameworks operate on the ground.

---

[247] *See* Gellman, supra *note* __, at 1197.

Contrary to what marketers say,

# Americans Reject Tailored Advertising

## AND THREE ACTIVITIES THAT ENABLE IT

**Joseph Turow**
Annenberg School for Communication, University of Pennsylvania

**Jennifer King**
University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

**Chris Jay Hoofnagle**
University of California, Berkeley, School of Law, Berkeley Center for Law & Technology

**Amy Bleakley**
Annenberg Public Policy Center, University of Pennsylvania

**Michael Hennessy**
Annenberg Public Policy Center, University of Pennsylvania

**Joseph Turow,** Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *Niche Envy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (U of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy. Several can be found at the Annenberg Public Policy Center website, APPCPenn.org.

**Jennifer King**, MIMS, is a Ph.D. student at the UC Berkeley School of Information. Most recently she was a researcher at the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley's School of Law. Her research areas include information privacy and security, usability and human-computer interaction, video surveillance and other sensor networks. With Chris Hoofnagle, King has published three reports exploring Californians' privacy attitudes; these are available at ssrn.com.

**Chris Jay Hoofnagle,** J.D., is director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice law in California and Washington, DC.

**Amy Bleakley,** Ph.D., MPH, is a Research Scientist in the Health Communication Group of the Annenberg Public Policy Center at the University of Pennsylvania. Dr. Bleakley studies adolescent sexual behavior, sexual and reproductive health policies, health behavior theory, and contextual influences on health behavior. Her current research focuses investigating the effect of sexual content in the media on adolescent sexual development.

**Michael Hennessy,** Ph.D., is Project Manager and Statistician in the Health Communication Group of the Annenberg Public Policy Center. His major interest is the integration of structural equation modeling and intervention program/behavioral theory, growth curve analysis of longitudinal data, and using factorial surveys to design both behavioral intervention programs and community-based clinical trials for experimental vaccines. He has published over 90 articles in *Evaluation Review*, *Structural Equation Modeling, AIDS and Behavior, Psychology Health & Medicine*, *The American Journal of Evaluation*, and *Evaluation and the Health Profession* among other journals.

September, 2009
This survey was supported by the Rose Foundation for Communities and the Environment, Tim Little, Executive Director, under grant 025629-003, Chris Jay Hoofnagle, Principal Investigator; and by The Annenberg School for Communication—Michael Delli Carpini, Dean.

**Overview**

Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising.

These are two findings from the first nationally representative telephone (wireline and cell phone) survey to explore Americans' opinions about behavioral targeting by marketers, a controversial issue currently before government policymakers. Behavioral targeting involves two types of activities: following users' actions and then tailoring advertisements for the users based on those actions. While privacy advocates have lambasted behavioral targeting for tracking and labeling people in ways they do not know or understand, marketers have defended the practice by insisting it gives Americans what they want: advertisements and other forms of content that are as relevant to their lives as possible.

We conducted this survey to determine which view Americans hold. In high percentages, they stand on the side of privacy advocates. That is the case even among young adults whom advertisers often portray as caring little about information privacy. Our survey did find that younger American adults are less likely to say no to tailored advertising than are older ones. Still, more than half (55%) of 18-24 year-olds do not want tailored advertising. And contrary to consistent assertions of marketers, young adults have as strong an aversion to being followed across websites and offline (for example, in stores) as do older adults. 86% of young adults say they don't want tailored advertising if it is the result of following their behavior on websites other than one they are visiting, and 90% of them reject it if it is the result of following what they do offline. The survey uncovered other attitudes by Americans toward tailored content and the collection of information about them. For example:

- Even when they are told that the act of following them on websites will take place anonymously, Americans' aversion to it remains: 68% "definitely" would not allow it, and 19% would "probably" not allow it.

- A majority of Americans also does not want discounts or news fashioned specifically for them, though the percentages are smaller than the proportion rejecting ads.

- 69% of American adults feel there should be a law that gives people the right to know everything that a website knows about them.

- 92% agree there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."

- 63% believe advertisers should be required by law to immediately delete information about their internet activity.

- Americans mistakenly believe that current government laws restrict companies from selling wide-ranging data about them. When asked true-false questions about companies' rights to share and sell information about their activities online and off, respondents on average answer only 1.5 of 5 online laws and 1.7 of the 4 offline laws correctly because they falsely assume government regulations prohibit the sale of data.

- Signaling frustration over privacy issues, Americans are inclined toward strict punishment of information offenders. 70% suggest that a company should be fined more than the maximum amount suggested ($2,500) "if a company purchases or uses someone's information illegally."

- When asked to choose what, if anything should be a company's single punishment beyond fines if it "uses a person's information illegally," 38% of Americans answer that the company should "fund efforts to help people protect privacy." But over half of Americans adults are far tougher: 18% choose that the company should "be put out of business" and 35% select that "executives who are responsible should face jail time."

It is hard to escape the conclusion that our survey is tapping into a deep concern by Americans that marketers' tailoring of ads for them and various forms of tracking that informs those personalizations are wrong. Exactly why they reject behavioral targeting is hard to determine. There may well be several reasons. One may be a general antagonism to being followed without knowing exactly how or with what effects. Americans may not want their behavior on one site to somehow affect the interaction with subsequent sites. Consumers may intend to divide their web browsing into different subjective contexts (e.g. shopping, work, play, education), and they may worry that tracking across those contexts may subject them to embarrassment (e.g. while using the computer in the work context, ads may be displayed that are relevant to play). Another reason might be a fear that selective presentation of advertisements, discount offers, or news will put them at a monetary or social disadvantage: some people might get more useful or interesting tailored content than others depending on the conclusions marketers draw about them. The rejection of even anonymous behavioral targeting by large proportions of Americans may mean that they do not believe that data about them will remain disconnected from their personally identifiable information. It may also mean that anonymity is not the only worry they have about the process. Being labeled in ways they consider unfair by marketers online and off may be just as important a concern.

Whatever the reasons, our findings suggest that if Americans could vote on behavioral targeting today, they would shut it down. The findings also suggest that marketers and government policymakers may be faced with a backlash if Americans were to organize around complaints that the laws they think protect them from the sale of their data actually don't exist. It is also important to note that this rejection of tailoring and behavioral tracking by marketers and media firms does not mean Americans reject the idea of customizing ads, discounts, and news themselves. To the contrary, evidence from around the digital world shows that they want to control and shape what

content they receive. The problem for marketers is that Americans are worried about others' use of data about them in ways they do not know or understand, and might not like.

In fact, our survey found that Americans want openness with marketers. If marketers want to continue to use various forms of behavioral targeting in their interactions with Americans, they must work with policymakers to open up the process so that individuals can learn exactly how their information is being collected and used, and then exercise control over their data. At the end of this report, we offer specific proposals in this direction. An overarching one is for marketers to implement a regime of *information respect* toward the public rather than to treat them as objects from which they can take information in order to optimally persuade them.

**Background**

Behavioral targeting (BT) has quickly become one of the central, yet most controversial, vehicles for reaching consumers in the digital age. Critics' calls for its restriction run parallel to marketers' statements about its crucial nature as a lifeline for the new media age. Yet the arguments about the process, which include claims about public attitudes, discuss it as if it is a single act, when it is really made up of many parts that can and should be evaluated separately from a public interest standpoint. To help with that evaluation, policymakers, social advocates, and marketers need public-opinion benchmarks about the distinct yet related activities that make up the process.

With that goal in mind, this study for the first time disentangles Americans' attitudes toward tailored content from their opinions about three common behavioral tracking methods. Behavioral tracking involves following an individual's activities over time and the using the information to select which advertisements to display to that individual. Advertisers believe the practice helps them deliver their persuasive messages to audiences who are most likely to be interested. Tailoring of content involves the creation or alteration of media material to suit marketers' perceived interests of an individual or individuals.

This study concerns three types of companies—websites, advertising networks, and offline retailers—that carry out contemporary behavioral targeting. Websites closely follow the movements of visitors—for example, what articles they read, what ads they clicked, what products they started to buy but didn't purchase. The site can serve up ads to the person based on the topic selected—for example, a movie ad if the person is viewing movie reviews. The sites can also save the records of these actions and link them to the visitor by placing identifying text files called *persistent cookies* on the visitor's computer. When a user of that computer returns, the site can serve relevant advertisements based on the visitor's previous activity patterns. For example, if the past visits indicate particular attention to newspaper site's travel section, the website can serve ads from its travel advertisers to that visitor.

Advertising networks also track visitors and store their peregrinations, but across thousands, even tens of thousands, of websites that accept ads from those firms and share in the revenues. This approach means that ads served to site visitors by networks owned by Google, Yahoo, AOL,

ValueClick and many other firms may reflect a history of movements through the online world. In the most basic sense, a person who visited an auto site to search for used Mini Coopers might find himself shown a Mini Cooper ad on a newspaper site he visits the next day if the newspaper is part of the same advertising network.

Offline retailers also track visitors, most often through frequent shopper cards. As in the online world, supermarkets and drug stores may use the data to selectively send advertisements to different cardholders based on the different shopping experiences. The stores may also present special prices and shopping experiences to individuals whom they identify while they are in the stores. The Stop-and-Shop supermarket chain, for example, has experimented with giving people carts with devices activated by their frequent-shopper cards to which they can email shopping lists and which present them with offers based on past and present shopping behavior. Beyond bringing digital technology to the physical store, merchants are also merging the data they have about their customers from the web, the phone, and the store floor in an attempt to get a unified view of individual customers' behavior.

Websites, advertising networks, and offline retailers often rely on database technology companies to help them carry out behavioral targeting in the most sophisticated ways possible. One such firm, Audience Science, states that its work involves "recording billions of behavioral events daily and reaching over 385 million unique Internet users" who then make the data available to its clients: "Web publishers, marketers, networks, exchanges, and agencies to create intelligent audience segments to connect people with relevant advertising driving the transition to data-driven audience marketing online."[1] To further enhance their knowledge of individual customers, offline stores and individual websites often go beyond tracking behavior to explore the backgrounds of members of their audience who seem to be particularly good prospects for sales or to present to advertisers. Over the past few decades, the sale and purchase of information on individuals has become big business. American privacy law is sectoral, meaning that certain businesses are restricted from selling information without consumer consent, but those rules apply in limited circumstances. Generally, companies have virtually free rein to use data in the U.S. for business purposes without their customers' knowledge or consent. Websites and stores can therefore easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them.

Unlike individual websites and offline retailers, however, advertising networks today typically don't know the names or postal addresses of the people they track across the web. The networks consequently can't buy personally identifiable data about them. They have, however, parlayed the desire to know consumers' personalities and demographics into major enterprises to connect the millions of information dots they have about their users in ways that will appeal to advertisers. Complex dot-connecting formulas are used by ad networks of Google, Yahoo, AOL, Value Click and other firms to label millions of people according to categories that reflect inferences about gender—whether a person's search habits are feminine or masculine—as well as lifestyle and

personality—for example, whether a person is a soccer mom and/or world traveler. Ad networks still hold rather few geographic, demographic, and psychographic and lifestyles categories about individual web users. Nevertheless, the knowledge in these networks is growing and the tracking is spreading beyond the web to mobile handsets and television set-top boxes.

The reason websites, advertising networks and offline retailers are so intent on keeping track of their visitors has to do with the desire to tailor the messages that they deliver. Many advertisers believe that learning customers' present and past browsing and shopping habits can suggest what products would appeal to them and what advertising messages will catch their attention. Just as the process of making inferences about consumers is proceeding apace, so the technology to tailor commercial messages to them is becoming increasingly efficient across a variety of digital media, including television. Coupons are already tailored for individuals in physical stores, websites, and mobile handsets based on data-driven shopping , traveling and demographic patterns. And although advertisers' contemporary focus is on ads and coupons, it is also possible to present people with different offerings of entertainment and news based on analyses of their interests or their marketing profiles—starting with the kinds of recommendation engines characterized by Amazon.com and going far beyond them. News and entertainment distributors may increasingly explore the proposition that tailoring material—even just headlines and promotional materials—based on what they have learned from tracking audiences will encourage return visitors who will provide yet more information to use for targeting ads to them. Technology companies such as Visible World already offer technology that can insert products into television entertainment programs in real time based on information about the family that their cable company has placed into their set boxes based on their viewing behaviors and additional information the firm has learned about them.

**Critics and Defenders**

Critics of behavioral targeting complain that it is wrong to gather so much data about individual Americans, create dossiers about them without their awareness, and use the data to surround them with ads based on social and consumer categories that the citizens have not validated and might not agree with. While deleting one's browser cookies is often recommended as a quick fix for preventing tracking, it's a practice users must repeat often because websites place new cookies at each new visit. In addition, an increasing number of websites are installing *Flash cookies*, which also allow site visits to be tracked. More than half of the internet's top websites use them, according to a recent UC Berkeley study led by Ashkan Soltani and Chris Hoofnagle.[2] Also known as local shared objects (LSOs), Flash cookies are stored in connection with the Adobe Flash player and cannot be erased through the cookie privacy controls in a browser. In order to delete Flash cookies on a user's computer, a user must visit Adobe's website and use an online settings manager tool.[3] The consequence, noted a *Wired* magazine article, is that "even if a user thinks they have cleared their computer of tracking objects, they most likely have not." Moreover, sites have even begun to use the Flash cookies as backups to reinstate traditional cookies that a user deleted, a process that is called *re-spawning*.

Calls for an opt-in approach whereby individuals would have to consent to being tracked, are often dismissed by the advertising industry as unrealistic. Demands to let users opt out have met with half-hearted assent. Companies that allow opt out possibilities often make it hard for consumers to learn how to do it. Regardless, when a consumer clears his or her browser cookies, any opt out cookies are erased along with regular cookies, putting consumers in an impossible bind between refusing to allow cookies (causing most websites to be completely unusable), or deleting unwanted cookies manually, one by one. The difficulty even applies to sites belonging to the National Advertising Intiative's Opt-Out Program: Note 11 of its FAQ points out that "If you ever delete the 'opt-out cookie' from your browser, buy a new computer, or change Web browsers, you'll need to perform the opt-out task again."[4] Note, too, that in some cases opting out of advertising does not prevent websites from tracking. Instead, it stops them from sending tailored ads. If one conceives of the privacy objection to online advertising as related to tracking, opting out does nothing to quell that concern.

TRUSTe, a company that promotes privacy practices and a related approval seal to websites as a way to gain consumer confidence, noted in March 2009 that "Behavioral advertising still represents un-charted territory, without clearly applicable laws or regulations." In February 2009, the Federal Trade Commission (FTC) published guidelines for companies collecting behavioral data of web users with the aim of presenting tailored advertising to them. The principles encourage transparency and customer control, security of customer data and the retention of customer information for a limited period.[5] Seemingly in response to such pressure, Google now allows visitors to its site to learn the categories it identifies with their browser's cookie, and to opt out of such cookie-linking if they wish. Google's "permanent opt-out" process takes several steps, however, and neither Google nor any other major company explains where it received such information, how it arrived at its conclusions, or gives people the right to challenge what they consider misperceptions.[6] In fact, as *Wired* magazine noted in August 2009, the attempts at self-regulation by the online tracking and advertising industry "have conspicuously failed to make the industry transparent about when, how and why it collects data about internet users."[7]

A key reason advertising executives have held back allowing transparency and offering consumers choices regarding behavioral tracking might be the activity's immense value—it is "the future in digital advertising," in the words of a TRUSTe executive[8]—together a parallel concern that consumers would opt out if they learned about it. *New York Times* reporter Louise Story put their dilemma concisely:

> Underscoring all the debates about online privacy, behavioral targeting and Internet advertising is a hard, cold reality: content costs money. . . .
>
> As mass advertising dies, there is more pressure for media companies to develop audiences with more specific interests and characteristics. From an economic standpoint, the drop in the total number of eyeballs means the eyeballs that remain must become more lucrative.

> Media companies are also using targeting, often called behavioral targeting, to provide more valuable eyeballs. . . .[9]

Marketing executives typically justify behavioral targeting by making two claims related to tailoring and tracking. The first is that Americans want advertisements tailored to their interests; implicitly this requires learning about them through tracking their behavior. The other assertion is that only older consumers worry about the privacy issues related to behavioral tracking.

The notion that the younger generations really don't care about tracking was repeated recently by Disney CEO Robert Iger who told a July 2009 Fortune Brainstorm Tech conference that media companies should use individual tracking data to target ads and that younger people "don't care" about the privacy aspects around this. "Kids don't care," Iger said, adding that his own adult children "can't figure out what I'm talking about" when he asks them about their online privacy concerns.[10]

Iger went on to herald the value for Disney of using tracked data to tailor ads: "If we know that you've gone online and looked at five different autos online, you are a great consumer for us to serve up a 30-second ad for a car," he said. To marketers, it is self-evident that consumers want customized commercial messages. Typical of this claim for tailoring is the perspective of an executive at customer-relationship-management firm Dunnhumby USA. He notes that "Something amazing happens when marketing efforts are actually relevant to people. We see this step as initiating that crucial dialogue. And shoppers, for their part, are replying; essentially giving their permission to marketers to learn their habits and respond accordingly."[11] Reflecting that assumption, AudienceScience states that its "sophisticated behavioral targeting technology enables the company to improve its user experience by making the ads shown more relevant to each viewer, as well as offer its advertisers a higher level of engagement and return."[12] Similarly, Google's light description for the public of its AdSense contextual and behavioral advertising program states that "It's our goal to make these ads as relevant as possible for you. While we often show you ads based on the content of the page you are viewing, we also developed new technology that shows some ads based on interest categories that you might find useful."[13] And the National Advertising Initiative, in its web page that allows opting out of member advertising networks, informs visitors thinking about the decision in bold type that "Opting out of a network does not mean you will no longer receive online advertising. It does mean that the network from which you opted out will no longer deliver ads tailored to your Web preferences and usage patterns."[14]

## The Right Questions of the Right Samples

The advertising industry's stress on the utility of behavioral targeting for Americans because they enjoy relevant advertising raises a number of basic questions: First, do Americans in fact want advertisers to tailor advertising to their interests? Second, if they say they want tailored advertising, would they continue to want it when told that it results from following their activities—for example,

on individual websites, across websites, and in physical stores? And is it indeed the case that younger American adults tend not to be concerned about tracking and tailoring?

Prior to the research reported here, we did not have straightforward answers to these separate questions. Several studies do show strong concern for internet privacy among Americans and a desire for firms not to collect information about them online. It seems clear, too, that Americans value the right to opt out from this sort of collection. For example, in a 2008 national telephone survey, Consumers Union found that 72% of Americans 18 years and older "want the right to opt out when companies track their online behavior." But regarding Americans' response to behavioral targeting and tailoring, the findings are less clear. As far as we can tell the only publicly available studies on the subject are from a 2008 survey by TRUSTe that was repeated in 2009 and a 2009 survey from the Privacy Consulting Group, led by Alan Westin. Both suffer from a number of conceptual and methodological problems which we had to consider when developing our own questions and methods.

TRUSTe's questionnaire, fielded two years in a row by TNS, asked about behavioral targeting and tailoring in a way that asked respondents whether they agreed or disagreed with a statement about both activities that also added the promise of anonymity: "I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information." In response, about 57% said they either strongly agreed (18%) or agreed (39%). The Westin study, conducted by Harris Interactive online, also posed a standalone question about how "comfortable" people felt with behavioral targeting and tailoring: "As you may know, websites like Google, Yahoo! And Microsoft (MSN) are able to provide free search engines or free e-mail accounts because of the income they receive from advertisers trying to reach users on their websites. How comfortable are you when those websites use information about your online activity to tailor advertisements or content to your hobbies or interests?" Westin found that 59% said they were uncomfortable, with younger people (18-24 and 25-29) having lower percentages than older people—though still over 50%. Westin then asked people to assume that "websites" adopted four stringent privacy and security policies (explaining how the tailoring process would work, offering choices of tailoring, safeguarding information, and promising not to share any user's name or address) and found that now most people apart from those 63+ were "comfortable" with behavioral targeting and tailoring. Still, the percentages "not comfortable" despite these stringent standards were substantial—38% for 18-31 year olds, 44% for 32-43 year olds, 48% for 44-62 year olds and 54% for those 63+.

Both surveys have the major limitation of being online investigations in which people responded to ads to partake in the companies' research. The survey firms acknowledge that the sample is not representative and no confidence levels can be presented. The particular nature of the topic of this survey makes the findings particularly suspect. One might worry that people who volunteer to participate would feel less concerned about companies using their data online than would a representative sample of adults who use the internet but would not volunteer for an online survey. Another drawback to emphasize is that both these surveys combined two ideas into one question:

the issue of whether sites should serve tailored content and whether the tailoring should be based on a certain kind of tracking. A further problem is that both surveys say nothing about the particular nature of the targeted behavior. Westin's explanation of tracking said "those websites use information about your online activity," while TRUSTe described it as "using my browsing history." Neither is specific about whether the tracking takes place on a particular website or across websites, and neither suggests the possibility that data collected offline might be used to serve tailored ads. The latter is an increasing activity that is beginning to receive attention from policymakers.

It is also important to know whether Americans consider the very idea of tailored advertising a good idea, irrespective of how data are collected. To justify behavioral targeting, marketers in recent months been insisting that Americans do in fact want tailored ads. Westin's report suggests that people would want tailored advertising if the four FTC self-regulatory policies were observed. The TRUSTe study uses responses to a statement having nothing to do with tailoring—"If given the option, I would choose to only see online ads from online stores and brands that I know and trust"—to conclude that "individuals want their advertising to be more relevant."

Marketing executives who speak to the trade press tend to take for granted that Americans want tailored ads because they are relevant ads. So, for example, a Facebook executive recently noted that "there is nothing controversial" about using member profiles and wall postings to create tailored ads for them. "The controversy," he added "comes in when a user's behavior without their knowledge is tracked across the internet, which is not something we do."[15] The contention underscores the point that tailoring can take place through a variety of methods other than behavioral targeting. It also raises key questions: Do Americans consider tailoring of advertising, discounts or news suited their interests to be a service they appreciate? Separately, do Americans accept behavioral tracking as the means for providing that tailored content?

**The Study and the Population**

We explored these questions as part of a larger survey of Americans' opinions about and understanding of a variety of online and offline privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: "Do you go on online or use the internet, at least occasionally?" and "Do you send or receive email, at least occasionally?"

The survey questions we included in this report focus on four areas. One explores Americans opinions about tailored content and three different forms of behavioral tracking. A second investigates people's knowledge of rules of the marketplace when it comes to sharing information in the online and the offline world. A third area of questions asks Americans their opinions about laws that might associate with the tracking their information as well as misusing their information. And a fourth area inquires into people's beliefs about their control over their personal information, whether businesses "handle the personal information they collect about consumers in a proper and

confidential way" and whether they believe "existing laws and organizational practices provide a reasonable level of protection for consumer privacy today."

The survey was conducted from June 18 to July 2, 2009 by Princeton Survey Research Associates International. PSRA conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 adult internet users living in the continental United States. A combination of landline (n=725) and wireless (n=275) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged 20 minutes. Based on a 7-callback procedure and using the American Association of Public Opinion research (AAPOR) RR3 method, a standard for this type of survey, the overall response rates were a rather typical 18 percent for the landline sample and 22 percent for the cellular sample. Statistical results are weighted to correct known demographic discrepancies.[*] The margin of sampling error for the complete set of weighted data is ±3.6 percent at the 95% confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 provides an introductory snapshot of the population we interviewed. As Table 1 indicates, women slightly outnumber men; 78% designate themselves as White; 9% identify themselves as blacks or African American; Asian Americans make up 4%; and Native Americans comprise about 1%. Hispanics (white and black) comprise about 11% of the sample. About 56% are under age 45 and 53% are married. Most have at least some higher education, and 33% report over $75,000 household income while 21% list it as below $30,000; 10% refused to reveal their household income.

**Rejecting Tailored Content and Behavioral Tracking**

The telephone interviewer asked all these people the following questions in a randomly rotated manner:

- Please tell me whether or not you want the websites you visit to show you ads that are tailored to your interests

[*] A two-stage procedure was used to weight this dual-frame sample. A first-stage weight was applied to account for the overlapping sample frames. The first stage weight balanced the phone use distribution of the entire sample to match population parameters. The phone use parameter was derived from an analysis of the most recently available National Health Interview Survey (NHIS) data along with data from recent dual-frame surveys. (See Blumberg SJ, Luke JV, "Wireless substitution: Early release of estimates from the National Health Interview Survey, July-December, 2008." National Center for Health Statistics. May 2009.) This adjustment ensures that the dual- users are appropriately divided between the landline and cell sample frames.

The second stage of weighting balanced total sample demographics to population parameters. The total sample was balanced to match national population parameters for sex, age, education, race, Hispanic origin, region (U.S. Census definitions), population density, and telephone usage. The basic weighting parameters came from a special analysis of the Census Bureau's 2008 Annual Social and Economic Supplement (ASEC) that included all households in the continental United States. The population density parameter was derived from Census 2000 data. The telephone usage parameter came from the analysis of NHIS data.

**Table 1: Characteristics of U.S. Adults in Sample (N=1,000)***

| | % |
|---|---|
| **Sex** | |
| Male | 48 |
| Female | 52 |
| **Age** | |
| 18-24 | 14 |
| 25-34 | 21 |
| 35-49 | 30 |
| 50-64 | 26 |
| 65-89 | 9 |
| **Race** | |
| White | 78 |
| Black or African American | 9 |
| Asian or Pacific Islander | 4 |
| American Indian or Alaskan Native | 1 |
| Mixed Race | 2 |
| Other/Don't Know/Refused | 6 |
| **Hispanic or Latino Background?** | |
| Yes | 11 |
| No | 88 |
| Don't Know/Refused | 1 |
| **Household Income** | |
| Under $30,000 | 21 |
| $30,000 to under $50,000 | 19 |
| $50,000 to under $75,000 | 17 |
| $75,000 and Over | 33 |
| Don't Know/Refused | 10 |
| **Region of the Country** | |
| Northeast | 19 |
| Midwest | 22 |
| South | 33 |
| West | 26 |

*When the numbers don't add to 100% it is because of a rounding error.

- Please tell me whether or not you want the websites you visit to give you discounts that are tailored to your interests.

- Please tell me whether or not you want the websites you visit to show you news that is tailored to your interests.

If a subject answered "yes" to any of the above questions about ads, discounts, and news, its corresponding question below as then asked:

- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on the website you are visiting?

- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do on OTHER websites you have visited?

- Would it be OK or not OK if these ads [discounts/news] were tailored for you based on following what you do OFFLINE—for example, in stores?

The interviewer also asked a general question about the acceptability of behavioral tracking for the purpose of tailored ads if the tracking is anonymous. The lead-up to the question noted that marketers "often use technologies to follow the websites you visit and the content you look at in order to better customize ads." The interviewer then asked whether the respondent would "definitely allow, probably allow, probably NOT allow, or definitely not allow advertisers" to "follow you online in an anonymous way in exchange for free content."

Tables 2 and 3 present the findings. Table 2 shows that fully 66% of the respondents do not want advertisements tailored for them. The proportions saying no are lower when it comes to tailored discounts and news, but they still represent around half the population—49% and 57% respectively.

Table 3 shows whether people who said yes to tailored ads, discounts or news continued to say they wanted the tailored content when the interviewers told them the three ways that the information the facilitate tailoring would be gathered. Two interesting patterns show up. One is that for each topic—ads, discounts, and news—the increase in the proportion of people saying no was substantially lower when told that the tracking would take place "on the website you are visiting" compared to tracking based on "*other* websites you have visited" and on "what you do *offline*—for example, in stores." Another notable pattern is for advertisements, discounts, and news, around 80% of the respondents reject tailoring either outright or when they learn they will be followed at other websites or offline.

So, for example, 66% of the 1,000 respondents said no to tailored ads before being told about the forms of tracking. When told the tailored advertising would be based on following them on other websites they have visited, 18% *more* of those 1,000 respondents said no to tailored advertising. That means that 84% of the respondents rejected tailored ads outright or when they found out it would

**Table 2: Please Tell Me Whether Or Not You Want Websites You Visit to . . .** (N=1,000)*

| | No, Would Not (%) | Yes, Would (%) | Maybe, DK (%) |
|---|---|---|---|
| Show you ***ads*** that are tailored to your interests. | 66 | 32 | 2 |
| Give you ***discounts*** that are tailored to your interests. | 49 | 47 | 4 |
| Show you ***news*** that is tailored to your interests. | 57 | 40 | 3 |

*See text for explanation. DK=Don't Know

**Table 3: Would It be OK or not OK if . . .** (N=1,000)*****

| | OK (%) | Not OK (%) | Maybe/ DK (%) | Didn't Want Tailoring (%) | Not OK + Didn't Want Tailoring (%) |
|---|---|---|---|---|---|
| *these **ads** were tailored for you based on following* | | | | | |
| what you do on the website you are visiting. | 24 | 7 | 3 | 66 | 73 |
| what you did on *other* websites you have visited. | 13 | 18 | 3 | 66 | 84 |
| what you do *offline*—for example, in stores. | 11 | 20 | 3 | 66 | 86 |
| *these **discounts** were tailored for you based on following* | | | | | |
| what you do on the website you are visiting. | 34 | 13 | 4 | 49 | 62 |
| what you did on *other* websites you have visited. | 18 | 29 | 4 | 49 | 78 |
| what you do *offline*—for example, in stores. | 18 | 29 | 4 | 49 | 78 |
| *this **news** was tailored for you base on following* | | | | | |
| what you do on the website you are visiting. | 25 | 14 | 4 | 57 | 71 |
| what you did on *other* websites you have visited. | 14 | 26 | 3 | 57 | 83 |
| what you do *offline*—for example, in stores. | 12 | 28 | 3 | 57 | 85 |

*See text for explanation. DK=Don't Know

happen through tracking them on other sites. The corresponding numbers for discounts and news are 78% and 83%, respectively.

Assurance of anonymous tracking doesn't seem to lower Americans' concerns about behavioral targeting. They are quite negative when it comes to the general scenario of free content supported by tailored advertising that results from "following the websites you visit and the content you look at" in a manner that keeps them anonymous. 68% definitely would not allow it, and 19% would probably not allow it. 10% would probably allow, and only 2% would definitely do it; 1% say they don't know what they would do.

Differences by Age

Americans' negative response to tailored ads, discounts, and news goes up with age in a statistically significant manner (Rho= -.24, -.22, and -.12 respectively). When we divide age into traditional marketing categories, however, we find that only the differences in ads and discounts emerge as statistically significant. Through cruder than the statistically significant correlations, the categorical approach allows us to see sharp variations between familiar social groupings. The spread is most pronounced between young adults and seniors. Specific comparison of these two groups revealed their differences are significant statistically across all three forms of content. As Table 4 shows, 55% of Americans 18 and 24 years old say no to tailored advertising, 37% say no to tailored discounts, and 54% reject tailored news. By contrast, among Americans over 65 the numbers are 82%, 70%, and 68% for ads, discounts, and news.

Note that while younger Americans are more welcoming of tailored content than are older ones, well over half of young adults nevertheless do say no to tailored advertising and news. Moreover, the percentage of young adults saying no to the three forms of tailored content becomes substantially higher when we include those who said yes to tailoring alone but then balked when told that their actions would be tracked in order for tailoring to be implemented. Tables 5-7 display the age breakdowns regarding the respondents who said *Not OK* or *OK* to tailoring and tracking. (We left out the 3% or 4% that answered *maybe*, it *depends*, or *don't know*). As Table 5 indicates, 67% of the 18-24 year old Americans say they do not want tailored advertising when we include those saying it is not OK to tailor for them based on what they do on the website they are visiting. 86% of 18-24 year olds say they don't want tailored ads when we include those saying it is not OK to tailor for them based on tracking on "other websites" they have visited. The rejection of tailored content goes up to 90% when what they do "offline—for example, in stores"—is the behavioral-tracking method.

Tables 6 and 7 show that the percentages of young adults saying no to tailored discounts and news are also quite high when we take into account those who say no to the types of behavioral-tracking. Looking across all the age groups, we see that not all the differences between them are significant statistically. Nevertheless, three broad patterns do emerge:

**Table 4: Please Tell Me Whether Or Not You Want Websites You Visit to Show You Ads/Discounts/News That Are Tailored To Your Interests.***

| | Age 18-24 | Age 25-34 | Age 35-49 | Age 50-64 | Age 65-89 | Total |
|---|---|---|---|---|---|---|
| **Tailored Ads*** | | | | | | |
| No | 55 | 59 | 67 | 77 | 82 | 66 |
| Yes | 45 | 41 | 33 | 23 | 18 | 34 |
| **Tailored Discounts*** | | | | | | |
| No | 37 | 44 | 50 | 58 | 70 | 51 |
| Yes | 64 | 56 | 50 | 42 | 30 | 49 |
| **Tailored News** | | | | | | |
| No | 54 | 52 | 57 | 62 | 68 | 58 |
| Yes | 46 | 48 | 43 | 38 | 32 | 42 |

* Using the $Chi^2$ statistic, the differences are significant at the .05 level. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation.

**Table 5: Saying *Not OK* or *OK* to Ads Tailored Based on Age and Three Tracking Activities§**

| .. based on | Age 18-24 | Age 25-34 | Age 35-49 | Age 50-64 | Age 65-89 | Total |
|---|---|---|---|---|---|---|
| "the website you are visiting"* | | | | | | |
| Not OK | 67 | 70 | 72 | 82 | 87 | 75 |
| OK | 33 | 30 | 27 | 18 | 13 | 25 |
| "*other* websites you have visited" | | | | | | |
| Not OK | 86 | 82 | 86 | 91 | 95 | 87 |
| OK | 14 | 18 | 14 | 9 | 5 | 13 |
| "what you do *offline*—for example, in stores." | | | | | | |
| Not OK | 90 | 88 | 86 | 92 | 95 | 89 |
| Not OK | 10 | 12 | 14 | 8 | 5 | 11 |

§*Not OK* includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the $Chi^2$ statistic, the differences are significant at the .05 level.

**Table 6: Saying *OK* or *Not OK* to Discounts Tailored Based on Age and Three Tracking Activities[8]**

| ..based on - | Age 18-24 | Age 25-34 | Age 35-49 | Age 50-64 | Age 65-89 | Total |
|---|---|---|---|---|---|---|
| "the website you are visiting"* | | | | | | |
| Not OK | 61 | 58 | 62 | 74 | 81 | 66 |
| OK | 39 | 42 | 38 | 26 | 19 | 34 |
| "other websites you have visited"* | | | | | | |
| Not OK | 77 | 76 | 80 | 86 | 90 | 81 |
| OK | 23 | 24 | 20 | 14 | 10 | 19 |
| "what you do *offline*— for example, in stores."* | | | | | | |
| Not OK | 74 | 80 | 80 | 86 | 91 | 82 |
| OK | 26 | 20 | 20 | 14 | 9 | 18 |

**Table 7: Saying *OK* or *Not OK* to News Tailored Based on Age and Certain Tracking Activities[8]**

| ..based on - | Age 18-24 | Age 25-34 | Age 35-49 | Age 50-64 | Age 65-89 | Total |
|---|---|---|---|---|---|---|
| "the website you are visiting" | | | | | | |
| Not OK | 68 | 73 | 72 | 77 | 85 | 74 |
| OK | 32 | 27 | 28 | 23 | 15 | 26 |
| "other websites you have visited"* | | | | | | |
| Not OK | 79 | 82 | 85 | 90 | 94 | 85 |
| OK | 21 | 18 | 15 | 10 | 6 | 15 |
| "what you do *offline*— for example, in stores." | | | | | | |
| Not OK | 84 | 85 | 85 | 91 | 96 | 87 |
| OK | 16 | 15 | 15 | 9 | 4 | 13 |

[8] In Tables 6 and 7, *Not OK* includes those who said no to tailored advertising at the outset. The table excludes the small percentages that said *Don't Know* or *Maybe*. See text for further explanation. *Using the $Chi^2$ statistic, the differences are significant at the .05 level.

- In the tables where the comparisons are statistically significant, older groups of Americans reject tailoring and the forms of behavioral tracking in higher percentages than do groups of younger Americans.

- All age groups have somewhat more tolerance for tailoring and behavioral tracking when carried out for discounts than when carried out for advertisements and news.

- Every age group has somewhat more tolerance for behavioral tracking when carried out on the website they are visiting compared to when carried out on other websites or offline, as in stores.

These interesting distinctions should not let us lose sight of the overarching finding: *When we combine Americans who reject tailored content outright with those who said they would want it but changed their minds when told of one or another form of tracking that would yield the tailored content, we find that substantially over 60% of all groups—and often over 80%— say no to the activity.* That includes the younger Americans who marketing executives have asserted don't care about being tracked as long as they can get relevant content.

**Attitudes Toward Tailored Ads By Privacy Experience, Institutional Confidence, And Privacy Knowledge**

Because of current policy interests in advertising-related behavioral targeting, we sought to understand whether Americans' acceptance or rejection of toward tailored advertising related to three aspects of their lives—bad experiences they might have had with information theft, their confidence in the way businesses and the law handle their information, and their knowledge of laws that relate to whether or not firms can sell their information in the online and offline worlds. We defined "bad privacy experiences" as ever having had one or more of the following happen: someone "used or revealed personal information about you without your permission" (it happened to 39%), someone "made a purchase on your credit card or opened a new credit card in your name without your permission" (that happed to 28%), and you "receive a notice in your postal mail that your personal information has been lost or stolen—for example, in a security breach" (it happened to 31%). We defined confidence in business and law through three statements noted in Table 8 that are borrowed from privacy researcher Alan Westin.[16] And we defined online and offline knowledge via the true-false questions in Table 8.

Each of these areas in itself provides an important insight into Americans' relation to their personal information. Further analysis of the answers revealed that 38% of Americans have never had one of the bad privacy experiences noted, 32% have had one experience, 21% have had two, and 9% have had all three. We also found that 47% of our respondents agree and 20% agree strongly that "consumers have lost all control over how personal information is collected and used by consumers." Despite these bad experiences and a belief that they have no control over their personal information, Americans have confidence that businesses and laws do protect them: 53% of our respondents agreed and 5% agreed strongly that "most businesses handle the personal

information they collect about consumers in a proper or confidential way." Most also express confidence in "laws and organizational practices," with 50% agreeing and 4% agreeing strongly that they "provide a reasonable level of protection for consumer privacy today."

Part of the reason that majorities believe that businesses or laws protect them may well be because Americans mistakenly assume that laws do not allow businesses to sell personal information . Table 9 shows that, in fact, a substantial majority does not know the correct answers to most true-false statements about companies' rights to share and sell information about them online and off. Further analysis revealed that individual respondents on average answered only 1.5 of the 5 online statements and 1.7 of the 4 offline statements correctly.

The score on the online or offline privacy indexes—that is, knowledge a person has about privacy law—has no statistical relationship with whether or not a person will agree to tailored ads. Likewise, having one or more bad privacy experiences does not associate with being for or against receiving tailored ads. By contrast, beliefs about personal control and social protection do make a difference, as Table 10 indicates: Agreeing that consumers have lost all control over personal information is significantly associated with not wanting tailored advertising. And having confidence that companies and existing laws protect people increases the statistical likelihood that that a person will want tailored advertising.

**Asserting Rights Around Behavioral Tracking**

Shifting attention from tailored content to behavioral tracking of people online and off, Table 11 presents the responses to five questions about an individual's opinions about laws that ought to apply to firms' behavioral tracking. Large majorities share the same views:

- 69% feel there should be a law that gives people the right to know everything that a website knows about them.
- 92% believe there should be a law that requires "websites and advertising companies to delete all stored information about an individual, if requested to do so."
- 63% believe advertisers should be required by law to immediately delete information about their internet activity.
- 70% stated that a company should be fined more than the maximum amount suggested ($2,500) "if a company purchases or uses someone's information illegally."

The responses about the maximum fine suggested a level of indignation, even anger, by the public when it comes to misusing information. More evidence of this reaction can be seen in the belief by 18% that a company that uses a person's information illegally should "be put out of business" and the additional 35% who agree that "executives who are responsible should face jail time." (See Table 12.)

**Table 8: Americans' confidence in the way businesses and the law handle their information** (N=1,000)

| | Strongly Agree (%) | Agree (%) | Disagree (%) | Strongly Disagree (%) | DK (%) |
|---|---|---|---|---|---|
| Consumers have lost all control over how personal information is collected and used by companies. | 20 | 47 | 27 | 4 | 2 |
| Most businesses handle the personal information they collect about consumers in a proper and confidential way. | 5 | 53 | 32 | 6 | 4 |
| Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. | 4 | 50 | 34 | 8 | 4 |

DK=Don't Know

**Table 9: Americans' Knowledge of Laws Online and Offline* (N=1,000)**

| **Online**: | *False* (%)* | True (%) | DK (%) |
|---|---|---|---|
| If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission. | 22 | 62 | 16 |
| If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government. | 46 | 26 | 28 |
| If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so. | 20 | 54 | 26 |
| If a website violates its privacy policy, it means that you have the right to sue the website for violating it. | 19 | 46 | 35 |
| If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission. | 48 | 33 | 19 |
| **Offline:** | | | |
| When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission. | 49 | 36 | 15 |
| When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission. | 31 | 44 | 25 |
| When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission. | 57 | 28 | 15 |
| When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission. | 33 | 49 | 18 |

***For each statement, *false* is the correct answer**.

**Table 10: Americans' Desire For Tailored Ads Based on Confidence In The Way Businesses And The Law Handle Their Information**

| Please tell me whether or not you want websites you visit to show you ads tailored to your interests. ▸ | No, would Not (%) | Yes, Would (%) |
|---|---|---|
| Consumers have lost all control over how personal information is collected and used by companies.* | | |
| Agree | 71 | 29 |
| Disagree | 60 | 40 |
| Most businesses handle the personal information they collect about consumers in a proper and confidential way. * | | |
| Agree | 61 | 39 |
| Disagree | 77 | 23 |
| Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.* | | |
| Agree | 61 | 39 |
| Disagree | 76 | 24 |

* Using the $Chi^2$ statistic, the differences are significant at the .05 level.

**Table 11: Asserting Rights Around Behavior Tracking**

| | N=1,000 (%) |
|---|---|
| *Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?* | |
| Yes, there should be a law | 69 |
| No, a law is not necessary | 29 |
| DK | 2 |
| *Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, if requested to do so.* | |
| Yes, there should be a law | 92 |
| No, a law is not necessary | 7 |
| DK | 1 |
| *Advertisers would like to keep and store information about your internet activity. How long should they be able to keep it? Do you think--* | |
| They should have to delete it immediately, OR | 63 |
| They should be allowed to keep it for a few months, OR | 25 |
| They should be allowed to keep it for a year, OR | 6 |
| They should be allowed to keep it for as long as they want | 4 |
| DK | 2 |
| *If a company purchases or uses someone's information illegally, about how much—if anything—do you think that company should be fined?* | |
| $100 | 2 |
| $500 | 4 |
| $1,000 | 9 |
| $2,500 | 7 |
| More than $2,500 | 70 |
| It depends | 4 |
| DK | 4 |
| *Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which one of the following ways to punish companies do you think is most important?* | |
| The company should fund efforts to help people protect privacy | 38 |
| Executives who are responsible should face jail time | 35 |
| The company should be put out of business | 18 |
| The company should not be published in any of these ways | 3 |
| It depends | 2 |
| DK | 4 |

DK=Don't Know

**Table 12: "Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which *one* of the following ways to punish companies do you think is most mportant?"**

| | N=1,000 (%) |
|---|---|
| The company should fund efforts to help people protect privacy. | 38 |
| Executives who are responsible should face jail time. | 35 |
| The company should be put out of business | 18 |
| The company should not be punished in any of these ways | 3 |
| It depends; don't know | 6 |

## Conclusion

It is noteworthy that 38% of Americans told us that companies that use a person's information illegally should "fund efforts to help people protect privacy." While the choice doesn't suggest the anger of "the company should be put out of business" or "executives who are responsible should face jail time," it does reflect concern about the state of information privacy that is demonstrated in the answers about tailored content and behavioral tracking. Americans' widespread rejection of relevant tailored advertising is particularly startling because it flies in the face of marketers' consistent contention that Americans desire for relevant commercial messages justifies a variety of tracking activities. When three contemporary forms of behavioral tracking are highlighted, rejection of tailored ads is even more widespread. The finding applies across all age groups, including young adults, a cohort that media executives have insisted cares little about information privacy.

The desire by a majority of Americans not to be followed for the purpose of tailored content comes at a time when behavioral targeting is a fast-growing advertising practice upon which many content providers have staked their businesses. A mini-industry is growing up around the process, with companies such as DoubleClick, Audience Science, and Akamai following the activities of individuals in ways that yield detailed suggestions about what kinds of people they are, what that means for their perspectives on life, how that has translated into what they bought recently, and how that might transfer into the products and services they might buy in the near future. At this point the sketches are often not connected to a person's "offline" or real name and postal address. However, a political consensus is emerging that this point hardly matters when the person's digital trail is a treasure trove of data that marketers can use to de facto identify the individual across the internet, drawing inferences about personality, gender, location, interests, purchasing power, and more.

Our research did not inquire into why Americans do not want companies to tailor relevant advertising, discounts, or news for them. We can suggest, however, that many of them understand that behavioral targeting can lead to hidden forms of social discrimination. Many may be

uncomfortable with the realization that tailored content and tracking go hand-in-hand. They may know that these activities can lead marketers to retail policies that place them at a disadvantage compared to other consumers. They may fear receiving tailored ads for products that are not as upscale and tailored discounts that are not as generous as the ones their neighbors get. They may worry, too, that news served to them based on criteria they don't understand may separate them from views of the world received by others whom marketers judge differently.

Whatever the reasons explaining Americans' dislike of behavioral targeting, our findings indicate that they expect companies to take privacy rules extremely seriously. Our results show that Americans consumers believe (albeit mistakenly) that an array of strong laws prohibit companies from sharing or selling of data about them. Recall, too, that 70% went beyond the highest option we provided for fines resulting from illegal use of people's data, and that a substantial proportion wanted significant non-monetary sanctions, including liquidation of companies and jail time for employees. Moreover, when asked whether or not they want regulations demanding control and transparency, they say "Yes" in large proportions. 63% prefer immediate deletion of data marketers hold about them, and 25% choose the next most restrictive option—"a few months." 92% percent want a law requiring websites and advertising companies to delete all stored information upon request. While data-intensive companies have resisted calls to reduce data retention and have grudgingly accepted shorter retention times, Americans want them to go farther.

Such a strong preference for a right to delete means that consumers want a way to meaningfully object and withdraw from certain practices around the collection and use of their data. This response is not possible today short of engaging in some very disciplined internet browsing habits or refusing to use the internet at all. And even if they do opt out, their actions are still tracked, and data about their internet use can still be collected. Moving forward, policymakers must be savvy to similar self-regulatory proposals that create illusory protections. There is a real risk that future industry proposals will use technical means to ensure continued website ("first party") and cross-website or even cross-media ("third party") tracking while leading the consumer to believe that such tracking has been limited--for example, by masking third-party tracking to imply it is carried out by the first party.

This survey's findings support the proposition that consumers should have a substantive right to reject behavioral targeting and its underlying practices. Rejection could take the form of a reinvigorated opt out right that actually pertains to collection of information. It could also be implemented through a procedure to enforce an option to delete records. In fact, default rules creating opt in and opt out may be less important than time limits for keeping data. While some accommodations may need to be made for keeping data for security reasons, firms should not be able to use data for marketing purposes for periods longer than those consumers want.

In recent months, a variety of suggestions have been made in this direction by industry and advocacy groups.[17] Our survey findings indicate that the most persuasive of these approaches

encourage transparency and retention limits in marketers' actions and consumers' ability to exercise control over the data companies collect about them. To these important suggestions, we would like to add a broad operating value: Companies need to *respect* their publics rather than to treat them as objects from which they can take information in order to optimally persuade them with no clear option not to participate. Traditionally the potential for harm and unwanted intrusion have been cited as justifications for protecting the privacy of people's information. Respect ought to be encouraged as a positive, trust-building reason for protecting information privacy. Respect as a value requires marketers to promote information reciprocity. That is, in return for collecting and using consumers' data, marketers should allow those consumers to learn exactly where the information came from and how it is being used. Marketers should also allow consumers to decide which of the collected data should be used and for what purposes, and which should be deleted.

Joseph Turow has suggested that marketers create a privacy dashboard that would allow consumers to interact with data the firms have collected about them.[18] Beyond informing people about the information circulating about them, their interaction with data through these dashboards will do more to make the public savvy about their information and how to protect it than will wordy paragraphs and lengthy privacy policies on websites. Implementing a regime of respect around the collection and use of consumer information will not be easy. Our findings in this survey suggest, however, that such activities are imperative for a public that broadly dislikes the emerging contemporary data-gathering regime.

## REFERENCES

[1] Audience Science Press Release, "AudienceScience Behaviorally Targets Video Advertising With Hulu," *Marketwire*, July 14, 2009, via Lexis Nexis.

[2] Ashkan Soltani et al., "Flash Cookies and Privacy," University of California School of Information, 2009, http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1446862

[3] See http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

[4] NAI, "FAQs," http://www.networkadvertising.org/managing/faqs.asp#question_11, accessed August 31, 2007.

[5] Federal Trade Commission, "Self-Regulatory Principles for Online Behavioral Advertising," February 2009.

[6] See Holly Sanders Ware, "Google Is Faulted On Privacy," *New York Post*, July 10, 2009, p. 37.

[7] Ryan Singel, "You Deleted Your Cookies? Think Again," *Wired*, August 10, 2009.

[8] Collin O'Malley, VP of Strategic Business at TRUSTe, in TRUSTe press release, "Behavioral Targeting: Not that Bad?!" *Marketwire*, March 4, 2009, via Lexis Nexis.

[9] Louise Story, "Bits" New York Times, November 5, 2007, p. C-6.

[10] Noelle McElhatton, Noelle McElhatton, Marketing Direct, July 27, 2009, http://www.marketingdirectmag.co.uk/channel/directmarketing/article/922859/Disney-CEO-says-young-consumers-dont-care-behavioural-targeting-privacy/ , accessed September 3, 2009.

[11] Mark Wilmot, "The Welcome Mat," *Marketing Daily*, July 28, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=110489

[12] Audience Science Press Release, "AudienceScience Behaviorally Targets Video Advertising With Hulu," *Marketwire*, July 14, 2009, via Lexis Nexis.

[13] Google, "Make the Ads You See More Interesting," accessed on August 31, 2009.

[14] National Advertising Initiative, "Opt Out of Behavioral Advertising," http://www.networkadvertising.org/managing/opt_out.asp accessed August 31, 2009. Emphasis in original.

[15] Mediapost, August 14, 2009

[16] See Ponnurangam Kumaraguru and Lorrie Faith Cantor, "Privacy Indexes: A Survey of Westin's Studies," Carnegie Mellon University (CMU-ISRI-5-138), December 2005.

[17] See, for example, "Online Behavioral Tracking and Targeting, Legislative Primer," produced by the Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group, and World Privacy Forum, September 2009; and Arnold and Porter, LLP, "The Great Behavioral Advertising (BA) Debate Continues," *Consumer Advertising Law Blog*, Sept 17, 2009, http://www.consumeradvertisinglawblog.com/2009/09/the-great-ba-debate-continues.html

[18] See Saul Hansell, "An Icon That Says They're Watching You," New York Times, March 19, 2009, http://bits.blogs.nytimes.com/2009/03/19/an-icon-that-says-theyre-watching-you/

# HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES & POLICIES?

**APRIL 14, 2010**

"We suggest...that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data." (see page 20)

**Chris Hoofnagle**
UC Berkeley School of Law, Berkeley Center for Law and Technology

**Jennifer King**
UC Berkeley School of Information

**Su Li**
UC Berkeley School of Law, Center for the Study of Law and Society

**Joseph Turow**
Annenberg School for Communication, University of Pennsylvania

**Chris Jay Hoofnagle**, J.D., is director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law. Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice law in California and Washington, DC.

**Jennifer King**, MIMS, is a Ph.D. candidate at the UC Berkeley School of Information. Most recently she was a researcher at the Samuelson Law, Technology, and Public Policy Clinic at UC Berkeley's School of Law. Her research areas include information privacy and security, usability and human-computer interaction, video surveillance and other sensor networks. With Chris Hoofnagle, King has published three reports exploring Californians' privacy attitudes, available at SSRN.com.

**Su Li**, Ph.D., recently joined Berkeley Law as its new Statistician in Empirical Legal Studies. Her research interests include gender and social inequality, economic sociology, social network analysis, and the sociology of education. Li received her Ph.D. in Sociology and a Master's in Mathematical Models for Social Science at Northwestern University. An expert in quantitative methodology, Li was Assistant Professor of Sociology at Wichita State University before joining Berkeley Law.

**Joseph Turow**, Ph.D., is Robert Lewis Shayon Professor of Communication at the Annenberg School for Communication, University of Pennsylvania. Among his several books are *Niche Envy: Marketing Discrimination in the Digital Age* (MIT Press, 2006) and *Breaking Up America: Advertisers and the New Media World* (U of Chicago Press, 1997). Since 1999 he has conducted national telephone surveys that have moved forward public discourse on digital media, marketing, and privacy. Several can be found at the Annenberg Public Policy Center website, APPCPenn.org.

This survey was supported by the Rose Foundation for Communities and the Environment, Tim Little, Executive Director, under grant 025629-003, Chris Jay Hoofnagle, Principal Investigator; and by The Annenberg School for Communication—Michael Delli Carpini, Dean.

## Overview

Media reports teem with stories of young people posting salacious photos online, writing about alcohol-fueled misdeeds on social networking sites, and publicizing other ill-considered escapades that may haunt them in the future. These anecdotes are interpreted as representing a generation-wide shift in attitude toward information privacy. Many commentators therefore claim that young people "are less concerned with maintaining privacy than older people are."[1] Surprisingly, though, few empirical investigations have explored the privacy attitudes of young adults.[2] This report is among the first quantitative studies evaluating young adults' attitudes. It demonstrates that the picture is more nuanced than portrayed in the popular media.

In July 2009, we commissioned a nationally representative telephone survey (landline and cellular) of Americans in order to understand the public's views of both online and offline privacy issues. Our first report from this effort, *Americans Reject Tailored Advertising and Three Activities that Enable It*,[3] released in October 2009, investigated Americans' comprehension of online tailored advertising and related privacy concerns. In this report, we compare young adults and older adults with respect to attitudes toward online privacy protection, whether they carry out certain privacy-protecting behaviors, their public policy preferences regarding privacy, and their knowledge of information privacy law that might affect them in their everyday lives. We found that expressed attitudes towards privacy by American young adults (aged 18-24) are not nearly as different from those of older adults as many suggest. With important exceptions, large percentages of young adults are in harmony with older Americans when it comes to sensitivity about online privacy and policy suggestions. For example, a large majority of young adults:

---

[1] Ariel Maislos, chief executive of Pudding Media, quoted in Louise Story, *Company Will Monitor Phone Calls to Tailor Ads*, New York Times, Sept. 24, 2007, available at: http://www.nytimes.com/2007/09/24/business/media/24adcol.html.

[2] Marwick, A., Murgia-Díaz, D., and Palfrey, J. (2010). Youth, Privacy and Reputation Literature Review. Berkman Center for Internet and Society, Harvard University.

[3] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, SSRN ELIBRARY (2009), http://ssrn.com/paper=1478214.

- Has refused to give information to a business in cases where they felt it was too personal or not necessary;
- Believes anyone who uploads a photo of them to the internet should get their permission first, even if taken in public;
- Believes there should be a law that gives people the right to know all the information websites know about them; and
- Believes there should be a law that requires websites to delete all stored information about an individual.

In view of these findings, why would so many young adults act in social networks and elsewhere online in ways that would seem to offer quite private information to all comers? A number of answers present themselves, including suggestions that people 24 years and younger approach cost-benefit analyses related to risk differently than do individuals older than 24. An important part of the picture, though, must surely be our finding that higher proportions of 18-24 year olds believe incorrectly that the law protects their privacy online and offline more than it actually does. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner.

## Background

Popular writings and comments suggest that America's youngest adults do not care about information privacy, particularly online. As evidence, many point to younger internet users' adoption and prolific use of blogs, social network sites, posting of photos, and general documenting and (over)sharing of their life's details online, from the mundane to the intimate, for all the world to consume. "Young adults**,"** exhorted one newspaper article to that segment of its readers, "you might regret that scandalous Facebook posting as you get older."[4] More broadly, Robert Iger, CEO of Disney, recently commented categorically that "kids don't care" about privacy issues, contending that complaints generally came from much older consumers. Indeed, he said that when

[4] Roger [no surname], "There is No Privacy," *Virginia Pilot*, April 4, 2009, p. B9.

he talked to his adult children about their online privacy concerns "they can't figure out what I'm talking about."[5]

Iger is not alone in making claims about differences between young people—even college students—and older members of the population when it comes to giving out personal information online. Anecdotes abound detailing how college-age students post photos of themselves unclothed and/or drunken, for the entire world—including potential employers—to see. It is not a leap to argue that these actions are hard-wired into young people. One psychological study found that adolescents (aged 13-16) and what they termed "youths" (those aged 18-22) are "more inclined toward risky behavior and risky decision making than are 'adults' (those older than 24 years) and that peer influence plays an important role in explaining risky behavior during adolescence." Their finding was more pronounced among adolescents than among the youths, but differences between youths and adults were striking in willingness to take risks—particularly when group behavior was involved.[6] Although the authors do not mention social media, the findings are clearly relevant to these situations. There the benefits of looking cool to peers may outweigh concerns about negative consequences, especially if those potential consequences are not likely to happen immediately. A related explanation for risky privacy behavior on social-networking sites is that they encourage users to disclose more and more information over time.

Young people's use of social media does not in itself mean that they find privacy irrelevant.[7] Indeed, the Pew Internet & American Life Project found in 2007 that teenagers used a variety of techniques to obscure their real location or personal details on social networking sites.[8] That study fits with the findings of other researchers, who have

---

[5] Gina Keating, "Disney CEO Bullish on Direct Marketing to Consumers," Reuters, July 23, 2009, http://www.reuters.com/article/idUSTRE56M0ZY20090723?pageNumber=2&virtualBrandChannel=0

[6] Margo Gardner and Laurence Steinberg, "Peer Influence on Risk Taking, Risk Preference, and Risky Decision Making in Adolescence and Adulthood: An Experimental Study," *Developmental Psychology* 41:4, 625-635. No one 23 or 24 years of age was in the sample.

[7] Raynes-Goldie, Kate. "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook" *First Monday* [Online], Volume 15 Number 1 (2 January 2010); Lenhart, Amanda and Madden, Mary. "Teens, Privacy, and Online Social Networks." Pew Internet & American Life Project, April 18. 2007. Available at: http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx; and more generally danah boyd's excellent bibliography of Social Networking Studies at: http://www.danah.org/researchBibs/sns.html.

[8] Lenhart and Madden, *Id*.

urged the importance of reframing the issue to ask *what dimensions* of privacy younger adults care about.[9] While differences between young adults and those older than they may be important, other more subtle commonalities may be ignored. In recent years older age groups have rushed to social networking in large numbers with discussions of personal issues and details. A common anecdotal observation is that young adults and adolescents are more likely than their elders to post racy photos or document episodes of untoward behavior. If research shows this distinction is accurate, the question nevertheless remains whether the same, higher, or lower percentages of Americans over 24 years old reveal more subtle but important private information about themselves that might lead to embarrassing and unfortunate incidents, such as identity theft.

In spite of vigorous social concerns and discussions, there does not appear to be research that shows definitively that young adults are fundamentally different from older Americans when it comes to privacy attitudes. Moreover, comparisons of what people of different ages do online must be placed within a context of how they understand the norms and laws of privacy in their society. What, if anything, have they done to protect their privacy? What do they believe about privacy norms when presented with the opportunity to think rationally about them? And what protections do they believe laws afford them when they do present themselves in various online environments? The extent to which Americans of different ages have similar or different answers to these questions will suggest whether they converge on similar policy approaches despite seemingly different decisions in the heat of online activities. That is the topic we chose for this study.

In our earlier report on tailored advertising we compared age groups' responses to three questions that asked, "Please tell me whether or not you want websites you visit to show you *ads* [another question substituted *discounts* and a third *news*] that are tailored to your interests." We found that while young adults' concerns were lower compared to other age categories, substantial proportions nevertheless said they did not want tailoring of ads, discounts, and news (55%, 37%, and 54% respectively). Moreover, the percentages saying no rose to very high levels when the young adults were told that the information required to tailor advertisements would come from following them on the

[9] See Raynes-Goldie (2010).

website they were visiting (67% said no), on other websites they have visited (86% said no) and what they do offline—for example, in stores (90% said no).[10] The findings led us to believe that these tendencies might apply to young adults' approaches to privacy in general. We hypothesized a dual dynamic: A smaller percentage of young adults than older adults would evidence privacy concerns, but that percentage would still be large, typically exceeding 50% of young adults. We did find this dynamic at work. But we also noted that differences in privacy attitudes and practices between young adults and older ones were at times so small as to not be statistically significant.

## Methods

In 2009, we commissioned a survey on behalf of the Berkeley Center for Law and Technology at the University of California, Berkeley School of Law in order to gauge the American public's attitudes towards and knowledge of the rules and practices surrounding the collection and use of personal information. In this report, we present a summary of our findings for a subset of our survey questions.[11] These questions were part of a survey of Americans' opinions about and understanding of a variety of online and offline privacy issues. We cast our population net broadly. We included people in our study if they were 18 years or older said yes to one of the following questions: "Do you go on online or use the internet, at least occasionally?" and "Do you send or receive email, at least occasionally?"

The survey was conducted from June 18 to July 2, 2009 by Princeton Survey Research Associates International. PSRA conducted telephone interviews with a nationally representative, English-speaking sample of 1,000 American adults living in the continental United States. A combination of landline (n=725) and wireless (n=275) random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. The interviews averaged 20 minutes. Based on a seven callback procedure and using the American Association of Public Opinion research (AAPOR) RR3 method, a standard for this type of survey, the overall response rates were a typical 18 percent for the landline sample and

[10] *Id*. at Fn. 3.
[11] *Id*.

22 percent for the cellular sample. Statistical results are weighted to correct known demographic discrepancies.[12] The margin of sampling error for the complete set of weighted data is ±3.6 percent at the 95 percent confidence level. The margin of error is higher for smaller subgroups within the sample.

Table 1 presents the characteristics of the sample. For this report, we created cross-tabulations of a subset of our survey questions to compare responses across typical age categories (18-24, 25-34, 35-44, 45-54, 55-64, and 65+). Because some people didn't reveal their age, the total for this study's sample is 975 individuals. We considered chi-square values for each table significant at the level of $p < .05$. When the chi-square tests were significant, we used two sample t-tests to discover whether there are statistically significant differences between the 18-24 year olds and all the older adults (i.e. 18-24 compared to 25-65+). We also used Scheffe post-hoc tests to examine if any two age groups are significantly different from each other (e.g. 18-24 vs. 25-34 or 18-24 vs. 35-44) on each possible answer to the question being asked in the tables. For both t-tests and Scheffe tests[13] we considered significance to be at the level of $p < .05$.

All tables presented in this paper are based on the weighted sample of the data,

[12] A two-stage procedure was used to weight this dual-frame sample. A first-stage weight was applied to account for the overlapping sample frames. The first stage weight balanced the phone use distribution of the entire sample to match population parameters. The phone use parameter was derived from an analysis of the most recently available National Health Interview Survey (NHIS) data along with data from recent dual-frame surveys. (See Blumberg SJ, Luke JV, "Wireless substitution: Early release of estimates from the National Health Interview Survey, July-December, 2008." National Center for Health Statistics. May 2009.) This adjustment ensures that the dual- users are appropriately divided between the landline and cell sample frames.

The second stage of weighting balanced the total sample demographics to population parameters. The total sample was balanced to match national population parameters for sex, age, education, race, Hispanic origin, region (U.S. Census definitions), population density, and telephone usage. The basic weighting parameters came from a special analysis of the Census Bureau's 2008 Annual Social and Economic Supplement (ASEC) that included all households in the continental United States. The population density parameter was derived from Census 2000 data. The telephone usage parameter came from the analysis of NHIS data.

We conducted all analyses in this report using SPSS on a weighted random sample. Due to the unique way that SPSS handles weight, we applied the standardized weight in all analyses so that the sample was corrected by population proportion but not by population size. That is, the sample size was not inflated to the original population size in our analysis. Using the standardized weight prevents the risk of unduly reducing standard errors in significance tests and thereby prevents the risk of having type I errors in the analysis.

[13] Since Tables 15 and 16 involve indexed variables, on top of the tests on the comparisons of percentages we conducted additional t-tests and Scheffe tests to compare the means of the created indexed variables. See text for details.

with a valid sample size of 975. However, applying weights causes rounding errors in cross-tabulations, which is the reason that the Ns in all tables, except for Table 11, appear as a number other than 975.

**Table 1: Characteristics of U.S. Adults in Sample (N=1,000)***

| | % |
|---|---|
| **Sex** | |
| Male | 48 |
| Female | 52 |
| **Age** | |
| 18-24 | 14 |
| 25-34 | 21 |
| 35-44 | 20 |
| 45-54 | 19 |
| 55-64 | 15 |
| 65+ | 8 |
| Refused | 3 |
| **Race** | |
| White | 78 |
| Black or African American | 9 |
| Asian or Pacific Islander | 4 |
| American Indian or Alaskan Native | 1 |
| Mixed Race | 2 |
| Other/Don't Know/Refused | 6 |
| **Hispanic or Latino Background?** | |
| Yes | 11 |
| No | 88 |
| Don't Know/Refused | 1 |
| **Household Income** | |
| Under $30,000 | 21 |
| $30,000 to under $50,000 | 19 |
| $50,000 to under $75,000 | 17 |
| $75,000 and Over | 33 |
| Don't Know/Refused | 10 |
| **Region of the Country** | |
| Northeast | 19 |
| Midwest | 22 |
| South | 33 |
| West | 26 |

*When the numbers don't add to 100% it is because of a rounding error.

## Findings

The following tables will elaborate on a basic theme: Large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions. In several cases, there are no statistically significant differences between young adults and older age categories on these topics. For most of the questions we asked, there is a statistically significant difference between the youngest adults and older age categories. However, even in these cases over half of the young adult-respondents did answer in the direction of older adults. There clearly is *social significance* in that large numbers of young adults—in some cases, 80-90 percent—agree with older Americans on issues of information privacy.

### Table 2 – Refused to Provide Information

| **Have you ever refused to give information to a business or a company because you thought it was not really necessary or was too personal?** | **Total** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Yes, have* | 88% | 82% | 84% | 91% | 93% | 92% | 85% |
| *No, have not* | 11% | 18% | 13% | 9% | 7% | 7% | 14% |
| *Don't know/refused* | 1% | 0% | 3% | 0% | 0% | 1% | 1% |
| *Total* | 974 | 139 | 206 | 197 | 195 | 151 | 86 |

$x^2$= 34.158, df = 10, $p < .001$

### Table 3 – Uploading Where I am Recognizable

| **Generally speaking, anyone who uploads a photo or video of me to the internet where I am clearly recognizable should first get my permission.** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Strongly agree or Agree* | 86% | 84% | 81% | 86% | 90% | 91% | 88% |
| *Strongly disagree or Disagree* | 13% | 16% | 18% | 13% | 9% | 9% | 8% |
| *Don't know/refused* | 1% | 0% | 2% | 1% | 1% | 0% | 3% |
| *Total* | 973 | 140 | 206 | 197 | 195 | 150 | 85 |

$x^2$= 22.8, df = 10, $p < .05$; Differences are significant but not related to young adults vs. older adults. See text.

## Table 4 – Right To Know

| **Do you think there should be a law that gives people the right to know everything that a website knows about them, or do you feel such a law is not necessary?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Yes, should be a law* | 68% | 62% | 68% | 73% | 71% | 64% | 69% |
| *No, law is not necessary* | 30% | 35% | 31% | 24% | 28% | 31% | 30% |
| *Don't know/refused* | 2% | 3% | 2% | 3% | 1% | 5% | 1% |
| *Total* | 976 | 141 | 206 | 197 | 196 | 150 | 86 |

$x^2$= 12.3, df = 10, $p$ = .27 : Differences not significant

## Table 5 – Right To Delete

| **Do you think there should be a law that requires websites and advertising companies to delete all stored information about an individual, or do you feel such a law is not necessary?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Yes, should be a law* | 92% | 88% | 91% | 90% | 94% | 94% | 90% |
| *No, law is not necessary* | 8% | 11% | 7% | 10% | 5% | 5% | 9% |
| *Don't know/refused* | 1% | 1% | 1% | 0% | 1% | 1% | 1% |
| *Total* | 975 | 139 | 207 | 197 | 195 | 150 | 87 |

$x^2$= 10.6, df = 10, $p$ = .39 : Differences not significant

These dynamics are visible quite clearly in Tables Two through Five, which report on Americans' sensitivity regarding privacy issues. Large proportions of all age groups have refused to provide information to a business for privacy reasons. They agree or agree strongly with the norm that a person should get permission before posting a photo of someone who is clearly recognizable to the internet, even if that photo was taken in public. They agree that there should be a law that gives people the right to know "everything that a website knows about them." And they agree that there should be a law that requires websites and advertising companies to delete "all stored information" about an individual. In the case of the first issue (see Table Two), a statistically significant lower proportion of 18-24 year olds agrees with these positions, but this proportion of young adults agreeing or agreeing strongly was nevertheless over 80%.[14] With respect to

[14] In Table 2, when comparing the 18-24 year olds to the rest of the sample, the differences in the percentages between the two groups are statistically significant at .05 level according to a two-sample t-test. Interestingly, the Scheffe tests of differences between 18-24 year olds and each of the other groups show no significance at .05 level. With respect to Table 3, although answers to this question are

the other three issues (see Tables Three through Five), the differences between the 18-24 year olds and the other adults are not statistically significant: both young and old alike are in agreement.

Privacy Practices

We also sought to determine whether young adults were different from other adult categories when it came to common privacy-related practices—whether they read privacy policies, how frequently they erase their browser cookies, whether or not they had ever changed their mind about an online purchase because of a privacy or security concern, and how frequently they check their credit report. In the case of reading privacy policies, there are no statistical differences among age groups. As Table 6 shows, about half the adult population, including young adults, says it reads policies often or sometimes. When it comes to erasing cookies (Table 7), 58% of young adults say they erase cookies often or sometimes. Statistical tests beyond the chi-square also indicate that age differences are essentially not statistically significant. The t-test tells us that the only statistically significant finding involves the higher proportion of 18-24 year olds answering "hardly ever" compared to the rest of adults. The Scheffe test finds no significance at all between the answers of young adults and the other age groups when it comes to erasing cookies.

About half of young adults have changed their mind about a purchase because of some privacy concern. Post hoc comparisons of the data in Table 8 show no significant difference between young adults and the rest of the population.

We did find a difference regarding checking credit reports. A substantially lower percentage of 18-24 year olds does that, with statistically significant differences from the other age groups centering on their answers of "about once a year," and "less often than once a year." Young adults have a significantly higher proportion of people who answered "never" than the other age groups.[15] This distinction between young adults and the others is understandable because credit reports become relevant to older adults, as they buy homes and use credit cards that are not cosigned by their parents.

---

significantly related to age, neither Scheffe tests nor t-tests show clear patterns of significance between young adults and the rest of the sample or between the youngest adults and each of the older groups.

[15] The comparison between the 18-24 year olds and the rest of the sample was statistically significant at .05 level according a two sample t-test.

## Table 6 – Reading Privacy Policies

| **Do you read the privacy policies of websites ...** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Often* | 14% | 14% | 12% | 16% | 15% | 14% | 15% |
| *Sometimes* | 36% | 37% | 32% | 40% | 34% | 39% | 36% |
| *Hardly ever* | 32% | 31% | 32% | 28% | 37% | 32% | 27% |
| *Never* | 18% | 16% | 24% | 16% | 13% | 14% | 22% |
| *Don't know/refused* | 1% | 1% | 0% | 1% | 0% | 1% | 0% |
| *Total* | 974 | 141 | 207 | 196 | 195 | 149 | 86 |

$x^2$= 21.9, df = 20, $p$ = .349 : Differences not significant

## Table 7 – Erasing Cookies

| **When using the internet, do you erase your cookies . . .** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Often* | 39% | 33% | 36% | 51% | 40% | 39% | 33% |
| *Sometimes* | 24% | 25% | 31% | 19% | 20% | 28% | 16% |
| *Hardly ever* | 17% | 25% | 12% | 18% | 20% | 13% | 13% |
| *Never* | 12% | 14% | 14% | 7% | 12% | 13% | 17% |
| *Not familiar with cookies* | 6% | 4% | 3% | 3% | 5% | 7% | 17% |
| *Don't know/refused* | 3% | 0% | 4% | 3% | 4% | 1% | 5% |
| *Total* | 974 | 139 | 206 | 196 | 195 | 150 | 88 |

$x^2$= 73.7, df = 25, $p$ < .001

## Table 8 – Changing Mind About Purchase

| **Have you ever changed your mind about buying something online because of a privacy or security concern?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *Yes, have* | 56% | 49% | 55% | 66% | 58% | 56% | 41% |
| *No, have not* | 38% | 44% | 39% | 29% | 38% | 39% | 47% |
| *Does not shop online* | 6% | 7% | 6% | 5% | 4% | 5% | 12% |
| *Don't know/refused* | 0% | 0% | 0% | 1% | 1% | 1% | 0% |
| *Total* | 974 | 140 | 207 | 196 | 196 | 150 | 85 |

$x^2$= 27.7, df = 15, $p$ < .05

**Table 9 – Checked Credit Report**

| In general, how often do you check your credit report? | Overall | 18-24 | 25-34 | 35-44 | 45-54 | 55-64 | 65 + |
|---|---|---|---|---|---|---|---|
| *At least once a month* | 10% | 14% | 9% | 12% | 5% | 9% | 9% |
| *Every few months (quarterly)* | 18% | 13% | 19% | 17% | 17% | 22% | 17% |
| *About once a year* | 34% | 16% | 40% | 39% | 40% | 33% | 31% |
| *Less often than once a year* | 18% | 5% | 17% | 24% | 21% | 21% | 20% |
| *Never* | 19% | 48% | 14% | 8% | 17% | 15% | 21% |
| *Don't know/refused* | 1% | 4% | 1% | 1% | 1% | 1% | 1% |
| *Total* | 972 | 139 | 206 | 197 | 194 | 150 | 86 |

$x^2 = 144.4$, df = 25, $p < .001$

Levels of Concern

The tendencies noted above carry over to levels of privacy concern. We fielded a two-prong question. The first asked the individual whether his or her privacy concern was greater, the same, or less than five years ago; the responses are in Table 10. Answers are significantly associated with age, but the 18-24 group was not significantly different than all older respondents, or any single group. Contributing to the significance in this table is the 65+ group, which is more concerned than the 25-34 year olds ($p < .05$).

The obvious problem with Table 10 is that there is no baseline—we don't know the level of concern at which the person began five years ago. But we pursued the question so we could ask people whose privacy concerns increased to note "the most important reason" for the rise. The responses, in Table 11, reveal no statistically significant association with age or differences between the 18-24 year olds and the other age groups.

**Table 10 – Concern About Privacy Issues**

| **Compared to five years ago, would you say you are more concerned about privacy issues on the internet, less concerned, or that you have the same level of concern?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *More concerned* | 55% | 54% | 44% | 59% | 55% | 60% | 67% |
| *Less concerned* | 6% | 9% | 8% | 5% | 6% | 5% | 4% |
| *Same level* | 38% | 36% | 47% | 36% | 39% | 35% | 29% |
| *Don't know/refused* | 1% | 1% | 2% | 1% | 1% | 0% | 0% |
| *Total* | 974 | 140 | 206 | 196 | 196 | 150 | 86 |

$x^2$= 26.7, df = 15, $p < .05$

**Table 11 – Concern About Privacy Issues – Most Important Reason**

| **Please tell me which one of the following is the most important reason you are more concerned about privacy issues on the internet than you were five years ago.** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *You know more about privacy risks online* | 48% | 42% | 59% | 41% | 51% | 47% | 46% |
| *You have more to lose if your privacy were violated* | 30% | 32% | 23% | 29% | 29% | 32% | 39% |
| *You have had an experience that has changed your mind about privacy* | 17% | 22% | 13% | 23% | 15% | 17% | 12% |
| *Some other reason?* | 3% | 0% | 4% | 6% | 3% | 2% | 4% |
| *Don't know/refused* | 2% | 4% | 0% | 2% | 2% | 2% | 0% |
| *Total* | 532[16] | 74 | 90 | 115 | 107 | 89 | 57 |

$x^2$= 23.0, df = 20, $p$ = .29 : Differences not significant

## Penalties for Information Misuse

One way to judge a person's concern about privacy laws is to ask about the penalties that companies or individuals should pay for breaching them. We asked respondents one question related to the monetary penalties a firm should pay and another regarding what should happen to executives involved in illegal privacy breaches. As seen in Tables 12 and 13, the two tendencies we have seen throughout can be found here. Table 12 shows a clear majority of 18-24 year olds selecting the highest dollar amount of punishment offered (more than $2,500), though a t-test demonstrates that they were

[16] N is small because only people who answered "more concerned" in the previous question were asked this question.

significantly less likely to choose that amount than the rest of the population ($p < .001$), and more likely to select $1,000 ($p < .05$).

In Table 13, around half of the sample chose the harshest penalties for the companies or individuals—being put out of business and facing jail time, while a third or more thought the company should fund efforts to protect privacy. Though answers to this question are associated with age, 18-24 year olds differed[17] significantly from all other age groups only in selecting "The company should not be punished in any of those ways" ($p < .01$).

**Table 12 – Illegal Use of Personal Information**

| **If a company purchases or uses someone's personal information illegally, about how much—if anything—do you think that company should be fined?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *$100* | 2% | 3% | 3% | 1% | 1% | 1% | 2% |
| *$500* | 4% | 5% | 5% | 5% | 5% | 1% | 3% |
| *$1,000* | 9% | 14% | 10% | 10% | 8% | 7% | 6% |
| *$2,500* | 7% | 11% | 9% | 6% | 7% | 3% | 5% |
| *More than $2,500* | 69% | 54% | 63% | 68% | 76% | 79% | 77% |
| *It depends* | 4% | 10% | 1% | 5% | 3% | 5% | 2% |
| *Don't know/refused* | 4% | 3% | 8% | 5% | 1% | 5% | 5% |
| *Total* | 979[18] | 141 | 207 | 196 | 196 | 152 | 87 |

$x^2 = 70.8$, df = 35, $p < .001$

**Table 13 – Punishing Companies for Illegal Uses of Information**

| **Beyond a fine, companies that use a person's information illegally might be punished in other ways. Which ONE of the following ways to punish companies do you think is most important?** | **Overall** | **18-24** | **25-34** | **35-44** | **45-54** | **55-64** | **65 +** |
|---|---|---|---|---|---|---|---|
| *The company should be put out of business* | 18% | 16% | 19% | 18% | 14% | 20% | 22% |
| *The company should fund efforts to help people protect privacy* | 38% | 33% | 46% | 33% | 43% | 36% | 31% |
| *Executives who are responsible should face jail time* | 35% | 40% | 29% | 40% | 33% | 34% | 40% |
| *The company should not be punished in any of those ways* | 3% | 7% | 2% | 5% | 2% | 2% | 2% |
| *It depends* | 2% | 0% | 2% | 2% | 2% | 3% | 2% |
| *Don't know/refused* | 4% | 4% | 3% | 3% | 7% | 5% | 2% |
| *Total* | 973 | 139 | 206 | 197 | 195 | 151 | 85 |

$x^2 = 39.0$, df = 25, $p < .05$

[17] 18-24 year olds have a higher percentage choosing the no penalty option.

[18] The slightly inconsistent N is caused by rounding errors as explained in the methods section.

Privacy Knowledge

Do the similarities between young adults and other age groups carry over to knowledge of existing privacy laws? In order to explore this question, we gave the respondents a set of true/false statements to evaluate and answer. (See Table 14.) All of the answers are false. Consistently answering *true* reflects a belief that the law protects an individual's online and offline privacy more than it does in these common circumstances. We read the statements in separate clusters relating to online and offline privacy; within these clusters, we read the statements in random order. To simplify presentation of the findings, we created a composite index tallying the number correct for each age group.

**Table 14 – Online and Offline Privacy Questions**

| **Online Questions** | **Answer** |
|---|---|
| If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission. | False |
| If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government. | False |
| If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so. | False |
| If a website violates its privacy policy, it means that you have the right to sue the website for violating it. | False |
| If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission. | False |
| **Offline Questions** | **Answer** |
| When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission. | False |
| When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission. | False |
| When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission. | False |
| When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission. | False |

As Table 15 indicates, the savvy that many attribute to younger individuals about the online environment doesn't appear to translate to privacy knowledge. The entire population of adult Americans exhibits a high level of online-privacy illiteracy; 75 percent answered only two or fewer questions correctly, with 30 percent getting none right. But the youngest adults perform the worst on these measures: 88 percent answered

only two or fewer correctly, and 42 percent could answer none correctly. A t-test shows that the difference between the average number correct for 18-24 year olds and the other adults—1.12 correct compared to 1.61 for the others—is statistically significant ($p < .001$). When focusing particularly on how these differences play out between young adults and the particular groups, a Scheffe test reveals that the 18-24 year olds were more likely to get none correct than the 25-34 and 35-44 year olds ($p < .05$ in both cases). Young adults were also less likely to get 3-4 correct than the 35-44 and 55-64 groups ($p < .05$ in both cases). In all of these statistically significant cases, a substantially larger percentage of young adults know less about online privacy regulations.

When it came to our offline privacy knowledge questions, the differences between young adults and the other age groups were even more pronounced. Eighty-eight percent of 18-24 year olds answered two or fewer of our offline questions correctly, compared to 74 percent overall. A t-test showed that 18-24 year olds only answered 0.9 correctly compared to 1.8 for the other groups ($p < .001$). Moreover, Scheffe tests note statistical significance compared to each of the other groups. Young adults were more likely to answer no questions correctly than any other age group; conversely, they were less likely to answer 3-4 questions correctly than any other age group.

Getting these questions right is important because it indicates whether the respondents know that privacy laws protect them in common commercial transactions. We found that while young adults tend to be similar to older adults in attitudes, practices, and policy preferences regarding information privacy, they are quite more likely than older adults to be wrong in judging whether the legal environment protects them.

**Table 15 - Online Privacy Knowledge Questions (5 total)**

| Age Range | 0 Correct | 1-2 Correct | 3-4 Correct | 5 Correct |
|---|---|---|---|---|
| 18-24 (N=139) | 42% | 46% | 11% | 1% |
| 25-34 (N=206) | 25% | 58% | 16% | 2% |
| 35-44 (N=197) | 24% | 38% | 30% | 8% |
| 45-54 (N=196) | 26% | 48% | 24% | 3% |
| 55-64 (N=150) | 39% | 32% | 28% | 1% |
| 65 and Older (N=86) | 31% | 43% | 24% | 1% |
| Overall (N=974) | 30% | 45% | 22% | 3% |

$x^2 = 73.1$, df = 15, $p < .001$

**Table 16 - Offline Privacy Knowledge Questions (4 total)**

| Age Range | 0 Correct | 1-2 Correct | 3-4 Correct |
|---|---|---|---|
| 18-24 (N=139) | 50% | 38% | 12% |
| 25-34 (N=206) | 34% | 37% | 29% |
| 35-44 (N=197) | 24% | 33% | 43% |
| 45-54 (N=196) | 26% | 41% | 34% |
| 55-64 (N=150) | 26% | 32% | 42% |
| 65 and Older (N=86) | 27% | 37% | 36% |
| Overall (N=974) | 27% | 35% | 38% |

$x^2 = 69.9$, df = 20, $p < .001$

## Conclusion

In policy circles, it has become almost a cliché to claim that young people do not care about privacy. Certainly there are many troubling anecdotes surrounding young individuals' use of the internet, and of social networking sites in particular. Nevertheless, we found that in large proportions young adults do care about privacy. The data show that they and older adults are more alike on many privacy topics than they are different. We suggest, then, that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.

Public policy agendas should therefore not start with the proposition that young adults do not care about privacy and thus do not need regulations and other safeguards. Rather, policy discussions should acknowledge that the current business environment along with other factors sometimes encourages young adults to release personal data in order to enjoy social inclusion even while in their most rational moments they may espouse more conservative norms. Education may be useful. Although many young adults are exposed to educational programs about the internet, the focus of these programs is on personal safety from online predators and cyberbullying with little emphasis on information security and privacy.[19] Young adults certainly are different from older adults when it comes to knowledge of privacy law. They are more likely to believe that the law protects them both online and off. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner.

But education alone is probably not enough for young adults to reach aspirational levels of privacy. They likely need multiple forms of help from various quarters of society, including perhaps the regulatory arena, to cope with the complex online currents that aim to contradict their best privacy instincts.

[19] "Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force." The Berkman Center for Internet & Society, December 31, 2008. Available at: http://cyber.law.harvard.edu/pubrelease/isttf/

**BEFORE THE PUBLIC UTILITIES COMMISSION OF THE**

**STATE OF CALIFORNIA**

| | |
|---|---|
| Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System | Rulemaking 08-12-009 (Filed December 18, 2008) |

# JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

JENNIFER LYNCH, Attorney[1]
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

Dated: March 9, 2010

[1] Berkeley Law students Jonas Herrell, David Marty, and Shane Witnov, along with School of Information Masters Candidate, Longhao Wang, participated in the drafting of these comments.

**BEFORE THE PUBLIC UTILITIES COMMISSION OF THE**

**STATE OF CALIFORNIA**

| | |
|---|---|
| Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System | Rulemaking 08-12-009 (Filed December 18, 2008) |

# JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

## I. Introduction

The Center for Democracy & Technology ("CDT") and the Electronic Frontier Foundation ("EFF") file these joint comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010 ("Joint Ruling"). CDT and EFF thank the Commission for the opportunity to submit comments discussing these important questions and commend the Commission's initiative on the matters to date.

The Center for Democracy & Technology is a non-profit, public interest organization with broad experience and expertise in matters of consumer privacy and emerging technologies. CDT has offices in Washington, DC and San Francisco, California. EFF is a non-profit member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology.

In addressing the issues raised by the Joint Ruling, we recommend the following:

- Privacy concerns raised by data collection within the Smart Grid require regulatory action on the part of the Commission. (*See Section II)*
- The Commission's authority to regulate consumer privacy and data access issues on the Smart Grid is derived from the California Constitution, Senate Bill 17, and the Commission's past decisions. (*See Section III*)
- The Commission should define the scope of customer energy data that warrants privacy protection. (*See Section IV)*
- The Commission should adopt privacy and security principles based on the Fair Information Practice principles (FIPs) to ensure that Smart Grid proposals will provide the privacy protections required by state and federal law. (*See Section V*)
- To fulfill the requirements of Senate Bill 17, the Commission should require utilities to employ Fair Information Practice principles as part of their Smart Grid deployment plans. (*See Section VI*)
- The Commission should consider and adopt our recommended modification to the Proposed Access Rule, as provided in our Appendix A. (*See Section VII*)
- The Commission should include privacy-related quantitative metrics for Smart Grid implementations. (*See Section VIII*)
- The Commission should not wait for privacy standards from the national standard setting bodies, and should adopt the Fair Information Practice principles now. (*See Section IX*)

We hope that our comments and recommendations here will both advance the Commission's understanding of the important privacy interests that are at stake in these proceedings and provide useful guidance to the Commission as it seeks compliance with the requirements and mandates of State Senate Bill 17, the Federal Energy Independence and Security Act of 2007, and the California Constitution.

## II. Privacy Concerns Raised By Data Collection within the Smart Grid Require Regulatory Action on the Part of the Commission

### A. Data Flows Enabled by Smart Grid Technology Represent a Profound Shift in the Customer-to-Utility Relationship

The Smart Grid promises great benefits to consumers and the environment, including lowered energy costs, increased usage of environmentally friendly power sources, and enhanced security against attack and outage. At the same time, however, the Smart Grid presents new privacy threats through its enhanced collection and transmission of detailed consumption data – data that can reveal intimate details about activities within the home and that can easily be transmitted from one party to another. The following aspects of these expanded data flows represent a profound shift from the traditional customer-to-utility relationship:

> **(1) Granularity of Usage Information:** The Smart Grid entails collection of much more detailed data about consumer energy consumption than previous technologies allowed. Whereas historically a consumer's consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new systems will collect and record this data at much shorter time intervals—down to real-time or near real-time intervals. The emergence of increasingly sophisticated metering technologies is enabling the unprecedented collection of energy consumption data—from 750 to 3,000 (or more) data points a month— and will reveal variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.[2]
>
> **(2) New Types of Information:** Smart Grid technologies collect a much greater variety of information than has been collected by conventional energy services. In addition to detailed energy consumption data, utilities may collect distributed generation data, unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles, just to name a few. And this is only the raw data. With this data in

[2] Jack I. Lerner & Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3. 3 (2008).

hand, it becomes trivial to infer presence and absence in the home, sleep schedules, and other highly personal routines.[3]

**(3) Third Party Incentives and Access:** The sheer volume of granular data provided by Smart Grid technologies, combined with its revealing nature, will make it highly attractive to a number of parties other than the utilities themselves, including marketers, law enforcement or other government actors, civil litigants, and criminals,[4] The attraction for marketers, for example, has already created an emerging market in consumer energy data. Within the new Smart Grid, third-party, non-utility operations will have unprecedented incentives to gain access to customer data. Beyond direct access to data held at utilities, third parties will seek to use utilities as conduits for customer information or will market devices that pull customer data directly from within the home, bypassing the utility's equipment.

The challenge for the Commission is to develop rules that both protect the consumer against misuse of this data and empower the consumer to access this data, use it and share it with entities other than the utility as they offer new and useful services to consumers.

### B. New Technologies and Services Create Attendant Privacy Risks

New energy services that allow consumers access to their own detailed usage data present potential benefits in terms of energy efficiency and reliability. Yet these services will allow entities other than utilities to receive consumer energy consumption data and use it in new ways. This profound shift in the data flow away from the traditional consumer-to-utility relationship challenges key assumptions underlying existing privacy laws and regulations.

Further, the emergence of increasingly sophisticated metering technologies, which enable the unprecedented collection of energy consumption data, will remove a "latent structural limitation" that previously protected the revelation of intimate details about household activities.[5]

---

[3] Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at 11-20.
[4] *See* § II.B, *infra*.
[5] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605, 1626 (2007) (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints.").

For example, new non-intrusive appliance load monitoring ("NALM") techniques make it easy to reconstruct information about energy consumption of individual appliances from a household's aggregate smart meter data,[6] and researchers have already compiled libraries of appliance load signatures.[7] Research shows that analyzing fifteen-minute interval aggregate household energy usage data can by itself pinpoint the use of most major home appliances.[8] As the time intervals between data collection points decrease, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.[9]

Activities that might be revealed through analysis of home appliance use data include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, presence or absence of persons in the home, and activities that might seem to signal illegal, or simply unorthodox, behavior.[10] As a result, information collected by the Smart Grid becomes highly valuable for many purposes other than energy efficiency, most prominently: commercial exploitation by advertisers and marketers, household surveillance by law enforcement, and access by criminals attempting to break into homes or commit identity theft.

### 1. Commercial Interests in Acquiring Customer Energy Data Create Privacy Risks

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be used for purposes especially contrary to consumer interests and expectations. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral

---

[6] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies* app. A at A-1 (2009), *available at* http://ssrn.com/abstract=1462285.

[7] *Id*. at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.

[8] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731.

[9] California utilities are already deploying smart meters that are capable of taking usage readings every five seconds. *See* Calif. Energy Comm'n, CEC-400-2008-027-CT, *Proposed Load Management Standards* 25 (Draft Comm. Report, 2008), *available at* http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF.

[10] Lerner & Mulligan, *supra* note 2.

targeting products might wish to enhance existing customer profiles with energy usage data that reveals customer activities and habits, following a recent trend in the merging of online and offline data sources to enhance targeted third-party advertising.[11]

### 2. Government Agency Incentives to Acquire Customer Energy Data Create Privacy Risks

The detailed and revealing nature of Smart Grid data also will be valuable for surveillance by government agencies. For example, law enforcement agencies already use electricity consumption data. In *Kyllo v. United States*,[12] the government relied on electrical utility records to develop its case against a suspected marijuana grower.[13] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.[14] In 2004, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household.[15] In 2000, the California Narcotic Officers' Association unsuccessfully attempted to get the Commission to overturn its previously ruling that utilities only provide customer data to law enforcement with proper legal service.[16]

As Smart Grid technologies continue to collect ever more finely-grained data about household habits, law enforcement officials will become even more interested in accessing that data to develop cases. In investigating crimes, for example, agencies may want to establish or confirm presence at an address at a certain critical time; this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat.

---

[11] For more about recent trends in data aggregation and the development of enhanced customer profiles for advertising purposes, see CDT, *CDT's Guide to Behavioral Advertising*, http://cdt.org/privacy/targeting/.
[12] 533 U.S. 27 (2001).
[13] *Id*. at 30.
[14] *United States v. Kyllo*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).
[15] Jo Moreland, *Drug Raid Has Carlsbad Family Seeing Red*, N. County Times, Mar. 25, 2004, *available at* http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html.
[16] D.01-07-032 at 1.

While Smart Grid data certainly may be useful for these purposes, the privacy implications of law enforcement access, especially in the traditionally protected area of the home, call for strong, constitutionally adequate protections for this information, careful procedures on the part of utilities and others with access to this data, and technology design that allows for strong data protection.

### 3. Civil Litigants' Incentives to Acquire Customer Energy Data Create Privacy Risks

Civil litigants may also place a high value on detailed energy usage data. For instance, an insurance company contesting a homeowner's claim might seek access to the homeowner's energy data to disprove that he actually owned the specific appliances he claimed. Similarly, in a custody proceeding, a spouse may seek energy data to show the other spouse took the children out of the state for two days without proper consent. In both cases, the detailed usage data would certainly be relevant to proving or disproving the contested fact. As with access by government agencies, effective procedural protections should be required, as should careful procedures for managing civil requests on the part of utilities and other providers. These include first requiring litigants to seek data from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way to obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information, and the entity should provide energy customers with notice and an opportunity to object before disclosing data.

### 4. Criminal Incentives to Acquire Customer Energy Data Create Privacy Risks

Criminals might also seek access to smart meter data or other information collected by the Smart Grid, in hopes of using this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future crimes. The information could also be used by criminals to commit identity theft, especially if utilities or other providers use unsecured paths to transmit data. For instance, many utilities use energy

consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account.[17] Failing to encrypt data transmission within the Smart Grid compounds these threats to customer data security.

### C. Current Privacy Legal Frameworks Offer Some Protections for Energy Data But Are Insufficient to Fully Protect Data in the Smart Grid

The significant privacy risks to consumers, described above, are compounded by the dearth of clear rules that apply to the new technology landscape. As the National Institute of Standards and Technology (NIST) noted in its First Draft NISTIR 7628, there remains a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use," creating "a privacy risk that needs to be addressed."[18]

In this proceeding, the Commission has been presented with the important opportunity and responsibility[19] to develop privacy protections for California citizens' energy data. Both the California and Federal Constitutions, as well as various regulatory decisions and provisions, provide some protections for energy data, but these protections were not designed to cover the unprecedented volume of data, nor varieties of new data, that the Smart Grid will make available about household activities. As such, these protections need to be supplemented to ensure that Californians can continue to enjoy the level of privacy they expect and are entitled to in their homes.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on disclosure of consumer energy data.[20] Generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data, putting California in a leadership position.[21] Because the

---

[17] For instance, San Diego Gas and Electric (SDGE) uses the amount of the last SDGE bill to authenticate its customers when the customers sign up for an online account. *See* SDGE*, My Account*, https://myaccount.sdge.com/myAccountUserManager/pageflows/usermanager/Registration/begin.do.

[18] Nat'l Inst. of Standards & Tech., *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements* (2009), *available at* http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf.

[19] *See, e.g.*, D.09-12-046 at 26 (finding that the Commission should create rules about privacy and security to protect customers); D.90-12-121 at 11 (holding that utilities can only provide data to law enforcement pursuant to legal process).

[20] Quinn, *supra* note 6, at 24.

[21] For example, the National Association of Regulatory Utility Commissioners (NARUC) will consider a resolution in 2010 that would encourage member states to support several regulatory protections on consumer data collected in

existing laws alone do not provide adequate protection for the categories and quantities of data that the Smart Grid will generate, the Commission should use its regulatory authority to ensure that the Smart Grid does not undermine the privacy protections guaranteed to California citizens.

Specifically, as we describe in later sections, the Commission should (1) define the scope of customer energy data that warrants privacy protection, (2) broadly adopt cyber security and privacy principles to ensure that smart grid proposals will provide sufficient privacy protections, (3) require utilities to employ Fair Information Practice principles (FIPs) as part of Smart Grid deployment plans, (4) provide additional privacy protections in the Proposed Access Rule, (5) request privacy-related quantitative metrics from utilities in smart grid implementations, and finally, (6) the Commission should not wait for privacy standards from the national standard-setting bodies, but should adopt FIPs immediately.

## III. The Commission's Authority to Regulate Consumer Privacy and Data Access Issues on the Smart Grid Is Derived from the California Constitution, Senate Bill 17 and the Commission's Past Decisions

The Commission stated its policy objective in D.09-12-046 to "[e]nsure all information is secure and that a customer's privacy is protected."[22] It further stated it would require utilities put in place "sufficient privacy and security measures . . . to mitigate the potential for fraud and hacking" and that "access to usage data must be provided consistent with the rules [the Commission] adopt[s] to ensure that access is provided consistent with EISA, the general public interest, and state privacy rules."[23]

The California Constitution's privacy provision,[24] along with Senate Bill 17,[25] support these goals and provide the Commission with broad authority to adopt rules and protocols designed to protect and preserve consumer privacy rights. We discuss these and additional grounds for the Commission's authority in this section.

---

the Smart Grid. *See* NARUC, *Draft Resolutions Proposed for Consideration at the 2009 Annual Convention of NARUC* 14-17 (2009), *available at* http://annual.narucmeetings.org/09_1106_Proposed_Resolutions.pdf; *see also* Nat'l Inst. of Standards & Tech., *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, at 84 (2009), *available at* http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf.

[22] D.09-12-046.

[23] *Id.*

[24] Cal. Const. art. I, § 1.

[25] Specifically Cal. Pub. Util. Code §§ 8360(i), (j).

In *White v. Davis*[26] the California Supreme Court explained that "the moving force" behind California's constitutional right to privacy "was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society," and that its "primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."[27]

Importantly, our state constitutional privacy right protects Californians against private businesses as well as the government. As the *White* court put it, the right "prevents government and business interests from collecting and stockpiling unnecessary information about us," partly because "[t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives."[28] Thus, among the "principal 'mischiefs'" targeted by the constitutional right are "the overbroad collection and retention of unnecessary personal information by government and business interests" and "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party."[29]

The Commission has recognized its constitutional obligations to protect privacy in past decisions. When confronted with the consumer privacy concerns presented by telephone monitoring technologies, in Decision No. 88232, the Commission unequivocally stated that, "[o]ur constitutional responsibilities and those of the utilities we regulate, are paramount. . . ."[30] In *The Matter of the Application of Pacific Bell,* when confronted with the consumer privacy concerns presented by Pacific Bell's default installation of caller identification technology, the Commission drew upon its constitutionally granted authorities and rightly refused to allow commercial expediency to take precedent over the rights of California citizens. It stated:

> If the service is to be offered consistently with constitutional guarantees and the public interest, it must be offered in a way that maximizes the ease and freedom with which California citizens may choose not to disclose their calling party numbers. We will not compromise an individual's free exercise of his or her right of privacy in order to place in the hands of the Caller ID subscriber a more valuable mailing list, a marginally better

[26] *White v. Davis*, 13 Cal.3d 757 (1975).
[27] *Id*. at 774.
[28] *Id*.
[29] *Id*. at 775.
[30] *In re PT&T Co.*, 83 C.P.U.C. 149 (1977).

> method of screening or managing telephone calls, or even a slightly more effective deterrent to unlawful or abusive uses of the telephone.[31]

Smart Grid technology poses far greater, yet far less visible, threats to consumer privacy than Caller ID. Unlike Caller ID, which only transmits the caller's phone number, Smart Grid technologies can reveal minute details about the lives in a household. This suggests even greater reason for the Commission to address these issues. Further, these precedents strongly support interpreting the Commission's constitutional obligations to include protecting consumers from the full range of privacy threats.

California State Senate Bill 17 (Padilla), which added sections 8360 through 8369 to the California Public Utility Code, also provides the requisite authority to protect consumer privacy. Specifically, section 8360(i) requires that the Commission "[d]evelop standards for communication and interoperability of appliances and equipment connected to the electric grid."[32] The Commission is empowered to regulate the privacy and security of consumer energy data because such privacy and security are critical aspects of any "standards for communication." Likewise in section 8360(j), the legislature has tasked the Commission with "[i]dentifying and lowering [ ] unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services." Because customers will be dissuaded from adopting Smart Grid technologies unless the risk to privacy posed by such technologies is addressed, the Commission can and should use its authority under section 8360 to create consumer privacy protections, thus lowering resistance to adoption.

## IV. The Commission Should Define the Scope of Customer Data that Warrants Privacy Protection

Designing an effective framework to protect customer data requires a specific articulation of what information requires protection. We recommend that the Commission adopt a robust and expanded interpretation of the term "customer information" to account for the new types of information on the Smart Grid. The Commission should then act to regulate the collection, use, and dissemination of that customer information as we describe in subsequent sections.

[31] *In re Pacific Bell*, 44 C.P.U.C.2d 694 (1992).
[32] Cal. Pub. Util. Code § 8360(i).

The California Public Utility Code currently describes "customer information" in section 394.4 as including "customer specific billing, credit, or usage information."[33] This section importantly requires Electric Service Providers to treat such information as confidential unless the customer consents otherwise in writing.[34] Affiliate Transaction Rule IV.A similarly articulates the confidentiality requirement that attaches to customer information, in this case, when the information is in the hands of the utilities.[35] The rule provides that: a "utility shall provide customer information to its affiliates and unaffiliated entities on a strictly non-discriminatory basis, and *only with prior affirmative customer written consent.*[36]

"Customer information" should be construed to cover the broad set of intimate information that is now collectable within the Smart Grid and should apply to all entities collecting, storing or transmitting customer data. We suggest that, beyond its current denotation, the term be expressly interpreted to include all usage data and device data capable of revealing either personally identifiable information or household-identifiable information.[37] Specifically, the Commission should expressly interpret the meaning of "customer information" to include:

> (1) *traditional personally identifiable information* (PII), such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information;
>
> (2) *data collected about an individual household* in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of data include, without limitation: granular usage data from individual households, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering and device data (e.g. thermostat temperature); and

[33] *See* Cal. Pub. Util. Code § 394.4(a) ("Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information.").
[34] *See id.*
[35] D.97-12-088, app. A, Rule IV.A, *rev'd by* D.98-08-035, *amended by* D.98-12-075.
[36] *Id.* (emphasis added).
[37] This distinction between personal identifiability and household identifiability is intended to emphasize the importance of protecting the privacy of households, in addition to the privacy of individual persons. We focus here on protections that the home and household deserve, but we note that the energy usage data of organizations such as churches, political associations, and medical offices may warrant similarly strong protections.

(3) *energy usage data collected from the home by entities without the permission or intervention of the utility*, to the extent that the authority of the Commission covers such entities.

Sometimes information in the second category will be personally identifiable when combined with other types of information or when the number of people in a household is small. Regardless of whether it is individually identifiable, however, household-identifiable information is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. It can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising serious privacy issues. Further, given that 32.2 million people live alone in the U.S. and twenty eight percent of American households have single-person occupancy,[38] household-identifiable information is functionally equivalent to "personally identifiable information" for a significant number of consumers.

The principles discussed here for customer information outline the minimum protections required for this basic category of data. Some of the information included within the customer information, such as PII and location-identifying information, will require additional protections.

## V. The Commission Should Adopt Privacy and Security Principles Based on the Fair Information Practice Principles (FIPs) to Ensure that Smart Grid Proposals Will Provide the Privacy Protections Required by State and Federal Law

In section 5.5 of the Joint Ruling, the Commission asks broadly what cyber security and privacy principles Smart Grid proposals should meet.[39] As has also been discussed at length elsewhere,[40] the privacy issues associated with home energy usage data can and should be addressed through robust application of the full set of FIPs. We strongly urge the Commission to use the FIPs as a general overarching framework to guide the privacy principles and rules it adopts. These principles reflect international guidelines, and go beyond the currently dominant—

[38] U.S. Census Bureau, *Facts for Features: Unmarried and Single Americans Week*, July 21, 2009, http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/014004.html.
[39] *Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid* 33-39 (Feb. 8, 2010) [hereinafter "Feb. Joint Ruling"].
[40] *See* CDT, *Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security and Requirements, National Institute of Standards and Technology* (2009) *available at* http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf.

and discredited[41]—model of "notice and choice." The FIPs have been used for information management since 1973 and provide a well-tested framework for balancing and harmonizing privacy concerns with other interests. They have gained broad acceptance by national and international privacy regulators and have been applied in many contexts related to consumer privacy. The FIPs are well-aligned with the requirements of SB 17. Properly formulated and rigorously implemented, the FIPs provide a broad, comprehensive privacy framework that should underlie all privacy principles for Smart Grid deployment. Adopting FIPs as a framework is an essential part of protecting consumer privacy and ensuring that the Smart Grid maximizes "benefit to ratepayers"[42] by creating a system that carefully weighs the tradeoffs between disclosure and privacy protection.

### A. The Fair Information Practice Principles

The Commission should adopt the FIPs framework because it provides a complete system for considering privacy and consumer security issues. We rely here on the articulation of the FIPs recently adopted by the US Department of Homeland Security,[43] on the belief that a framework developed for information systems affecting the national security is also well-suited to the issues posed by the Smart Grid. The DHS framework includes the following eight principles: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing. These principles are described at length in this section and referred to extensively throughout our recommendations in the sections that follow.

1. **Transparency:** Data management practices should be transparent and should provide meaningful, clear, full notice to the consumer regarding the collection, use, dissemination, and maintenance of customer information.

An entity that handles customer information must make comprehensive and accurate disclosures to customers about the collection, use, dissemination and maintenance of customer

[41] For example, National Telecommunications and Information Administration Associate Director for Domestic Policy Daniel J. Weitzner recently stated "[t]here are essentially no defenders anymore of the pure notice-and-choice model." *See* Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. Times, Feb. 28, 2010, *at* Bus. 4, http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html (quoting Mr. Weitzner).
[42] SB 17.
[43] *See*, U.S. Dept. of Homeland Sec., *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

information. This disclosure must be made to the consumer prior to any collection. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. Further, Smart Grid entities, including utilities, should also provide consumers with access to the personally identifying information collected about them, as well as all usage data collected about their homes. This principle aligns closely with section 8360(h), which requires that consumers be provided with "timely information and control options."[44] This principle is also essential to the successful implementation of many of the following principles, especially Individual Participation and Accountability and Auditing.

2. **Individual Participation:** Regulable entities should involve the individual in the process when they use customer information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of customer information.

New smart meters create the need for regulable entities to give customers a choice about the types of customer information collected and its use, transfer, and maintenance, including retention. To fully recognize the principle of individual participation, regulable entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Under the Public Utilities Code, customer information, including usage information, is confidential.[45] To protect consumer privacy, regulable entities should be required to get affirmative written customer consent prior to the collection and use of customer information for any secondary purposes beyond what is strictly required for the provision of service. Consumers implicitly agree to the minimum data disclosures required for utilities to provide energy generation and billing. However, any other uses that are not strictly necessary require affirmative consent. For example, affirmative written consent would be required for a utility to

[44] Cal. Pub. Util. Code § 8360(h).
[45] *Id.* § 394.4(a).

use customer information for delivering advertisements to its customers because it is not strictly necessary to the primary purpose of providing energy service.

3. **Purpose Specification:** Regulable entities should specifically articulate the purpose or purposes for which customer information will be used.

Regulable entities should provide consumers with information about how the entity will use their data *before* the time of collection. The specification of purpose should fully describe the purposes for which the data being collected will be used. These will likely include uses of customer energy data necessary for core entity operations and services, such as efficient and reliable delivery of electricity, demand response, and billing. To the extent that utilities plan to use data for purposes not strictly necessary to the performance of core operations and services, such as marketing, customers should also have sufficient opportunity to separately and expressly consent to such uses.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that "customer information" will be used for the purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. If a utility plans to share customer information with any third-party service providers, the utility must disclose that fact along with all uses for which the third-party will use the data. If the utility later wishes to change the purpose for which the customer information is used, the utility must first notify consumers and give them the choice whether to consent to that new use.

4. **Data Minimization:** Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as necessary to fulfill the specified purpose.

Generally, Smart Grid standards should support, and technologies should be capable of, appropriate data minimization. The Data Minimization principle dictates that regulable entities may only collect and maintain customer data necessary for the performance of specified purposes, as defined above.[46] Unnecessary information should not be collected; as soon as collected information becomes unnecessary for a stated purpose, it should be deleted.[47]

[46] *See supra* § V.A.3.

[47] OpenADR is an example of a technology that can contribute to data minimization by significantly reducing data collection while still enabling demand response functionality. Demand Response Research Ctr., CEC-500-2009-

In addition to supporting consumers' privacy interests, data minimization is an important part of Smart Grid cyber security, which the Commission is responsible for overseeing under section 8360(b) of SB 17, and also is important to protecting customer safety as required by section 8363.[48] As previously discussed, energy data could be used for many unauthorized and sometimes malicious purposes.[49] Minimizing data collection is a powerful tool for protecting against these security and privacy threats: if the data does not exist, it cannot be compromised. Therefore, adequate minimization requirements for the data that regulable entities collect and keep will address security and privacy concerns, while leaving untouched the data that entities need to fulfill their core operations.

The initial technical architecture that regulable entities adopt to implement the Smart Grid can have a substantial impact on the long-term scope of their data collection practices. For example, collecting and aggregating usage data at the meter level (or household level) could help protect consumer privacy through data minimization. Smart meters deployed in California are already furnished with memory and processing power. The current smart meters could compute electricity bills based on time-of-use pricing, and only periodically transmit aggregate usage and billing information back to the utility, at user defined time spans such as weekly or monthly. These changes would not affect the accuracy of billing or reveal the consumer's consumption data on a granular level to the utility. Yet, all smart meters are not equally smart. When a utility installs smart meters that do not have aggregation capabilities, consumers lose their ability to choose what level of data the utility can see. Consequently, they may surrender more data than the utility actually needs.

Consumers should be provided with tools to aggregate their energy usage data at the meter level before the data is sent along. Consumers should be able to decide the frequency of aggregated smart meter data reported to regulable entities. This requirement is easily implemented because smart meters can be remotely updated, which is all that is required to implement this aggregation function. Provide consumers with tools to decide the time intervals

---

063, *CEC OpenADR-Version 1.0 Report* 1 (Pier Final Project Report, 2009) *available at* http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf (last visited Mar. 9, 2010).

[48] Cal. Pub. Util. Code §§ 8360, 8363.

[49] *See supra* § II.B.

of smart meter reading reported enables households to fully participate in the decision to share their customer information outside of the home.[50]

Residential energy management systems also can minimize data collection by regulable entities. Instead of registering individual smart devices with utilities, consumers could use residential energy management systems, under their control, to manage their devices.[51] In this architecture, smart devices only register with consumers' own residential energy management systems and are invisible to the utilities and other regulable entities who communicate directly with the residential energy management system.[52] Residential energy management systems are being actively developed by commercial entities[53] as well as researchers at University of California.[54]

Importantly, it is presently unclear whether utilities need to collect information about the functioning of individual appliances, or even individual houses, in order to implement effective load management or demand response programs. For many purposes and programs, such detailed data should not be necessary. Given the privacy interests in household-level usage data, the collection and use of it should be subject to scrutiny. Because entities seeking to collect this type of data are in the best position to demonstrate why it is needed, these entities should bear the burden of proving the need for granular customer information, and should be required to show why it is necessary for specific purposes.

The Commission should also apply the Data Minimization principle to regulable entities' data retention practices and should consider revising the current retention periods for customer records, which widely reflect the industry standard of seven years.[55] Although regulable entities may need to retain some data like billing records and load research data for longer periods of time, they should be required to destroy unrelated or unnecessary data. For example, for billing

---

[50] Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed, *supra*, § II.C.

[51] S. Cal. Edison, *SmartConnect Use Case: C6 - Customer Uses an Energy Management System (EMS) or In-Home Display (IHD)*, at 18 (2009), *available at* http://www.sce.com/NR/rdonlyres/C39473B2-50BF-48C6-BAC7-4904DEE0D51F/0/C6_Use_Case_090105.pdf.

[52] *Id.*

[53] Press Release, Tendril, Tendril Achieves First Open ADR Compliant Platform (Jan. 29, 2009) *available at* http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/.

[54] David Auslander & Daniel Arnold, Reference Design for Residential Energy Gateway, http://mechatronics.berkeley.edu/gateway.htm (last visited Mar. 9, 2009).

[55] *See* P.S. Subrahamanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, & Jack Lerner, CyberKnowledge & Univ. of Cal. at Berkeley, *Network Security Architecture for Demand Response/Sensor Networks* 87 (2006), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf.

purposes the utility may need monthly totals of energy consumption; however it would not need to keep the intermediate granular measurements of consumption and load. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to regulable entities in terms of decreased storage and maintenance costs.[56] Monthly totals are less revealing and serve an important record-keeping purpose and can thus justifiably be retained for longer than near-real-time consumption information.

5. **Use Limitation:** Customer information should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected.

Where regulable entities collect customer information for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the entity to departments with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an affirmative consent regime, as introduced above.[57] For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a regulable entity or third party service provider, unless such use was specified to the consumer, who specifically and affirmatively consented to the use. Similarly, the entity should not share customer information or use it for behavioral advertising or other marketing purposes on behalf of a third party without explicit written authorization from the consumer. The Commission should require regulable entities to explain how they implement these use limitations.

6. **Data Quality and Integrity:** Regulable entities should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Regulable entities should provide consumers with tools to correct mistakes or challenge information provided in profiles.

Consumers need to be able to review and, where necessary, correct their information. This is required by section 8360(h), which states that customers must be provided information

[56] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), http://epic.org/reports/dmfprivacy.html.
[57] *See supra* § V.A.2

and control options.[58] To comply with this requirement, the Commission should require regulable entities implement standards and technical requirements that will allow for easily-accessible interfaces that give consumers the opportunity to review and correct their customer information. Such review provides the best means of ensuring that consumer data is accurate.

7. **Data Security:** Regulable entities must protect customer information through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards.

Reasonable security in the Smart Grid requires that any transmission of customer information must be secure and that regulable entities' data practices include meaningful safeguards for customer information. For example, encryption should be required for all communications that are sent over open wireless protocols or that could otherwise reasonably be intercepted on organization-owned infrastructure and third-party communication services. More broadly, the Commission should review technical standards for implementation and, if necessary, revise them to require that smart device communications provided by regulable entities be truly secure.

Further, customer information collected, used and maintained by regulable entities must be stored securely, made available only to those with a documented and authorized need for the information, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of customer information, the regulable entity should be required to notify affected customers and take all reasonable steps to minimize harm to customers.

8. **Accountability and Auditing:** Regulable entities should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use customer information and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements.

The Commission should require regulable entities to have regular privacy training and ongoing awareness activities. Systems storing customer information should have access logs to document who is accessing private data. The Commission should require regulable entities to

[58] *See* Cal. Pub. Util. Code § 8360(h).

conduct regular audits of these logs to ensure that access is in compliance with appropriate and disclosed uses of the data. The Commission should further require rigorous reporting and auditing requirements that examine regulable entities' compliance and adoption of each of these privacy principles. Without a robust accountability and auditing mechanism, there will be no way for the Commission to ensure compliance with the various privacy commitments utilities make in their Smart Grid deployment plans.

### B. The Principle of "Data Ownership" Alone Will Not Create Sufficient Privacy Protections for Consumers and Must Be Supplemented with the Fair Information Practice Principles

Consumer data ownership rules are often discussed as potential solution to privacy concerns. Although we generally support consumer ownership of data (assigning data ownership to utilities would turn them into information gatekeepers and could impede realization of both privacy and innovation policy goals), consumer ownership, alone, rarely solves privacy and security issues. Data ownership without attendant and real control over data can leave consumers with the limited ability to choose between alienating their data or not. Utilities and other third parties may require consumers to surrender control, if not ownership of customer information as part of service agreements and conditions of service. Instead, consumers need ongoing rights in their data—regardless of where it is stored and by whom it is held—complimented by assurances that those to whom they entrust it are bound by clear rules requiring them to abide by consumers' decisions. Such a framework respects the ongoing implications such data has for the consumer's privacy and safety.

The FIPs provide this broader privacy framework. FIPs do not require a specific data ownership regime, but are compatible with and complimentary to consumer data ownership. In particular the Transparency and Purpose Specification principles, discussed above in this section, ensure the data owner can make informed decisions about authorizing uses of data. The requirements of Data Quality and Integrity help the consumer maintain control over his data even when it is held by another party.

We encourage the Commission to recognize a consumer's ownership interest in customer information. However, to provide meaningful protections, the Commission needs to issue regulations that give consumers real control over their data even when it is held by third parties. The Fair Information Practice principles should provide the framework for the protections

necessary to ensure that utilities cannot force or induce consumers to contract away all their rights in their data, depriving them of any privacy protections.

### C. Security and Privacy Principles Adopted by the Commission Should Specifically Require Data Breach Notification

Data breach notification is an important privacy practice implicated by the FIPs Data Security Principle. It warrants further elaboration and special attention by the Commission. California's Data Breach Notification Law, section 1789.29 of the Civil Code, made California a leader in data breach notification by requiring entities to report any breach in security to a system that contains personally identifiable information to all impacted individuals.[59] Forty-four other states have followed California's lead in this matter.[60]

We urge the Commission to keep California in the forefront of data breach notification by applying the requirements of section 1789.29 to regulable entities as part of their Smart Grid proposals. They should be required to report any breach of security in customer information to all impacted consumers and to the Commission.

Data breach notification rules will provide additional incentives for regulable entities to develop strong privacy and security standards. The cost and embarrassment resulting from breach notification can be a strong motivator. Further, by providing consumers' notice of data breaches, they can take appropriate measures to protect themselves from identity theft and other possible crimes. These notifications can also help the public and the Commission to evaluate regulable entities' security efforts.

## VI. To Fulfill the Requirements of Senate Bill 17, the Commission Should Require Utilities to Employ Fair Information Practice Principles as Part of Utility Smart Grid Deployment Plans

The Commission has been tasked with determining the requirements for a Smart Grid deployment plan, which will guide the utilities in the development of their individual deployment plans.[61] It has asked for comments on the topics that should be addressed by the utilities'

[59] Cal. Civ. Code §§ 1798.29, 1798.82.
[60] Perkins Coie, *Security Breach Notification Chart* 134-35 (2008), *available at* http://www.digestiblelaw.com/files/upload/securitybreach.pdf (listing the effective dates for all forty-five states, plus Puerto Rico, that have enacted data breach notification laws).
[61] Feb. Joint Ruling, *supra* note 39, at 3.

plans.[62] It has also sought comment upon the proper evaluation and use of those deployment plans by the Commission.[63] We address both of these questions here.

In section V above, we have urged the Commission to adopt FIPs as a framework for ensuring privacy protections on the Smart Grid. Here, we specifically urge the Commission to incorporate the FIPs as requirements within the Smart Grid deployment plans. Specifically, utilities' deployment plans should take into account each of the following: (1) Transparency; (2) Individual Participation; (3) Purpose Specification; (4) Data Minimization; (5) Use Limitation; (6) Data Quality and Integrity; (7) Security; and (8) Accountability and Auditing.[64]

The Commission should ensure the privacy of the Smart Grid by requiring utilities to use the FIPs as part of their deployment plans in the following four ways. First, based on the FIPs, the Commission should define baseline privacy standards for Smart Grid deployment. Second, the Commission should require each utility to perform a privacy impact assessment as part of its Smart Grid planning process. Third, based on the assessment, each utility should adopt privacy practices meeting the minimum standards set by the Commission. These privacy practices should be responsive to each of the FIPs principles. Finally, the privacy impact assessments and the resulting privacy policies within the utilities' deployment plans should be revisited and re-approved in subsequent ratemakings and each time the Commission approves further investment pertaining to Smart Grid and Smart Device deployment. Only by an iterative process of problem definition, analysis, adoption, and review can the Commission and Californians be assured that their private information is being protected.

As part of the privacy impact assessment required by FIPs, a utility—in advance of actually building and deploying a system—would be required to answer key questions posed by the FIPs: What data will the utility be collecting? For what purpose? With whom will it share the data? How long will it keep the data? What confidence does it have that the data will be accurate and reliable enough for the purposes for which it will be used? How will it protect the data against loss or misuse? How will individuals have access to data about themselves? What audit, oversight and enforcement mechanisms will it have in place to ensure that it is following its own rules? The answers to these questions will provide important insights in the privacy and

[62] *Id.*
[63] *Id.* at 5-8.
[64] For a detailed discussion of these principles, please see *supra* § V.

security issues created by the Smart Grid. By identifying them early utilities can mitigate and guard against risks and protect consumer privacy at the lowest possible cost.

### A. The Commission Should Require Regular Review of Privacy Impact Assessments and the Resulting Privacy Policies Contained in Deployment Plans

To ensure compliance with the deployment plan requirements described above, the Commission should require periodic reviews of privacy impact assessments and privacy policies. Utilities should be required to evaluate their implementation and success of their privacy policies and report their findings to the Commission. Further, the Commission should require appropriate revisions to the privacy impact assessments and privacy policies when deployment plans are modified. Similarly, new assessments and policies should be completed prior to any new deployment or revision to Smart Grid architecture. Any privacy lapses or data breaches should be evaluated by the Commission prior to awarding new rates or approving new deployments to determine if the utility is taking and has taken appropriate steps to remedy the problem and generally to protect privacy.

### B. Privacy Considerations Must Be Built into the Design of the Smart Grid

Deployment plans can provide utilities an opportunity to address privacy concerns at an early design stage. Requiring strong privacy protections from the design stage will enable California's Smart Grid to maximize privacy and utility, while minimizing the cost of the protections. The Commission should require utilities adopt a "privacy by design" approach,[65] and build standards that reflect privacy interests into their deployment plans, rather than attempting to tack on privacy at a later point. Privacy by design is an effective and economically efficient means of protecting consumer privacy and security. Embedding privacy protections into the technology and design now, before smart meters and other Smart Grid technologies are fully deployed, and before the telecommunications infrastructures are installed, will prove less expensive than attempting to address these issues in the future and will make the grid more adaptable to changing threats to privacy and security as use increases.

[65] *See* Ann Cavoukian, Info. & Privacy Comm'r of Ont., *Privacy by Design*, http://www.privacybydesign.ca/ (last visited Mar. 9, 2010).

## VII. The Commission Should Consider and Adopt Our Recommended Modification to the Proposed Access Rule, as Provided in Appendix A

As the February 8, 2010 Joint Ruling notes, "[t]he Commission has adopted a policy to provide that some third parties can have access to [customer] data with the customer's permission."[66] The ruling goes on to express concern about a number of unintended and unauthorized uses of the data that the Smart Grid may effectuate. Third-party access to customer data may support third-party services that provide some of the benefits of the Smart Grid; at the same time, third-party access represents its greatest privacy threat. A utility, for example, is specifically subject to this Commission's rules and specific statutes that limit data use and disclosure.[67] A non-utility third party possessing the same data, on the other hand, may not face the same obligations, though general prohibitions against unfair or deceptive data practices (e.g., FTC Act § 5) and state security breach notification laws would apply. We support the Commission's suggestion to require customer authorization before a utility provides customer data to any third party. However, given the highly personal nature of the data that would potentially be shared, the Commission should adopt a strong privacy standard in its Proposed Access Rule[68] and should condition access on requirements that follow the Fair Information Practice principles.

Some third parties seeking access to customer data are likely to have business models based upon offering the consumer a service, perhaps for free, and then commercializing and selling the data. For example, a third-party service given access to granular usage data could offer consumers a useful service that helps them understand and control their energy consumption but base its profits on analyzing and selling behavioral information of interest to advertisers. Electronics retailers would like to know what appliances are in the home so they

---

[66] Feb. Joint Ruling, *supra* note 39, at 34.

[67] *See, e.g.*, Cal. Pub. Util. Code § 394.4 (requiring electric service providers to keep "customer information"—which encompasses "customer specific billing, credit, or usage information"—confidential unless the customer gives written consent to disclosure); D.97-12-088, app. A, § IV.A, *available at* ftp://ftp.cpuc.ca.gov/gopher-data/energy_division/affiliate/R9704011-Appendix%20A.doc ("A utility shall provide customer information to its affiliates and unaffiliated entities on a strictly non-discriminatory basis, and only with prior affirmative customer written consent."); Pac. Gas & Elec., *Rule 22 - Direct Access Rules* § C.3.a (1997), *available at* http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_22.pdf (requiring a customer to give written authorization for a utility to disclose usage data to direct access service providers); S.D. Gas & Elec., *Rule 25 - Direct Access Rules* § C.3.a (1999), *available at* http://www.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE25.pdf (same); S. Cal. Edison, *Rule 22 - Direct Access Rules* § C.3.a (2001), *available at* http://www.sce.com/NR/sc3/tm2/pdf/Rule22.pdf (same).

[68] Feb. Joint Ruling, *supra* note 39, app. B.

can market upgrades and accessories. A health insurance company may be interested in the number of hours a customer spends in front of the television. A dating website might be interested knowing that the number of residents at the household had recently fallen from two to one.

The consequences of utilities transferring customer data to third parties are significant. First, every copy and transmission of the data increases the risk of security breaches. Second, third parties may use the data in inappropriate or undisclosed ways. Third, the third parties may transfer the data on to yet other parties. Without proper protections, the customer could lose all control of her data once she authorizes third-party access. Customer trust in the Smart Grid is essential to its successful deployment and full adoption. Third-party misuse of data could be enough to undermine that trust. Therefore, the Commission's third-party data access rule should require utilities that deal with third parties to take appropriate steps to ensure that the third parties receiving data will provide appropriate privacy and confidentiality protections.

To actively protect against unexpected uses and the resulting harms, the Commission should adopt a robust regulatory framework granting affirmative control to customers as it extends to data generated by their households. This regulatory framework should attempt to maximize customer control over data and privacy protection, while enabling the benefits of the Smart Grid.

To reconcile these twin objectives, we propose a number of general changes to the Proposed Access Rule, based upon the Fair Information Practice principles. First, utilities should be required to obtain customer authorization based upon the full and complete disclosure of the uses that third parties will make of the data prior to giving third parties access to that information. If consumers agree to allow third-party access to such intimate information, the customer should be on specific notice of all uses prior to giving authorization. Second, utilities should be prohibited from sharing customer data with third parties unless the third parties agree, as a condition of receiving the data, to abide by specific FIPs principles, including: the full and complete disclosure of all uses of customer data; required reauthorization for changes in use; data breach notification; and privacy audits. The Commission should control downstream use of the data by conditioning access to the data on certain privacy and security requirements, including requiring regulated entities to condition third-party access to customer data on those

third parties agreeing to meet the requirements. The full text of our proposed rule can be found in Appendix A.

### A. Before a Utility May Transfer Data to a Third Party, the Third Party Must Disclose Uses to and Obtain Authorization from Customers

To protect consumers' privacy and security, the Commission should require utilities to include customer privacy protections in their contracts and dealings with third parties. First, to avoid unauthorized uses of a customer's data by a third party, third parties should disclose all of the intended uses of customer data before authorization. This disclosure will enable customers to make an informed decision and permit informed consent. Thus, our suggested modifications to the proposed Rule place certain disclosure requirements on third parties that contract with utilities for customer data. It requires third parties to disclose to the customer, prior to the customer's authorization to provide access to the third party: (1) "each specific use of the customer data," (2) "all other parties with whom the entity will share customer data," and (3) "a list of all of the data elements that will be transferred to the entity. . . ."[69] Clearly articulating the purpose of the data use, all parties that will use the data, and the exact data being shared, enables the consumer to make an informed choice before deciding to share data.

Further, the Proposed Rule currently requires utilities to provide authorized third parties with "advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information. . . ."[70] The default rule should not be full disclosure of all proprietary customer information. Our modified Rule provides that utilities only disclose information "that is necessary to accomplish the uses specifically disclosed to and authorized by the customer."[71] Utilities should review third parties' disclosed uses and should only provide the individual data fields necessary for those disclosed uses.

### B. Utilities Should Enforce Third Party Contractual Obligations

Once the utility transfers data to a third party a new set of risks and concerns arise. As described above, customer data is likely to be of interest to a wide variety of parties, for a wide

[69] *See infra* app. A, § 1(a)(i) (Modified Proposed Access Rule).
[70] *Id.* app. A, § 1.
[71] *Id.* app. A, § 1(b).

variety of purposes. Without intervention by the Commission, a third party that obtains customer information could sell that information to other third parties or use it in ways that were not authorized by the customer. The Commission should use its regulatory authority to ensure that any customer information transferred from a utility to a third party is sufficiently protected by requiring third parties to be contractually bound by the utilities as part of the consideration for receipt of customer data.

### 1. Prohibition On Non-Disclosed Uses and Parties

The Commission should require that utilities include clauses in contracts with third parties that require those third parties, as a condition of receiving customer data, to only use that data only for the specific purposes disclosed to the customer. Similarly, third parties should "not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer. . . ."[72] For example, a consumer should not receive unsolicited advertisements based upon energy usage data that her energy efficiency consultant sold to appliance marketers without her authorization. If a third party later wants to use customer data for other uses or provide it to other parties, it must obtain "specific re-authorization, in writing or via electronic signature" for those new uses or other parties.[73]

### 2. Privacy Impact Assessments

As part of the regular privacy impact audits and assessments we recommend the utilities conduct,[74] the Commission should require all entities in possession of customer data to conduct, and report to the Commission, "independent audit[s] of the security of customer data and entity compliance with its disclosed usage policy. . . ."[75] Such assessments are critical to understanding whether measures to protect privacy are successful or if they create cost without providing sufficient benefit, will guide entities in improving practices, and support the Accountability and Auditing principle.

[72] *Id.* app. A, § 1(a)(ii).
[73] *Id.* app. A, § 1(a)(iii).
[74] *See supra* § V.A.8 (Accountability and Auditing).
[75] *See infra* app. A, § 2.

### 3. Data Quality and Integrity

Customers should have the right to see what data an entity possesses about them and to correct any inaccuracies in that data. The requirement is an important component of the FIPs Data Quality and Integrity principle, discussed in more detail above.[76] Our modified rule would require that entities possessing customer data "provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies."[77]

### 4. Data Destruction

Based upon the FIPs Data Minimization principle,[78] our modified Rule would require entities in possession of customer information to "destroy customer data when it is no longer necessary for the uses disclosed to the customer. . . ."[79] Destroying unnecessary data significantly reduces the risk of unauthorized use and disclosure of customer information.

### 5. Data Breach Notification

In Section V.C, we urged the Commission to apply California's Data Breach Notification Law, section 1789.29 of the Civil Code, to regulated entities. The Commission should likewise require third parties that handle customer data to notify customers and the Commission of any unauthorized disclosure, use, or access of the customer data, so that the customer can take appropriate steps to protect herself and modify her behavior accordingly (for example, by ceasing to share information with the party that allowed the breach). Requiring third parties to provide notification will provide strong incentives for safe and secure information practices so they can avoid the cost and embarrassment of having to report a data breach. Section 3(c) of our proposed Rule thus requires any entity in possession of proprietary customer information to follow the section 1789.29 data breach notification rules.

[76] *See supra* § V.A.6 (Data Quality and Integrity).
[77] *Id.* app. A, § 3(a).
[78] *See supra* §V.A.4 (Data Minimization).
[79] *See infra* app. A, § 3(b).

### C. Other Third Party Access Rules That the Commission Should Consider

#### 1. Government Access to Customer Information

We urge the Commission to specify, within the Proposed Access Rule, when and how utilities should provide customer information to law enforcement officials and other government agencies. Under both California and Federal law, the home, as a retreat from the outside world and from the government, is an especially protected space, with an especially strong privacy interest attached to it.

Longstanding United States constitutional values and precedent afford special protection for activities occurring within the sanctity of individuals' homes because of their inherently personal nature. The Fourth Amendment draws "a firm line at the entrance to the house,"[80] because "privacy expectations are most heightened" in the "private home."[81] The Supreme Court affirmed this protection for all types of data found in the home, noting in *Kyllo v. United States* that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[82] In *Kyllo*, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement.[83] Data collected via Smart Grid technologies is similarly revealing of the intimate details of home life and should be subject to at least the same high levels of protection that the Supreme Court required of law enforcement in *Kyllo*.

Californian's constitutional privacy protections extend further than general Fourth Amendment protections and have been found to protect business records.[84] Although the California Supreme Court has not yet addressed energy privacy, it has recognized a protected privacy interest in other records held by third parties. For example, in *Burrows v. Superior*

---

[80] *Payton v. New York*, 445 U.S. 573, 590 (1980).
[81] *Dow Chemical Co. v. United States*, 476 U.S. 227, 237 n.4 (1986); *see Boyd v. United States*, 116 U.S. 616, 630 (1886) ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property[.]").
[82] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).
[83] *Id*. at 40.
[84] *See, e.g.*, *Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652 (1975).

*Court*,[85] the court held that customer information voluntarily disclosed by a bank to law enforcement officers without the customer's knowledge or consent was the product of an unlawful search and seizure under article I, section 13, of the California Constitution. The court went on to hold that customers expect that the information they share with their banks will remain private, and that "absent compulsion by legal process . . . [the customer expects the matters he] reveals to the bank will be utilized by the bank only for internal banking purposes."[86] Later cases have similarly protected telephone records.[87]

Article 1, section 1 of the California Constitution provides additional protections. In *Brillantes v. Superior Court*, the court held that "an intrusion upon constitutionally protected areas of privacy requires a balancing of the juxtaposed rights, and the finding of a compelling state interest."[88] The court allowed the seizure of medical records only where "the state [had] demonstrated a compelling interest in the medical records related to the Medi-Cal fraud investigation."[89] Similarly, in *McKirdy v. Superior Court*, the court affirmed "any [incursion into individual privacy] must be justified by a compelling interest."[90]

The Commission has already recognized that the privacy protections inherent in sections 1 and 13 of article 1 of the California Constitution extend to cover customer energy data. In Decision No. 90-12-121 and its appeal, Decision No. 01-07-032, the Commission extensively examined privacy concerns related to law enforcement access to utility data and, relying on the *Burrows*,[91] *Blair*,[92] and *Chapman*[93] line of cases, determined that it should not be disclosed to law enforcement without adequate legal process.[94] We urge the Commission to follow this precedent and re-affirm that law enforcement and government agencies must obtain adequate legal process before accessing customer energy usage data. Because of the unusually private nature of granular energy usage data, we urge the Commission to go a step further and require law enforcement to show probable cause in the form of a warrant before a utility releases such

[85] 13 Cal. 3d 238 (1974).
[86] *Id*.
[87] *People v. Blair*, 25 Cal. 3d 640, 653-54 (1979); *People v. Chapman*, 36 Cal. 3d 98 (1984).
[88] 51 Cal. App. 4th 323, 340 (1996).
[89] *Id.* at 342.
[90] 138 Cal. App. 3d 12, 22 (1996).
[91] 13 Cal. 3d 238.
[92] 25 Cal. 3d 640.
[93] 36 Cal. 3d 98.
[94] D.90-12-121; D.01-07-032.

data. Providing such data to law enforcement without a warrant would be inconsistent with Californians' constitutional right to privacy[95] and the federal Constitution.

### 2. Civil Litigant Access to Customer Information

In the context of civil litigation, given the sensitivity of smart meter data and its potential to reveal private details of home life, there should be a preference for seeking such data not from the utility, but from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way a civil litigant can obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information.

In *White v. Davis*,[96] the first California Supreme Court case to interpret article 1, section 1, of the state constitution, the Court solidified Californian's right to informational privacy. The court held that the constitutional privacy right protects citizens from use of personal information "for another purpose or the disclosure of it to some third party."[97] The court later held in *Hill v. National Collegiate Athletic Assn.,*[98] and affirmed in *American Academy of Pediatrics v. Lungren*,[99] that in cases where there is an obvious invasion of a right fundamental to informational privacy or autonomy, a "compelling interest must be present to overcome the vital privacy interest."[100] If, in contrast, the privacy interest is less central, or in bona fide dispute, a general balancing test is employed.[101] Because of the intrusive nature of energy usage data, as described above, civil litigants should be required to show a compelling interest in the information.

Further, California case law has held that entities receiving subpoenas for private information on their customers must notify the customers prior to disclosing the information and allow time for them to respond. The Commission should similarly protected customer energy information. In *Valley Bank of Nevada v. Superior Court,* the California Supreme Court held that "before confidential customer information may be disclosed in the course of civil discovery

---

[95] Cal. Const. art. I, §§ 1, 13.
[96] 13 Cal 3d 757 (1974).
[97] *Id*. at 775.
[98], *Hill v. Nat'l Collegiate Athletic Assn.,* 7 Cal. 4th 1 (1994).
[99] *Am. Academy of Pediatrics v. Lungren,* 16 Cal. 4th 307 (1997).
[100] *Hill*, 7 Cal. 4th at 34.
[101] *Id.*

proceedings, [a] bank must take reasonable steps to notify its customer."[102] Similarly, in *Sehlmeyer v. Department of General Services*, the court held that the constitutional right to privacy requires "that an administrative subpoena duces tecum [seeking a third party witness's medical records] must be preceded by notice to the witness."[103] The courts have also recognized the need to "afford the third party a fair opportunity to assert her interests by objecting to disclosure, by seeking an appropriate protective order[,] or by instituting other legal proceedings to limit the scope or nature of [discovery]."[104]

To keep utility practices in line with California case law, the Commission should require that utilities and other regulated entities only disclose customer data to civil litigants upon being provided with a court order based on a showing of compelling interest and after notifying the customer to provide her with a chance to object.

### 3. Rules Regarding Third-Party Handling of Customer Information Received Directly from Consumers

The discussion above urges the Commission to adopt rules regulating the use of customer information by utilities and third parties to whom utilities provide customer data. These suggestions are in response to the Commission's specific questions regarding these entities. However, numerous other third parties presently obtain, or plan to obtain, energy usage data directly from the consumer via devices installed in the home, below the meter. For example, Google's' "Power Meter" device captures energy usage data directly from consumers, below the meter. Google presently does not charge for the service.[105] In these situations, the utilities may not be able to act as a gatekeeper for the information. The customer data obtained by these third parties is no less private than the customer data collected and transferred by the utilities, nor would its misuse be any less invasive. As such, we urge the Commission and other regulators to adopt rules similar to the ones outlined here[106] for all parties collecting, using, and transmitting customer information, whether they obtain that data above or below the meter.

---

[102] 15 Cal. 3d 652, 658 (1975).
[103] 17 Cal. App. 4th 1072, 1079 (1993).
[104] *Id.* at 1085 (citing *Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652, 658 (1975)).
[105] For information on Google's service, see Google Power Meter, Frequently Asked Questions, http://www.google.org/powermeter/faqs.html (last visited Mar. 9, 2010).
[106] *See supra* §§ VII.A, B; *see also infra*, app. A.

## VIII. The Commission Should Include Privacy-Related Quantitative Metrics for Smart Grid Implementations

We support the Commission's proposed use of metrics as a measure of Smart Grid deployment and strongly support the specific use of privacy metrics as a means of measuring the privacy vulnerabilities of the deployed Smart Grid. We recommend that such metrics should be required components of all Smart Grid deployment plans and should be updated by regulated utilities in subsequent proceedings relating to discrete Smart Grid implementations and ratemakings. We propose the following additions and modifications to the Commission's proposed metrics in Attachment C of the Joint Ruling, based on our identification of privacy risks in Section II.B and discussion of Fair Information Practice principles in Section V above.

### A. Cyber Security Metrics

The Commission should add the following metrics to Section 2 of the Proposed Metrics to fill the placeholder for cyber security metrics:

- Number of security breaches experienced by the utility or third parties to which the utility provides customer information.
- Number and percentage of customers affected by the security breaches.
- Number and percentage of customer records accessed during the security breaches.
- Average number of days between the security breach and when the customers are notified.
- Number of attempted cyber attacks on the utility or third parties to which the utility provides customer information.
- Monetary damages suffered by utilities or consumers as a result of cyber attacks on the utility or its infrastructure.
- Amount of annual operational expenditure on cyber security.
- Percentage of expenditure on cyber security in the overall operating expense.

- Amount of damages incurred to customers' smart devices as a result of cyber attacks.

- Number of security and privacy impact assessments performed by utilities.

### B. Privacy Metrics

We also recommend the following modifications and additions to the proposed metrics in Attachment C of the Joint Ruling to prevent additional privacy harms and to give the Commission specific insight into consumer privacy protections:

- Remove the first item under Section 5 which presently reads "the number and percentage of electricity customers . . . served by appliances and/or equipment which can communicate information automatically about on/off status and availability for load control." This proposed metric encourages the use of customer devices to reveal detailed status information to the utility. This metric is adverse to the privacy interest of residential customers and should be removed.

- Allowing customers to control the granularity of data flowing outside their homes is crucial to privacy. Therefore, we recommend adding the following metrics to Section 9 "Provide Consumers with Timely Information and Control Options:"
    - Number of customers able to control the time interval of smart meter reading reported to utility.
    - Number of customers that exercise control over the time interval of smart meter reading reported to utility.
    - Number of customers able to control their smart devices with their own Energy Management System.
    - Number of customers that exercise control over their smart devices with their own Energy Management System.

- Customer concern about privacy represents a barrier to Smart Grid adoption. Therefore, we recommend adding the following metrics to Section 11 "Lowering Barriers to Adoption of Smart Grid:"
    - Amount of customer information collected about an average residential customer and retention period of such data.
    - Number and type of third party entities receiving customer information under the [Proposed] Access Rule.
    - Number and type of law enforcement or other government requests to access customer information held by the utility or the third parties to whom the utility provides information, and the compliance with such requests.
    - Number of individuals whose customer information was provided to law enforcement or other government agencies.
    - Number and type requests by civil litigants to access customer information held by the utility and the compliance with such requests.
    - Number and type of third parties to whom the utility provides information, and the compliance with such requests.
    - Number and type of data breach notifications during the reporting period.

Finally, the Commission should delete the first metric in Section 6 of the Proposed Metrics: "Number of consumer devices actively communicating with Home Area Networks." This metric is detrimental to data minimization and therefore to privacy protection, as it requires utilities to obtain information about appliances within consumers' homes. A consumer may have deployed a Home Area Network for the express purpose of protecting her privacy by hiding the devices within the home from the utility. Such metrics, relating to in-home deployment, should take into account the fact that privacy-friendly smart devices may be invisible to the utilities. The Commission's metrics should respect customers' desire for privacy and not encourage the utilities to collect detailed device information from residential customers.

## IX. The Commission Should Not Wait for Privacy Standards from the National Standard-Setting Bodies, and Should Adopt Fair Information Practice Principles Now

State Senate Bill 17 instructs the Commission to "adopt standards and protocols to ensure functionality and interoperability developed by public and private entities, including, but not limited to, the National Institute of Standards and Technology, Gridwise Architecture Council, the International Electrical and Electronics Engineers, and the National Electric Reliability Organization recognized by the Federal Energy Regulatory Commission."[107] As the Commission has observed, however, the national standard-setting organizations have not yet released final drafts of their standards and protocols.[108] The Commission seeks comment on three possible approaches to this problem.

1) Deferring Commission consideration in this proceeding until a number of the listed agencies have adopted standards or protocols;

2) Deferring Commission consideration of protocols to another proceeding that will commence after a number of the listed agencies have adopted standards or protocols; or

3) Adopting a "performance standard" in this proceeding requiring that those implementing a Smart Grid technology take steps to ensure that it has the capability to function and operate with devices developed pursuant to standards adopted by major standard setting agencies.[109]

In light of the rapid deployment of Smart Grid technologies already underway in California, approaches (1) and (2) above appear as problematically slow for addressing adequately issues of privacy and consumer protection. It is unclear how long it will take for "a number of the listed agencies" to adopt standards; smart devices deployed during this open-ended time period, risk non-compliance with both the technical standards and privacy standards that the Commission eventually adopts.

At the same time, approach (3) appears not to address privacy issues, at all, as the

[107] Cal. Pub. Util. Code § 8362.
[108] Feb. Joint Ruling, *supra* note 39, at 19.
[109] *See id*. These three options are slightly reworded from the language in the original ruling.

"functional operability with other devices" requirement carries no privacy protections or restrictions. Further, approach (3) shifts significant standards decision-making authority to the utilities themselves, creating a self-regulatory regime and depriving the utilities of meaningful Commission guidance on relevant standards. For this reason, it is unclear whether approach 3 succeeds in meeting the obligations imposed by SB 17.

We thus urge the Commission to pursue a fourth option, at least with regard to privacy requirements. The Commission should adopt concrete privacy requirements based on the Fair Information Practice principles without delay, and should compare technical and other standards presented to it against these requirements. If national standards or guidelines related to privacy protections are promulgated in the future, the Commission can open a new proceeding to consider these.

As described further above in Section V,[110] the FIPs are a widely recognized and well established framework for information management. Indeed, it is unlikely that any of the national standard-setting organizations would release privacy standards that were not reflective of, or influenced by, the Fair Information Practice principles. If the Commission later considers adoption of standards from these national standard-setting organizations, we urge the Commission to disregard outright any set of standards that does not reflect the FIPs framework.

Privacy is a valued constitutional right in California, and the Commission has adequate authority, under article 1, section 1 of the California Constitution to adopt Smart Grid privacy standards immediately and on its own initiative,[111] independent of authority granted it by SB 17. We urge that the Commission adopt the Fair Information Practice principles as California's Smart Grid privacy protection framework. California also has a strong history of being at the forefront of both environmental and privacy regulation. Where California leads, the rest of the states and the federal government follow. The Smart Grid provides the Commission with an opportunity to help California to continue to lead the country in environmental regulation and privacy protection.

[110] For a comprehensive overview and explanation of the FIPs, please refer to § V, *supra*.
[111] *See* discussion *supra* § III.

## X. Conclusion

The Center for Democracy & Technology and the Electronic Frontier Foundation appreciate the opportunity to submit these comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010. We commend the Commission on its careful consideration of the consumer privacy risks presented by the emerging Smart Grid, and we thank the Commission again for its consideration of the privacy recommendations we have presented here.

Respectfully submitted this March 9, 2010 at San Francisco, California.

/s/ Jennifer Lynch

JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

/s/ Lee Tien

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

**APPENDIX A – Modifications to Language of Proposed Third Party Access Rules[112]**

1. An electrical corporation shall provide a customer, the customer's electric service provider (ESP), the customer's demand response provider (DRP), or other third party entity authorized by the customer read-only access to the customer's advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information (collectively, "customer data") only as described herein in sections 1 through 8. ESPs, DRPs, or any other third parties that obtain customer data shall not disclose or use that customer data except as described herein in sections 1 through 8. The access shall be convenient and secure, and the data shall be made available no later than the next day of service. Such authorization may be made in writing or via electronic signature, consistent with industry, privacy and security standards and methods. The utility may only transfer customer data:

    a. to an entity that is either (i) already bound by this section or (ii) contractually agrees, in consideration of receiving the data, to

        i. fully disclose to the customer, prior to obtaining authorization:

            1. each specific use of the customer data,

            2. all other parties with whom the entity will share the customer data, and

            3. a list of all of the data elements that will be transferred to the entity (these may include, for example, name, address, social security number, meter readings [including the frequency of measurements being provided], appliance ID numbers, or any other discrete types of information being transferred);

[112] Throughout this Appendix A, we have used specific formatting to denote changes. The proposed additions that the Commission denoted in its Feb. Joint Ruling with underlined text have been included in our Appendix text without an underline. We have illustrated our further additions with an underline. Text that is formatted with a strikethrough *only* represents the text in the Feb. Joint Ruling that was also presented in strikethrough. Text that is contains both an *underline and a strikethrough* is text that was provided in the Feb. Joint Ruling and that we recommend omitting.

ii. not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer under (i), above;

iii. obtain separate, specific re-authorization, in writing or via electronic signature, for any new use of customer data or new entity with which it plans to share the data, consistent with (i), above; and

iv. abide by the regulations in sections 2 and 3, below; and

b. that is necessary to accomplish the uses specifically disclosed to and authorized by the customer.

2. An electrical corporation or other entity providing customer data shall use at a minimum industry standards and methods for providing secure customer, ESP, DRP and third party access to a specified customer's ~~meter~~ data. For purposes of these Rules, "industry standards" shall include those industries that routinely deal with highly personal, sensitive and confidential information, including but not limited to the financial industry and the medical information industry. ~~[The electrical corporation~~ All entities in possession of customer data shall have an independent security audit of the mechanism for customer and third party access to ~~meter~~ customer data conducted within one year of initiating such access and report the findings to the Commission.~~]~~ Thereafter, all entities in possession of customer data shall have an independent audit of the security of customer data and entity compliance with its disclosed usage policy on an annual basis and shall report the findings to the Commission, which shall make the reports publicly available.

3. All entities in possession of customer data shall:

a. provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies;

b. destroy customer data when it is no longer necessary for the uses disclosed to the customer;

c. follow the data breach notification rules described in Cal. Civ. Code § 1798.29, for the loss or unauthorized acquisition of or access to customer data; and,

d. only disclose customer data to law enforcement after being provided with a warrant.

e. only disclose customer data to civil litigants after being provided with a court order based on a showing of compelling interest and after notifying the customer to provide the customer with a chance to object to disclosure.

4. ~~3.~~ The California Independent System Operator, or any subsequent regional transmission organization or regional reliability entity, shall have access only to information necessary or required for wholesale settlement, load profiling, load research and reliability purposes.

5. ~~4.~~ A customer may authorize, either in writing or by electronic signature, its customer data to be available to an entity other than its Load Serving Entity or Utility Distribution Company, subject to the requirements of sections 1 through 3.

6. ~~5.~~ An electrical corporation shall provide access to data, as described above, in a manner consistent with and in accordance with the time frame as decided by the Commission in Decision _____,

   Revised rule modeled on Tariff Rule 22[56]

7. ~~3.~~ Providing Access to Customer Data Captured by AMI for Authorized Third Parties

   [Insert utility] will only provide customer-specific usage data to parties specified and authorized by the customer, subject to the provisions in sections 1 through 3 above, and the following provisions:

   a. ~~Except as provided in Section d, t~~The inquiring party must have ~~written~~ authorization from the customer, either in writing or by electronic signature, to release such

[56] Tariff Rule 22 was the tariff adopted by electric utilities to provide for Direct Access Service. A copy of PG&E's Tariff Rule 22 is available online at: external link: http://beta1.pge.com/nots/rates/tariffs/pdf/ER22.pdf. The relevant portion is at C.3, on tariff sheets 11-12.

information to the inquiring party only. Such authorization must be revocable. At the customer's request, this authorization may also indicate if customer information may be released to other parties as ~~specified~~ specified and authorized by the customer.

b. Subject to customer authorization, [~~I~~insert utility] will provide ~~a maximum of~~ not more than the most recent twelve (12) months of customer usage data ~~or the amount of data for that specific service account~~ in a format consistent with industry standards, including privacy and security standards, as approved by the Commission. Customer information will be released to the customer or an authorized agent ~~up to two (2) times per year per service account~~ at no cost to the ~~requesting party~~ or the customer. ~~Thereafter, [insert utility] will have the ability to assess a processing charge only if approved by the Commission.~~

c. ~~As a one time requirement at the initiation of Direct Access, [~~i~~~~I~~nsert utility] will make available a database containing a twelve (12) month history of customer-specific customer's data usage information with geographic and SIC information, but with customer identities removed, to a ~~customer's ESP, DRP or other~~ third party~~ies~~ approved by the Commission, subject to the requirements of this provision and provisions 1 through 3, and only where a customer has authorized such disclosure. ~~[Insert utility] will have the ability to assess a charge only if approved by the Commission.~~

~~d. By electing to take Direct Access service from an ESP, the customer consents to release to the ESP metering information required for billing, settlement and other functions required for the ESP to meet its requirements and twelve (12) months of historical data.~~

d. A third party receiving customer data pursuant to this section shall use such data only for the purposes to which the consumer consented and shall be subject to the same rules on privacy and security that are applicable to utilities handling customer data.

~~d. By authorizing third party to access their information, the customer consents to release to a third party information required for billing, settlement and other functions~~

and services required for that entity to meet its requirements and obligations and twelve (12) months of historical data.

CERTIFICATE OF SERVICE

I hereby certify that, pursuant to the Commission's Rules of Practice and Procedure, I have this day served a true copy of this document, JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID, on all parties identified on the attached official service list for Proceeding: R08-12-009. Service was completed by serving an electronic copy on their email address of record and by mailing paper copies to parties without email addresses.

Executed on March 9, 2010 at Berkeley, California

/s/ Jennifer Lynch
JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California – Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200

**SERVICE LIST**

carlgustin@groundedpower.com
jeffrcam@cisco.com
cbrooks@tendrilinc.com
npedersen@hanmor.com
slins@ci.glendale.ca.us
douglass@energyattorney.com
ffletcher@ci.burbank.ca.us
kris.vyas@sce.com
atrial@sempra.com
lburdick@higgslaw.com
liddell@energyattorney.com
mshames@ucan.org
ctoca@utility-savings.com
bobsmithttl@gmail.com
mtierney-lloyd@enernoc.com
ed@megawattsf.com
mterrell@google.com
mdjoseph@adamsbroadwell.com
pickering@energyhub.net
margarita.gutierrez@sfgov.org
lms@cpuc.ca.gov
fsmith@sfwater.org
srovetti@sfwater.org
tburke@sfwater.org
lettenson@nrdc.org
marcel@turn.org
mkurtovich@chevron.com
SSchedler@foe.org
cjw5@pge.com
nes@a-klaw.com
pcasciato@sbcglobal.net
steven@sfpower.org
mgo@goodinmacbride.com
mday@goodinmacbride.com
ssmyers@worldnet.att.net
lex@consumercal.org
farrokh.albuyeh@oati.net
Service@spurr.org
wbooth@booth-law.com
jwiedman@keyesandfox.com
kfox@keyesandfox.com
enriqueg@greenlining.org
gmorris@emf.net
kerry.hattevik@nrgenergy.com
rquattrini@energyconnectinc.com
seboyd@tid.org
martinhomec@gmail.com
dzlotlow@caiso.com
dennis@ddecuir.com
scott.tomashefsky@ncpa.com
jhawley@technet.org
lnavarro@edf.org
Lesla@calcable.org
cbk@eslawfirm.com
gstaples@mendotagroup.net
jlin@strategen.com
MNelson@MccarthyLaw.com
EGrizard@deweysquare.com
Mike.Ahmadi@Granitekey.com
r.raushenbush@comcast.net
tam.hunt@gmail.com
john.quealy@canaccordadams.com
mark.sigal@canaccordadams.com
barbalex@ctel.net
crjohnson@lge.com
julien.dumoulin-smith@ubs.com
david.rubin@troutmansanders.com
jennsanf@cisco.com
marybrow@cisco.com
jmccarthy@ctia.org
jay.birnbaum@currentgroup.com
bboyd@aclaratech.com
bob.rowe@northwestern.com
monica.merino@comed.com
sthiel@us.ibm.com
ed.may@itron.com
rgifford@wbklaw.com
leilani.johnson@ladwp.com
dschneider@lumesource.com
david@nemtzow.com
cjuennen@ci.glendale.us
fhall@solarelectricsolutions.com
mark.s.martinez@sce.com
case.admin@sce.com
michael.backstrom@sce.com
nquan@gswater.com
Jcox@fce.com
esther.northrup@cox.com

kfoley@sempra.com
kmkiener@cox.net
ygross@sempra.com
rwinthrop@pilotpowergroup.com
CentralFiles@semprautilities.com
tcahill@semprautilities.com
cmanson@semprautilities.com
jerry@enernex.com
traceydrabant@bves.com
peter.pearson@bves.com
dkolk@compenergy.com
ek@a-klaw.com
rboland@e-radioinc.com
sue.mara@rtoadvisors.com
juan.otero@trilliantinc.com
mozhi.habibi@ventyx.com
faramarz@ieee.org
elaine.duncan@verizon.com
mandywallace@gmail.com
norman.furuta@navy.mil
kgrenfell@nrdc.org
mcarboy@signalhill.com
nsuetake@turn.org
bfinkelstein@turn.org
andrew_meiman@newcomb.cc
ayl5@pge.com
DNG6@pge.com
fsc2@pge.com
filings@a-klaw.com
Kcj5@pge.com
mpa@a-klaw.com
rcounihan@enernoc.com
stephen.j.callahan@us.ibm.com
tmfry@nexant.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
cassandra.sweet@dowjones.com
jscancarelli@crowell.com
jas@cpdb.com
nml@cpdb.com
SDHilton@stoel.com
Diane.Fellman@nrgenergy.com
cem@newsdata.com
lisa_weinzimer@platts.com
prp1@pge.com
achuang@epri.com
caryn.lai@bingham.com
epetrill@epri.com
ali.ipakchi@oati.com
chris@emeter.com
sharon@emeter.com
ralf1241a@cs.com
sean.beatty@mirant.com
john_gutierrez@cable.comcast.com
t_lewis@pacbell.net
Valerie.Richardson@us.kema.com
nellie.tong@us.kema.com
Douglas.Garrett@cox.com
rstuart@brightsourceenergy.com
mrw@mrwassoc.com
cpucdockets@keyesandfox.com
dmarcus2@sbcglobal.net
rschmidt@bartlewells.com
jlynch@law.berkeley.edu
jurban@law.berkeley.edu
kco@kingstoncole.com
philm@scdenergy.com
j_peterson@ourhomespaces.com
joe.weiss@realtimeacs.com
michaelboyd@sbcglobal.net
bmcc@mccarthylaw.com
sberlin@mccarthylaw.com
mary.tucker@sanjoseca.gov
tomk@mid.org
joyw@mid.org
brbarkovich@earthlink.net
gayatri@jbsenergy.com
dgrandy@caonsitegen.com
demorse@omsoft.com
martinhomec@gmail.com
e-recipient@caiso.com
hsanders@caiso.com
jgoodin@caiso.com
wamer@kirkwood.com
tpomales@arb.ca.gov
brian.theaker@dynegy.com
danielle@ceert.org
dave@ppallc.com
jmcfarland@treasurer.ca.gov
shears@ceert.org
kellie.smith@sen.ca.gov
lkelly@energy.state.ca.us

mgarcia@arb.ca.gov
ro@calcable.org
steven@lipmanconsulting.com
lmh@eslawfirm.com
abb@eslawfirm.com
bsb@eslawfirm.com
glw@eslawfirm.com
jparks@smud.org
ljimene@smud.org
ttutt@smud.org
vzavatt@smud.org
vwood@smud.org
dan.mooy@ventyx.com
kmills@cfbf.com
rogerl47@aol.com
jellis@resero.com
michael.jung@silverspringnet.com
wmc@a-klaw.com
bschuman@pacific-crest.com
sharon.noell@pgn.com
californiadockets@pacificorp.com
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
am1@cpuc.ca.gov
crv@cpuc.ca.gov
df1@cpuc.ca.gov
dbp@cpuc.ca.gov
trh@cpuc.ca.gov
fxg@cpuc.ca.gov
gtd@cpuc.ca.gov
jw2@cpuc.ca.gov
jdr@cpuc.ca.gov
jmh@cpuc.ca.gov
kar@cpuc.ca.gov
kd1@cpuc.ca.gov
lau@cpuc.ca.gov
zaf@cpuc.ca.gov
mjd@cpuc.ca.gov
mc3@cpuc.ca.gov
wtr@cpuc.ca.gov
rhh@cpuc.ca.gov
srt@cpuc.ca.gov
scl@cpuc.ca.gov
scr@cpuc.ca.gov
tjs@cpuc.ca.gov
vjb@cpuc.ca.gov
wmp@cpuc.ca.gov
BLee@energy.state.ca.us
ab2@cpuc.ca.gov

**Before the**
**Department of Commerce**

**National Institute of Standards and Technology**

| | | |
|---|---|---|
| Request for Comments | ) | |
| | ) | |
| Draft NIST Interagency Report (NISTIR) | ) | Docket Number 0909301329-91332-01 |
| 7628, Smart Grid Cyber Security Strategy | ) | |
| And Requirements | ) | |

# COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

December 1, 2009


Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
585 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7338

on behalf of the
Center for Democracy & Technology


December 1, 2009

**Table of Contents**

## Executive Summary

We are grateful for and commend NIST's vitally important work in developing a Smart Grid Cyber Security strategy, and particular the effort to make recommendations for protecting consumer privacy, in the *NIST Interagency Report (NISTIR) 7628.*

The Smart Grid promises great benefits to consumers and the environment. At the same time, it presents new risks to privacy in its enhanced collection and use of highly granular consumption data, which can reveal intimate details about activities within the home. The entrance of new entities and technologies delivering energy services, the speed at which this new infrastructure is being deployed, and the lack of clear governing rules further support the need to address the privacy risks to consumers created by the Smart Grid.

As part of NIST's work to coordinate the development of a framework for a modernized and interconnected grid, it should develop and recommend strong privacy principles that can be incorporated into standards and technical requirements, and should develop robust, rigorous use cases that illustrate privacy-affecting scenarios in Smart Grid technologies and services, and show how privacy principles can be built into Smart Grid architecture. Creating privacy-protective systems and technologies for the Smart Grid should not require a tradeoff with functionality, but it will require thoughtful design. In adopting a "privacy by design" approach, rather than attempting to tack on privacy at a later point, NIST can support the most effective means of protecting consumer privacy in the Smart Grid, and provide needed guidance to state regulators and industry players.

Developing effective privacy protections for the Smart Grid must be grounded in a thorough examination of how the proposed technologies will affect consumer privacy interests. In this Comment, we provide an overview of consumer data flow in the Smart Grid under several proposed NIST standards and discuss the privacy risks and legal rules implicated by the unprecedented collection of detailed information about customers' energy and appliance use contemplated by Smart Grid technologies and services—information traditionally afforded strong legal protection within the home. We proceed to propose a specific framework for protecting privacy in the Smart Grid based on a robust and comprehensive set of Fair Information Practice Principles ("FIPPs"), including who should be covered, what types of data should be covered, and how a FIPPs-based framework can ensure meaningful protections for consumers' "Household Energy Data." All of the technical standards identified by NIST for implementation in the Smart Grid should be evaluated against these principles, and NIST should make recommendations regarding standards based upon them, and upon a rigorous set of use cases that can inform standards bodies and the design of new Smart Grid technologies.

**Before the**
**Department of Commerce**

**National Institute of Standards and Technology**

| | | |
|---|---|---|
| Request for Comments | ) | |
| | ) | |
| Draft NIST Interagency Report (NISTIR) | ) | Docket Number 0909301329-91332-01 |
| 7628, Smart Grid Cyber Security Strategy | ) | |
| And Requirements | ) | |

# Comments of the Center for Democracy & Technology

December 1, 2009

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the National Institute of Standards and Technology's ("NIST") request for comments on the *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements* ("Draft"). CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet**.**

## I. Introduction

NIST's work to develop a Smart Grid cybersecurity strategy, including recommendations for protecting consumer privacy in the modernized grid, is a vitally important effort. The transition to the Smart Grid promises great benefits for consumers, including lowered energy costs, increased usage of environmentally-friendly power sources, and enhanced security against attack and outage. At the same time, it presents new risks to consumer privacy. At the core of the modernized grid's functionality is fine-grained household data; in order to enable more efficient energy use, and to more actively engage individual consumers and their appliances in energy management, the Smart Grid, as currently envisioned by proponents, depends on the collection and use of highly granular consumption data.[1] Recent experiments using the simplest data mining and pattern matching techniques reveal how easily this information can be analyzed to expose intimate details about activities within the home with a high degree of accuracy.[2]

[1] Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE, May/June 2009.
[2] Mikhail Lisovich, Deirdre K. Mulligan, and Stephen B. Wicker, *Privacy Concerns in Upcoming Demand-Response Systems*,
http://wislsrv.ece.cornell.edu/~mikhail/Copy%20of%20Source%20Material/lisovich2007pci_v3.pdf.

From a consumer privacy perspective, we stand at a critical juncture in the development of Smart Grid technologies for several reasons. First, the emergence of increasingly sophisticated metering technologies are enabling the unprecedented collection of energy consumption data, removing a "latent structural limitation" that previously protected the revelation of intimate details about household activities.[3] Whereas historically a consumer's consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new demand response systems will collect a record of 750 to 3,000 data points a month, revealing variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.[4] Second, the transition to a highly-interconnected and less-bordered electrical infrastructure is inviting participation by new entities, such as third-party service providers offering new web-based portals for managing energy use, who are utilizing consumer data in new ways and presenting the need for privacy analysis extending beyond the more straightforward consumer-to-utility relationship. Third, the rapid pace of Smart Grid deployment, and the speed at which new Smart Grid technologies are moving out of the pilot project stage to large-scale implementation, is making the consideration of the consumer privacy issues presented by these technologies more urgent. Finally, against this landscape of rapid development, there remains a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use," creating "a privacy risk that needs to be addressed," as prudently noted in the NIST Draft.[5]

Against this backdrop, NIST's work to coordinate Smart Grid standards will ensure there is a common set of widely supported open protocols governing the modernized grid. But there is also an urgent need for NIST to issue recommendations based on strong privacy principles that can be reflected in these technical standards and requirements. Adopting a "privacy by design" approach, and building standards that reflect privacy interests, rather than attempting to tack on privacy at a later point, is the most effective means of protecting consumer privacy and security.[6] Embedding privacy protections into the technology now, before smart meters and other Smart Grid technologies are fully deployed, and as information systems are being developed, will also be less expensive than attempting to address these issues in the future, and will make the grid more adaptable to changing threats to privacy and security as use increases.

---

[3] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU Law Review 1605 (2007), http://ssrn.com/abstract=1004675, at 139 (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints").
[4] Jack I. Lerner and Deirdre K. Mulligan, Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home, 2008 Stan. Tech. L. Rev. 3. at 3.
[5] NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, http://www.nist.gov/smartgrid/.
[6] *See* Information and Privacy Commissioner of Ontario, *Privacy by Design*, http://www.privacybydesign.ca/.

Further, ensuring that a robust set of privacy principles underlie NIST's Smart Grid framework is important in providing guidance to state regulators, utilities, third-party service providers, and device manufacturers wrestling with privacy issues. California, for example, recently amended its Public Utility Code to require the Public Utility Commission to explicitly consider NIST standards as a candidate for implementation in the State's Smart Grid infrastructure.[7]

We commend NIST's efforts to date to consider the privacy implications of the consumer-to-utility information collection envisioned in the Smart Grid, and especially the work of the Cyber Security Coordination Task Group ("CSCTG") in performing an initial Privacy Impact Assessment ("PIA") of that collection in the *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements* document ("Draft"). However, much work remains to be done. Developing effective privacy protections for the Smart Grid must be grounded in a rigorous examination of how the proposed technologies will affect consumer privacy interests.

In this Comment, we provide an overview of consumer data flow in the Smart Grid under several standards identified by NIST for implementation, discuss the privacy risks and legal rules implicated by these technologies, propose a specific framework for further developing privacy protective principles that should be reflected in the technical standards and requirements ultimately recommended by NIST, and call for the rigorous development of relevant use cases that can inform standards bodies and technology design. While our Comment generally addresses the standards proposed in the NIST Draft Framework and Roadmap, 1.0 ("Framework"),[8] we focus specific attention on the discussion of consumer privacy and applicable principles in Chapter Two of NISTIR 7628, "Privacy and the Smart Grid."

## II. Smart Grid Consumer Data Flow and Applicable Standards Identified by NIST for Implementation

### A. Overview

We appreciate NIST's recognition that for customer-to-utility data flow, "the specific data items involved, and associated privacy issues, are very different" from the types of data flows between commercial meters and utilities.[9] In this section, we review and summarize data flow in the Smart Grid that implicates consumer privacy, especially consumer privacy within the home, and that is either presently covered by standards

[7] California Senate Bill 17, http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0001-0050/sb_17_bill_20091011_chaptered.html (signed Oct. 11, 2009).
[8] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Sept. 2009, http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 34.
[9] NIST, *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements*, http://www.nist.gov/smartgrid/, at 11.

identified for implementation by NIST, or available in representative products and services currently on the market. While we cannot be comprehensive, this data flow analysis conveys a basic picture of Smart Grid data flow, as implemented in existing standards and technologies.

Currently, smart meters comprise about 4.7%, or 6.7 million, of all electricity meters in the U.S., and the Department of Energy projects that 52 million more smart meters will be installed by 2012.[10] Using stimulus funds allocated to the modernization of the electrical grid, the Administration recently announced Smart Grid grants of $3.4 billion dollars to fund the implementation of smart meters in 18 million homes.[11] At the same time, manufacturers are working to roll-out "smart" versions of household appliances over the next several years, which will be capable of communicating with smart meters and other appliances, and directly with utilities in some instances.[12] In addition, consumers can purchase and install their own metering devices that monitor energy consumption of a home or an individual device in close to real time.[13]

As widely noted, Smart Grid technologies have the ability to collect far more detailed information about consumers than previous systems. This enhanced access to consumption information promises several benefits: it allows consumers to track their energy use at different times of the day, and enables utilities to implement time-of-use pricing, whereby consumers are charged higher prices for energy during peak demand periods and charged less when energy demand is low. In response, consumers can defer their energy consumption from peak demand periods to a later hour. This "demand response" process improves energy efficiency by reducing peak demand, and at the same time, may reduce consumer's energy bills. [14] Other major benefits of the transition to the Smart Grid, not directly related to consumer information, include reducing greenhouse gases by allowing the efficient use of clean energy sources and enhancing grid defenses against attack and outage.

The increased flow of data related to customers' homes in the Smart Grid exemplifies a paradigm shift from the traditional customer-to-utility data flow. First, the Smart Grid entails much more granular data collection compared to historical practice—all Smart Grid technologies contemplate or actively rely on the collection of energy consumption data at much shorter time intervals than historically collected from household consumers, down to real-time or near real-time. Second, Smart Grid

---

[10] Department of Energy Electricity Advisory Committee, *Smart Grid: Enabler of the New Energy Economy*, http://www.oe.energy.gov/DocumentsandMedia/final-smart-grid-report.pdf, at 14.
[11] Rick Merritt, *U.S. awards $3.4 billion in smart grid grants*, EEtimes.com, http://www.eetimes.com/news/design/showArticle.jhtml?articleID=220900617.
[12] Department of Energy, *Smart Grid System Report*, www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf.
[13] *See, e.g.,* TED 500, http://www.theenergydetective.com/ted-5000-features.html.
[14] Department of Energy Electricity Advisory Committee, *Smart Grid: Enabler of the New Energy Economy*, http://www.oe.energy.gov/DocumentsandMedia/final-smart-grid-report.pdf, at 9.

technologies may allow utilities to collect electricity consumption data for a single, uniquely identified home appliance, while historically, utilities have only collected aggregate electricity consumption data of all appliances within a household. Third, a much greater variety of information is collected by Smart Grid technologies than has been collected by conventional energy services. Utilities may collect not only energy consumption data, but also unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles in the Smart Grid, just to name a few. Finally, third-party entities that will have access to customers' private data, such as Google PowerMeter and Microsoft Hohm, have entered the energy marketplace.

To illustrate these changes, consider Pacific Gas & Electric's ("PG&E") SmartAC program, in which the utility company installs programmable thermostats for consumers' air conditioners, which communicate directly with the utility.[15] PG&E might use the communication channel to display messages on the screen of the thermostat, such as weather warnings, greetings, and system maintenance notices.[16] Consumers can also configure their thermostats on PG&E's website,[17] giving the utility company information about consumers' temperature preference in their homes. It is possible that utilities could use the same communication channel to collect real-time readings on the temperature of consumers' homes, which, if temperature is an indicator of presence, might reveal that residents are not home (e.g., a thermostat is left at 55 degrees in the winter for several days). If a consumer chooses to register other smart appliances or a home area network (HAN) with the utility company in order to enroll in certain utility-sponsored programs, detailed information about those appliances or the HAN could also be collected by the utility.[18] Utilities may remotely turn off consumers' registered devices,[19] or instruct consumers' devices to shed load.[20] Furthermore, if a consumer is interested in using a third-party service to monitor usage, such as a web interface offering a visualization of energy use through a graphical display, the consumer can authorize a provider such as Google PowerMeter to collect smart meter data directly from utilities.[21]

---

[15] PG&E, *SmartAC Frequently Asked Questions: What are the SmartAC technology options?,* http://www.pge.com/myhome/saveenergymoney/energysavingprograms/smartac/faq/.
[16] PG&E, *Honeywell Thermostat Operating Manual*, http://www.pge.com/includes/docs/pdfs/shared/smartac/thermostatuserguide.pdf.
[17] PG&E, *SmartAC Thermostat Programming Website Guide,* http://www.pge.com/includes/docs/pdfs/shared/smartac/pg-wc-7e_webguide_tstat[f]-screen.pdf.
[18] *See, e.g.*, UtilityAMI, *Home Area Network System Requirement Specification, 2.2.10*; Southern California Edison, *SmartConnect Use Cases C5*, http://www.sce.com/NR/rdonlyres/EC46A2AC-9D43-4674-90A7-CBE47F362CDE/0/C5_Use_Case_090105.pdf.
[19] For example, in Florida Power and Light Company's Residential On Call program, the utility company can remotely turn off customers' registered devices at critical times in exchange for a monetary reward to the customers. *See* http://www.fpl.com/residential/savings/oncall.shtml.
[20] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, D.2.2.3, "Load Control Event," at 141.
[21] Google PowerMeter utility partners, http://www.google.org/powermeter/partners.html.

This paradigm shift in data flow undermines key assumptions underlying existing privacy laws and regulations and imposes considerable privacy risks on customers, as we further explore below. Privacy principles developed for the Smart Grid should be grounded in a thorough review of the data flow implicating consumer privacy, including an analysis of how consumer data is being collected, used, and retained by various entities under the standards identified for implementation. We hope the information presented in this Comment may assist NIST in that effort.

### B. Data Flow in Standards Identified by NIST for Implementation

Under the Energy Independence and Security Act (EISA) of 2007, NIST is charged with the responsibility to "coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." In September 2009, NIST published its *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, which identified 31 existing standards that could be implemented in the Smart Grid. Of the standards identified for implementation by NIST, the standards related to demand response and to the Home Area Network (HAN) directly involve demand-side energy management of consumer appliances and implicate consumer privacy issues. As such, we explore some of these standards here: the ZigBee/HomePlug Smart Energy Profile, Open Automated Demand Response (OpenADR), and OpenHAN. [22] We note that this is by no means a comprehensive list of standards that may affect consumer privacy in the Smart Grid—many other aspects of architecture and practice will be relevant, as well. We include these below because of their direct relevance to consumer interaction with the Smart Grid and their obvious implications for privacy.

#### 1. ZigBee/HomePlug Smart Energy Profile

The ZigBee/HomePlug Smart Energy Profile is jointly developed by ZigBee Alliance and HomePlug Powerline Alliance members and was selected by NIST as an interoperable standard for HAN devices and communications. It is created to "further enhance earlier HAN specifications (specifically, the ZigBee Alliance Smart Energy Profile, v 1.0)"[23] and "serves as the basis for a following Technical Requirements Document (TRD), which is the next step in line with creating the actual specification."[24] Although the ZigBee/HomePlug Smart Energy Profile includes a variety of use cases and its Technical Requirements Document is still being developed, important details about its implementation can be gleaned from the ZigBee Alliance Smart Energy Profile

[22] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, 1.0*, at 34.
[23] ZigBee Alliance and the HomePlug Alliance, *ZigBee/HomePlug Smart Energy Profile*, http://www.zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx, at 3.
[24] *Id*. at 1.

Specification, v 1.0, [25] upon which the ZigBee/HomePlug Smart Energy Profile is based. The information below is based on our review of ZigBee Alliance Smart Energy Profile Specification, version 1.0.

A ZigBee Smart Energy network may consist of an Energy Service Portal (ESP), Metering Device, Programmable Communicating Thermostat (PCT), and Smart Appliance Device.[26] The ESP serves as the gateway that connects the utilities' communications network to the consumers' Smart Appliance Devices. The ESP may be installed within a meter, thermostat, In-Premise Display, or as a standalone device. A consumer's devices must join the ZigBee Smart Energy network to communicate with the ESP, other devices on the network, or the utility. Within a ZigBee Smart Energy network, the ESP communicates with customers' devices via encrypted wireless communication.

To join a Smart Appliance Device, such as a washing machine or refrigerator, to a ZigBee Smart Energy network and communicate securely with the ESP of the network, a customer needs to register the Smart Appliance Device with the utility. The registration process requires the customer to provide the utility with the 64-bit device identifier[27] that uniquely identifies the Smart Appliance Device, the first 24 bits of which could uniquely identify the manufacturer of the device.[28] The device identifier is conveyed from the customer to the utility via an out-of-band mechanism such as a telephone call, or web site registration. The utility then uses the device identifier to create keys for secure communication between the ESP and the joining Smart Appliance Device.[29] The device identifier may also be used by the ESP to maintain a list of authorized devices for a particular HAN.[30]

Metering information, including electric, gas, water, and potentially thermal consumption data, of smart devices may be collected by the ESP and potentially revealed to the customer's utility. Metering Devices may be fitted with Smart Appliance Devices, and measure energy usage at the device level.[31] In the design of ZigBee Smart Energy Profile Specification, Metering Devices and Programmable Communicating Thermostats (PCT) are all directly connected to the ESP.[32] Since the ESP is often embedded in smart

---

[25] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, available at http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx
[26] *Id*. at 71-77.
[27] *Id*. at 115.
[28] Wikipedia, Organizationally Unique Identifier, http://en.wikipedia.org/wiki/Organizationally_Unique_Identifier#64bit_Extended_Unique_Identifier_.28EUI-64.29 (last visited Dec. 1, 2009).
[29] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at115.
[30] *Id*. at 56.
[31] *Id*. at 72.
[32] *Id*. at 162-64.

meters that communicate with the utilities,[33] utilities could easily obtain metering information from Metering Devices or PCTs, revealing the energy usage of individual Smart Appliance Devices or the temperature inside customers' homes.

The demand response and load control commands in the ZigBee Smart Energy Profile Specification could reveal the functionality of customers' Smart Appliance Devices. The ZigBee standard defines 12 Device Classes, including water heater, interior/exterior lighting, electric vehicle, and spa.[34] Each Smart Appliance Device is assigned a Device Class by the device manufacturer. In a demand response or load control event, a command from the utility indicates the class of devices needing to participate in the event.[35] The Smart Appliance Device may report event participation in a unique manner as defined by the device manufacturer,[36] or ignore the event if the Device Class of the Smart Appliance Device does not match the Device Class in the command.[37] Therefore, utilities could easily identify the Device Class of a Smart Appliance Device inside a customers' home from the response the utilities receive to demand response and load control commands. For instance, if a utility sends a load control command indicating a customer's water heater needs to "reduce its average load by 10 percent"[38] and receives a response from the customer's ESP confirming participation in the event, the utility could easily tell that the customer has a water heater.

As such, technologies developed under the Zigbee standard could collect and communicate far more detailed information than has been collected in the past, and use of these technologies could result in information about the intimate life of a household leaving the home and being stored outside of it, in utilities' or other providers' systems.

### 2. Open Automated Demand Response (OpenADR)

The Open Automated Demand Response Communication Specification (OpenADR), developed by Lawrence Berkeley National Laboratory, is a communications data model[39] designed to facilitate automating demand response actions at the customer location.[40] OpenADR has been used in over 200 facilities in California[41] and has been

---

[33] PG&E, SDGE and SCE all have HAN gateway embedded in smart meters. *See* Home Area Network (HAN) Overview, Pacific Gas & Electric Company, Jan. 2009, www.edisonfoundation.net/iee/issueBriefs/PG&E_HAN_January_2009.pdf.
[34] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at143.
[35] *Id*. at 148.
[36] *Id*. at 157.
[37] *Id*. at 143 (noting that "if the Device Class and/or Utility Enrolment Group fields don't apply to your End Device, the Load Control Event command is ignored").
[38] *Id*. at 141.
[39] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, at http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at1.
[40] *Id*. at 2.
[41] *Id*. at 6.

identified by NIST as one of the Smart Grid standards available for implementation.[42] In contrast to the ZigBee/HomePlug Smart Energy Profile, which aims to enable "communication between utility companies and everyday household devices,"[43] OpenADR was initially developed to "provide interoperable signals to building and industrial control systems"[44] and is currently used by large businesses in California with centralized energy management systems.[45] However, OpenADR has also been successfully deployed in residential settings[46] and Programmable Communicating Thermostats (PCTs) are being developed to allow residential facilities to participate in OpenADR programs.[47]

In the OpenADR architecture, the Demand Response Automation Server (DRAS) is the intermediary for the communication between the utility and consumer.[48] The DRAS may be a standalone third-party service, or integrated with the utility or consumer's information system.[49] A DRAS Client is a device on the customer's premise that communicates with the DRAS.[50] OpenADR mandates that all public communication interfaces be subject to confidentiality, integrity, authentication and non-repudiation

---

[42] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.*

[43] ZigBee Alliance and the HomePlug Alliance, *ZigBee/HomePlug Smart Energy Profile*, http://www.zigbee.org/Markets/ZigBeeSmartEnergy/ZigBeeSmartEnergyOverview/tabid/431/Default.aspx, at 1.

[44] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf.

[45] *See* Southern California Edison, *Fact Sheet: Automated Demand Response*, http://www.sce.com/NR/rdonlyres/08EBB404-C15D-4FD1-ABBD-E364A82C2A57/0/2008_0201_AutoDRFactSheet.pdf (stating that "Auto DR Program is open to customers with demands equal to or greater than 200 kW who either have an Energy Management System (EMS) that is active or can be reactivated, or are willing to install an EMS"); PG&E, Auto-DR: How it Works, http://70.32.94.23/Auto-DR/pge_how_it_works.html (stating that "Auto-DR is appropriate for many commercial, industrial, and agricultural sites with billed maximum demand of 200 kW or greater").

[46] Tendril, *Tendril Achieves First Open ADR Compliant Platform,* http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/ (stating that "Tendril Residential Energy Ecosystem (TREE) Platform could automatically shed residential loads upon receiving critical peak pricing and real-time pricing messages from an OpenADR compliant server").

[47] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf (stating that "Programmable Communicating Thermostats (PCTs) are currently being developed that in the future may allow small commercial and residential facilities to participate in DR programs"), at APD-56. *See id.* at 3 (stating that the "Demand Response Research Center will also continue to evaluate end-use DR control strategies for homes, large and small commercial buildings, and industrial facilities").

[48] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at14.

[49] *Id.* at 33 (noting "in the architecture…that the DRAS itself is depicted as a standalone service…this is the most general case… [and that] specific incarnations of the DRAS may be integrated within either the utility or participant's IT infrastructure and services"). An example of a DRAS is the Akuacom DRAS, which "accepts DR events and tariff information from utilities and ISO's and turns these into standardized OpenADR signals that are sent to Energy Management Systems (EMS) at participant facilities." Akuacom, Solutions, http://www.akuacom.com/solutions/index.html.

[50] *Id*. at APD-4.

requirements, and has identified a minimum level of cipher suit for DRAS, which includes standards for key exchange, data encryption, message integrity and message authentication.[51] The OpenADR identifies its opt-out functionality as one of its defining features,[52] and requires that customers can opt out of a demand response program at any time.[53]

The OpenADR standard contains seven use cases,[54] and each use case covers three broad scenarios: configuration, execution, and maintenance.[55] For our purposes, we extract one-directional customer-to-DRAS, DRAS-to-utility, and customer-to-utility data flow from the use cases and scenarios.

Customers, or the DRAS Client on a customer's premise, provide the following information to the DRAS:

- Configuration information used to set up a connection with the DRAS, including identification and password of the customer and the DRAS Client, IP connection information, and the customer's contact information.[56]
- Customer's bid for load reduction, if the customer participates in the utility's bidding program.[57] After the customer receives a request for bids from the utility, the customer may submit a bid to the DRAS.[58] Customers may adjust or cancel their current bid.
- Feedback information from the DRAS Client to the DRAS when a demand response or bidding event is executed. The feedback information includes customer ID, near-real-time load, amount of load reduction, and load reduction end uses (e.g. HVAC or lighting).[59]
- Optionally, the load reduction potential of the customer.

The DRAS provides the following information to the utility:

---

[51] *Id*. at 113-116.
[52] *Id*. at 2.
[53] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at 28.
[54] *Id*. at Appendix D.2.
[55] *Id*. at 18.
[56] *Id*. at 25.
[57] OpenADR use cases contains two bidding programs: Demand Bidding Program, which pays an incentive to reduce electric load according to a voluntary bid made for a scheduled load reduction, and Capacity Bidding Program, which pays customer a monthly incentive to reduce load to a pre-determined amount. *Id*. at APD-12, APD-23.
[58] Demand Response Research Center, *CEC OpenADR-Version 1.0 Report*, http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf, at 28 (D.2.2, Demand Bidding Program, APD-15).
[59] *Id.* at 27. *See also* http://openadr.lbl.gov/src/FeedBack.xsd (a formal description of feedback information in XML Schema).

- Customer's standing bid, if the customer participates in the utility's bidding program.[60]
- Feedback information from the DRAS Client.
- Optionally, load reduction potential based upon all customers in program.

The utility also measures customers' electricity usage, but the details of the process are beyond the scope of the OpenADR standard.[61]

Under the OpenADR standard, utilities do not interact directly with customers' HAN devices, but interact with customers' energy management system. This design has three implications: first, to use OpenADR, customers must have their own energy management system that translates demand response signals from utilities to actionable instructions for Home Area Network devices (HAN devices).[62] Second, utilities collect far less information about customer's devices under OpenADR than under the ZigBee Smart Energy Profile Specification. For instance, customers do not need to register their HAN devices with utilities, since the utilities do not directly communicate with customers' HAN devices but with customers' energy management systems. Third, utilities exert less control over customers' HAN devices. For instance, instead of a command instructing customers' water heaters to reduce load by 10%, as is contemplated by the ZigBee Smart Energy Profile Specification,[63] an OpenADR command would only instruct a consumer's energy management system to reduce load[64] and then the consumer's energy management system would decide how to respond.

### 3. OpenHAN

The OpenHAN standard identified by NIST for implementation is the collaboration of more than a dozen investor-owned North American utilities and reflects utilities' view of the Home Area Network. It is a high-level policy statement rather than a requirements document.[65]

Similar to the ZigBee Smart Energy Specification, OpenHAN has use cases in which a HAN device is registered with the utility[66] and communicates with the utility via the Energy Service Interface, which may be embedded in smart meters.[67] In addition, OpenHAN has also included an Energy Management System (EMS) that receives

[60] *Id*. at APD-18.
[61] *Id.* at APD-6.
[62] The Tendril Residential Energy Ecosystem (TREE) Platform may already fulfill this function. *See* Tendril, Tendril Achieves First Open ADR Compliant Platform, Jan. 29, 2009, http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/.
[63] ZigBee Alliance, *ZigBee Smart Energy Profile Specification*, http://www.zigbee.org/DownloadZigBeeTechnicalDocuments/tabid/310/Default.aspx, at B.1.
[64] For a formal specification of commands under OpenADR, see http://openadr.lbl.gov/src/EventInfo.xsd.
[65] UtilityAMI, *OpenHAN System Requirement Specification*, at 9.
[66] *Id*. at 71.
[67] *Id.* at 27.

notification from utilities and controls connected HAN devices.[68] The EMS may be offered by third parties;[69] however, the utility may still require HAN device registration in the Energy Management use case for reliability programs, according to OpenHAN.[70]

### C. Data Flow in Real-World Products

We provide here some background on the role third party service providers are likely to play in the collection and use of consumer energy data in the Smart Grid. These products mainly include third-party web portals, consumer devices and Home Area Network vendors.

Third-party web portals, such as Google PowerMeter and Microsoft Hohm, collect customers' smart meter reading data. Third-party web portals may enter into partnership with utilities, and obtain customers' smart meter reading data from the utilities. The frequency of these readings may depend on customers' utility.[71]

Third-party web portals may also obtain customers' meter reading data from metering devices that customers purchase. For instance, one of Google PowerMeter's device partners, a company called TED (for "The Energy Detective"), uses "clip-on current transformers"[72] that can measure electricity consumption of a home, or an individual device,[73] with accuracy within 2%.[74] The electricity consumption data is collected in real-time and relayed to a customer gateway device via ZigBee wireless communication. The customer gateway device then provides the data to a stand-alone device or computer to be displayed to the customer, or provides the data to Google PowerMeter every 10 minutes if the gateway is connected to the Internet.[75]

Third-party web portals may also solicit customers to provide information about their homes via the web portal. For example, Microsoft Hohm encourages customers to provide detailed information about their home in order for Hohm to make energy-saving recommendations to customers. Information that Hohm solicits includes the heating

---

[68] *Id*. at 62.
[69] *Id*. at 28.
[70] UtilityAMI, *OpenHAN System Requirement Specification,* at 62 (noting that the "use case does not imply the Utility's preferred configuration or communication for reliability programs," meaning that the utility may still require HAN device registration).
[71] Google, *Google PowerMeter Privacy Policy Notice*, at http://www.google.com/powermeter/privacy.
[72] T.E.D., *Which TED Should I Buy?,* http://www.theenergydetective.com/which-ted.html.
[73] T.E.D., *TED 5000 Which TED*, http://www.theenergydetective.com/which-ted.html (stating that the "CTs are designed to be used to measure the entire home, but they can be used to measure an individual circuit just as well").
[74] T.E.D., *TED 5000 Features*, http://www.theenergydetective.com/ted-5000-features.html.
[75] Earth2tech, *Google PowerMeter Bypasses the Smart Meter*, Oct. 5, 2009, http://earth2tech.com/2009/10/05/googles-powermeter-bypasses-the-smart-meter-signs-up-first-gadget-partner/.

system of customer's house, the number of occupants, and materials used for walls and floors.

Although third-party web portals will have access to, store and use highly revealing customer data, they may not be held to the same confidentiality requirement as the utilities from which the third-party web portals obtains the data, as we will further explain in Section III.B.

The market for Home Area Network (HAN) devices and services is still nascent but rapidly evolving. Some vendors offer consumer-oriented devices such as programmable thermostats and in-home displays,[76] while other vendors provide comprehensive solutions to utilities with HAN as a part of the overall solution.[77] For instance, one vendor, Tendril, has developed a system, called Tendril Residential Energy Ecosystem (TREE) that implements the ZigBee Smart Energy Profile.[78] The TREE system includes data management, data transmission and demand response solutions for utilities, as well as a web portal called Vantage that provides utility customers the tools for HAN registration, device management, consumption data monitoring, etc.[79]

## III. Implications of Smart Grid Data Flow for Consumer Privacy

The details of data flow in the Smart Grid, as explored above, provide an important foundation for understanding a range of customer privacy and security issues created by an interconnected digital grid. While the wealth of information collected by Smart Grid technologies provides significant benefits to consumers, it also presents new privacy risks. The unprecedented amount of information collected about customers' energy and appliance use has the potential to reveal intimate details about daily lives and activities inside homes. These risks are compounded by the lack of a clear framework or rules to apply to the new technology landscape, which we discuss below.

### A. Customer Data Concerning Home Activities Presents Privacy Risks That Must Be Addressed

Our review in Section II comprises a partial picture of the great variety of information about customers' homes that is or could be collected by various Smart Grid

[76] For example, ZigBee Smart Energy Certified Products include displays, thermostats, and load controllers. See ZigBee Alliance, Zigbee Smart Energy Certified Products, http://www.zigbee.org/Products/CertifiedProducts/ZigBeeSmartEnergy/tabid/271/Default.aspx.

[77] *See* Presentation of Tendril and Landis+Gyr at Texas Smart Energy Forum, http://www.centerpointenergy.com/services/electricity/buildersanddevelopers/smartmeters/d270d7c7a0f33210VgnVCM10000026a10d0aRCRD/.

[78] Tendril, *The Tendril Residential Energy Ecosystem (TREE) Platform Whitepaper*, http://www.tendrilinc.com/wp-content/uploads/tree-whitepaper-v7.pdf.

[79] Tendril, *Put Your Customers in Control*, http://www.tendrilinc.com/utilities/utility-products/products/vantage/. (Note the image on the upper right corner of the webpage.)

technologies and practices. Such information may include device identifiers that uniquely identify a smart device and the manufacturer, control signals that reveal the function of smart devices, energy consumption at frequent time intervals at both the household and device level, temperature inside customers' home, status of smart devices such as IP address and firmware version, and customers' geographic region.

In addition, with the rapid development of analytical software, consumption data, either taken by itself or combined with other information, may be used to infer even more details about customers' lives inside their homes. For instance, even if energy consumption is not collected for individual appliances, information about energy consumption of individual appliances can be reconstructed from aggregate smart meter reading data of a household by using non-intrusive appliance load monitoring ("NALM") techniques.[80] Researchers can compile libraries of appliance load patterns and match similar patterns in the time series data of overall utility usage records.[81] Research shows that analyzing fifteen-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.[82] As the time intervals between data collection points decreases, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.

The great variety of information about customers' homes being collected or likely to be collected, as well as analysis of that information, gives rise to serious privacy concerns. Home appliance use reflects intimate details of people's lives and their habits and preferences inside their homes. As Justice Scalia recognized in *Kyllo v. United States, "*at what hour each night the lady of the house takes her daily sauna and bath" is "a detail that many would consider 'intimate.'"[83] Some of the activities that might be revealed through the Smart Grid include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, and activities that signal illegal, or simply unorthodox, behavior.[84] As a result, information collected by the Smart Grid is valuable for many purposes other than energy efficiency, most prominently commercial exploitation by advertisers and marketers, access by criminals who wish to peek into homes, and access to household information and surveillance by law enforcement, as discussed further below.

In identifying standards and making recommendations for technology design and service deployment, NIST should consider what uses of this information may emerge that could have an adverse impact on consumers, invading the traditionally protected zone of

---

[80] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at A-1.
[81] *Id*. at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.
[82] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, Feb. 15, 2009, http://ssrn.com/abstract=1370731, at 28.
[83] *Kyllo v. United States*, 533 U.S. 27, 38 (2001).
[84] Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

the home and home life. Without planning, such adverse impacts could drive opposition to the Smart Grid and prompt a backlash against data collection that could be socially beneficial when limited to the narrow purposes of improving efficiency. For example, much of the information collected by the Smart Grid about customers is commercially valuable, and could be resold for a profit. In other contexts, companies have repurposed information in ways that are beyond the bounds of consumer bargaining or expectations.[85]

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be put to especially trangressive purposes. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral targeting products might wish to enhance existing customer profiles with energy usage data revealing customer activities and habits, following a recent trend in the merging of online and offline data sources to support more targeted third-party advertising.[86] As explained in Section II, device identifiers and control signals reveal to the utilities the manufacturers, functionality, and usage of smart devices, which is valuable for the market research and marketing efforts of smart appliances manufacturers and others who wish to target particular demographic groups. Data brokers, advertisers, marketing research firms, and others might also find this type of detailed information about customer habits attractive.

Criminals might also seek access to smart meter reading data or other information collected by the Smart Grid, in hopes of using this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future attacks. If personally-identifying information accumulated by the Smart Grid is accessible to computer hackers or to "war drivers" monitoring a wireless network, the information could also be used by criminals to commit identity theft, especially when utilities or other providers use unsecured paths to transmit data. For instance, many businesses and others traditionally use energy

[85] There are many examples of this phenomenon, but recent examples include employers and insurance companies using information posted on social networking services to screen employees and to deny insurance claims. *See* Michal Czerwonka, *Facebook Page Costs Woman Her Benefits*, Wall St. Journal, Nov. 24, 2009, http://online.wsj.com/article/SB10001424052748704779704574554380064654604.html; BNA Privacy & Security Law Report, *Employment Issues: Court OKs Verdict Against Restaurant For Managers' Access of MySpace Account*, 8 PVLR 1474.

[86] For more about recent trends in data aggregation and the development of enhanced customer profiles for advertising purposes, see CDT, *CDT's Guide to Behavioral Advertising*, http://cdt.org/privacy/targeting/.

consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account.[87] Threats to customer data security are compounded if the data transmission within Smart Grid networks is not encrypted, in which case criminals may be able to easily intercept Smart Grid transmissions and acquire the content of communications.

For a variety of reasons, law enforcement officials may also be interested in the fine-grained data about household habits collected by the Smart Grid. As part of their investigatory work to solve crimes, officials may want to establish or confirm residence at an address at a certain critical time, and this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat. Law enforcement may also be interested in data collected by the Smart Grid that indicates illegal or other activities at home. For instance, access to smart meter reading data might be used in drug investigations, to enable law enforcement to learn about a suspect's marijuana growing cycle.[88] The data from Smart Grid technologies certainly may be highly useful for these purposes. At the same time, the privacy implications of law enforcement officials' interest in obtaining smart meter data suggest the need for strong Fourth Amendment procedural protections for this information, as well as careful procedures on the part of utilities and other providers, and technology design that allows for strong data protection. Already, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household.[89] Procedural safeguards may be especially important in light of the fact that Smart Grid data held by third parties as business records may not be subject to the same protections applicable to information kept within the home.[90]

### B. Longstanding Special Protections for Information about the Home and Home Life, Combined with the Lack of Clear, Consistent Rules for the Smart Grid, Highlight Privacy Risks and Create a Strong Need for Privacy Protections to Be Included in Technological Design and Service Provider Practices

Under longstanding U.S. constitutional values and law, activities occurring within the sanctity of individuals' homes, because of their inherently personal nature, have been

---

[87] For instance, San Diego Gas and Electric (SDGE) uses the amount of the last SDGE bill to authenticate its customers when the customers sign up for an online account. *See* SDGE*, My Account*, https://myaccount.sdge.com/myAccountUserManager/pageflows/usermanager/Registration/begin.do.

[88] P.S. Subrahamanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, and Jack Lerner, CyberKnowledge and University of California at Berkeley, *Network Security Architecture for Demand Response/Sensor Networks*, June 2006, http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf (under 3.2.4, Law Enforcement Practices) (hereinafter "Berkeley/CyberKnowledge Report").

[89] Channel10 San Diego News, *High Electric Bill Leads To Calif. Police Raid*, March 28, 2004.

[90] *See* Jack I. Lerner and Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3.

afforded special protection from intrusion by others.[91] The Supreme Court recently affirmed this strong protection for all types of data found in the home, noting in *Kyllo v. United States* that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained…in the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[92] In *Kyllo*, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement.[93] Data collected via Smart Grid technologies are similarly revealing of the intimate details of home life, and should be subject to similarly high levels of protection.

At the same time, the customer data collected and used in the Smart Grid is governed by a patchwork of broad state and federal laws that may be generally applicable, but those often neither specifically address the electrical grid nor were developed with Smart Grid technological advancements or business models in mind. In addition, at present, there is no federal customer privacy law in the U.S. that might generally cover commercial activities related to Smart Grid information.

We appreciate NIST's recognition that a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a privacy risk that needs to be addressed."[94] Rather than falling under a comprehensive single law, the Smart Grid intersects with a number of different federal and state rules regarding the privacy of activities occurring within the home, the handling of business records and identifiable customer information, the privacy of electronic communications, and access to computer systems.[95] Neither in isolation nor taken together do these existing laws provide adequate protection for the categories and quantities of data that may be generated by the Smart Grid. As such, technology design and utility and third-party service provider practices must be carefully considered and rigorously implemented in order to protect customer privacy and security.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on consumer energy data. [96] In some states, utilities may provide competitive suppliers access to

---

[91] *Id*.
[92] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).
[93] *Id*. at 40.
[94] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, Sept. 2009, http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 84.
[95] Berkeley/CyberKnowledge Report at 23.
[96] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at 24.

customer energy data without the ratepayer's affirmative consent.[97] While other state public utility codes place explicit restrictions on the sharing of customers' personal information, these rules contain some regulatory uncertainty as to their coverage of some types of Smart Grid data.[98] And generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data.[99] General state laws governing business' and third parties' collection and use of customers' personal data may apply to energy usage, but may be too narrow to cover the extensive and varied information generated by the Smart Grid, or the increasing number of entities that have access to the information. For example, California Public Utility Code §394.4 imposes a general requirement on electric service providers to ensure confidentiality of customer information,[100] However, the emergence of third-party service providers such as Google PowerMeter and Microsoft Hohm means that new entities have access to customers' private data, but likely stand outside the statutory confidentiality requirement because they are not "electric service providers" under California law.[101] Furthermore, new types of information, such as the unique identifiers of smart devices collected by the utilities, create uncertainties about whether current privacy law could be extended to these new types of information.[102] It is also important to note that California has a relatively protective regime for personal data and other states' privacy regulations may vary greatly in terms of the rules governing utilities and third party service providers.[103]

At the federal level, there is a similar patchwork of rules, which provides even less directly relevant guidance on the privacy protections applicable to the Smart Grid. The *Electronic Communications Privacy Act* (ECPA) sets out limitations on the interception of electronic communications and has been broadly applied to a range of communications systems. However, one of the greatest privacy concerns for consumers is

---

[97] Before the Federal Communications Commission in the Matter of International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act, *Comments of the Edison Electric Institute*, GN Docket No. 09-47, Oct. 2, 2009, at 28.

[98] *See* Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, available at SSRN: http://ssrn.com/abstract=1462285, at 17-22.

[99] For example, the National Association of Regulatory Utility Commissioners (NARUC) will consider a resolution in 2010 that would encourage member states to support several regulatory protections on consumer data collected in the Smart Grid. *Draft Resolutions Proposed for Consideration at the 2009 Annual Convention of NARUC*, submitted Nov. 5, 2009, http://annual.narucmeetings.org/09_1106_Proposed_Resolutions.pdf, at 14-17. *See also* NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, Sept. 2009, http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf, at 84.

[100] California Public Utility Code §394.4 ("Confidentiality: Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information").

[101] For a list of electric service providers registered with the California Public Utilities Commission, see http://docs.cpuc.ca.gov/published/ESP_Lists/esp_udc.htm.

[102] For example, California Penal Code §1326.1.(a) requires that law enforcement should show specific and articulable facts before accessing "utility records," which includes billing and payment information but may or may not include customers' device identifiers under California law.

[103] *See* Andrew B. Serwin, *Information Security and Privacy: A Practical Guide to Federal, State and International Law*, § 28:28 – 44 (2009) (providing an outline of California privacy protections).

what the utilities will do with information they receive from their customers, and ECPA places no limit on that. The FCC's Customer Proprietary Network Information (CPNI) Rules, which require telecommunications carriers to obtain customers' opt-in before using, disclosing, or permitting access to individually identifiable customer information, do not necessarily directly bear on the privacy issues surrounding a Smart Grid information network.[104] However, as the transmission of Smart Grid services grows increasingly complex and more communications-based, utilities may find themselves subject to laws governing telecommunications providers, meaning they would be bound by some privacy protections on data related to their service.[105] The *Computer Fraud and Abuse Act* (CFAA), which governs unauthorized access to computer systems, may also be relevant, under a broad construction, to regulate invasions of the Smart Grid. Unauthorized access to obtain information from or cause damage to devices like smart meters, wireless sensors, smart appliances, and a customer's home computing system might generate liability under an expansive reading of the CFAA.[106] Finally, the Federal Trade Commission (FTC) likely has general jurisdiction under Section Five of the FTC Act to pursue actions against Smart Grid entities engaging in "unfair and deceptive trade practices," such as, for example, failing to adopt, disclose, or adhere to reasonable privacy and security practices.[107]

This brief and introductory discussion of the rules possibly applicable to Smart Grid technologies reveals the disjointed and outdated nature of current customer protections for energy data. Industry lacks a clear set of privacy guidelines to govern Smart Grid technologies. In light of the legal patchwork, we are especially in need of a cohesive approach that reflects the realities of an interconnected and digitized electricity grid in which customers are active contributors of personal data. As further explored below, we encourage NIST to include in its Framework comprehensive privacy principles against which technical standards can be evaluated to ensure that both Smart Grid technologies and service providers are sufficiently protective of consumer privacy.

## IV. Proposed Framework for NIST Privacy Principles

The discussion of unique risks to privacy presented by the Smart Grid, and the present lack of comprehensive legal rules mitigating those risks, reveals the need to develop strong design and business practice mechanisms for protecting consumer privacy in the modernized grid. In the following section, we lay out the necessary elements for developing a comprehensive framework to protect privacy in the Smart Grid, including who should be covered, what types of data should be included, and how principles can

---

[104] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, May 9, 2009, http://ssrn.com/abstract=1462285, at 25-26.
[105] Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems,* SmartGridNews.com, July 1, 2008.
[106] 18 U.S.C. § 1030; *See also* Berkeley/CyberKnowledge Report at 28.
[107] *See* Mark Foley, *Data Privacy and Security Issues for Advanced Metering Systems*, SmartGridNews.com, July 1, 2008.

ensure the fullest protections for consumers' Household Energy Data. All of the technical standards identified by NIST for implementation in the Smart Grid should be evaluated against these principles, and ultimately, the Framework for standards and requirements released by NIST should reflect these principles.

### A. Privacy Principles Should Cover All Smart Grid Entities and Practices

Ensuring that the full range of companies touching consumer data in the Smart Grid are covered by any privacy protections is critically important. In the current NIST Draft, the examination of privacy risks and potential safeguards in Chapter Two focuses too narrowly on "consumer-to-utility" data flows.[108] Instead, the activities of utility companies, third party service providers, such as Microsoft and Google, and device manufacturers, such as General Electric and Honeywell, in collecting, using, and storing consumer data should all be considered, and technical standards should be evaluated in light of known business practices and service models in addition to technology capabilities. Privacy principles should not subject different entities to a different set of rules where the entities are similarly interacting with consumer data. Furthermore, recognizing this universe of participants now is important in fully incorporating "privacy by design" into the applicable standards and technologies underlying the Smart Grid.

In performing an evaluation of the proposed standards, a well-developed set of use cases explaining how privacy principles should be built into the Smart Grid will be important in ensuring the full implementation of consumer privacy protections. For the final Framework, NIST should develop use cases that reflect a comprehensive model of data flow, covering all entities and activities, and detail the necessary consumer privacy protections which should be required in all Smart Grid standards and technical requirements.

### B. Privacy Principles Should Cover "Household Energy Data"

Designing an effective framework to protect consumer data also requires specific consideration of what information requires protection. As drafted, the privacy principles in the NIST Draft are built upon the model of "personally identifiable information" ("PII"), including the "notice and purpose for PII use," "collection of PII," and the "use and retention of PII."[109] In the context of the Smart Grid, however, the privacy assessment of consumer data practices must extend beyond traditional notions of PII, which has a longstanding history of special legal consideration for its ability to directly identify an individual, such as a name, address, email address, or phone number. Certainly some of the data collected by utilities and third party service providers in the Smart Grid, such as name and address for billing purposes, would be considered PII

[108] NIST, *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements*, at 8.
[109] *Id*. at 12.

under traditional definitions. But based on the discussion of consumer data flow described above in Section II, it is clear that some data collected and used in the Smart Grid extends beyond traditional PII, yet is very revealing of traditionally protected household activities and intimate home life.

As such, we recommend that NIST adopt privacy principles that cover a somewhat broader set of intimate information: "**Household Energy Data**." Household Energy Data includes: any consumption or device data capable of revealing personal or household information that is not aggregated over long periods of time or over a large number of ratepayers.[110] Specifically, Household Energy Data includes both:

(a) traditional PII, such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information; and

(b) data collected about an individual household in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of Household Energy Data include: near real-time energy usage data, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering data (e.g. thermostat temperature).

Sometimes information in the second category will be personally identifiable when combined with other types of information, or when the number of people in a household is small, while sometimes it is unlikely to identify individual members of a household, at all. Regardless of whether it is identifiable, however, it is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. While not all Household Energy Data may uniquely identify an individual in a multi-person household, it can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising the serious privacy issues explored above. Further, given that 32.2 million people live alone in the U.S and twenty eight percent of American households have single-person occupancy,[111] Household Energy Data is revealing of individual activity for a significant number of Americans.

Examples of data not covered by "Household Energy Data" include usage records aggregated in 30-day increments—what is collected now through monthly metering readings—and other types of data aggregated across a large number of

[110] Utilities may generally refer to information of this type as "customer usage information," which may also be an appropriate term provided it includes the elements detailed above. *See* utilities' comments in a recent CPUC rulemaking, California Public Utility Commission, Proposed Decision of Commissioner Chong, Agenda ID #9052, Nov. 17, 2009, http://docs.cpuc.ca.gov/efile/PD/109890.pdf.

[111] U.S. Census Bureau, *Facts for Features: Unmarried and Single Americans Week*, July 21, 2009, http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/014004.html.

households. While still needing some safeguards, such data likely does not require the full scope of protections outlined here.

We also note that this working definition of Household Energy Data, and the following discussion of a privacy framework to protect this data, is intended to be a baseline for the least revealing information included within the definition. Some of the information included within the set of "Household Energy Data," such as PII and location-identifying information will likely require additional protections. The principles discussed here for Household Energy Data outline the minimum protections required for this basic category of data.

### C. Privacy Principles for Household Energy Data Should be Grounded in Comprehensive Fair Information Practice Principles (FIPPs)

Here, we consider the larger question of how to protect the Household Energy Data collected and used in the Smart Grid. Properly formulated and rigorously implemented **Fair Information Practice Principles ("FIPPs"**) provide a broad, comprehensive privacy framework that should underlie privacy standards for the Smart Grid. We urge NIST to adopt appropriately formulated FIPPs as the basis for its consumer privacy recommendations. While we appreciate the Cyber Security Coordination Task Group's (CSCTG) effort to consider a set of rules extending beyond notice and consent, the privacy principles as drafted need considerably more specificity and organization. Given the broad acceptance of FIPPs by national and international privacy regulators, the fact that they have been applied in many contexts related to consumer privacy, and the fact that the lesser-known Generally Accepted Privacy Principles (GAPP) cited in the NIST Draft are grounded in FIPPs, it is most sensible to revise the Draft's privacy principles to more fully reflect FIPPs.

In particular, the technical standards and requirements ultimately recommended by NIST should incorporate FIPPs, and should recommend that relevant technologies be designed to have the capacity to implement FIPPs, and to interoperate based upon them, enabling "privacy by design." While various versions of FIPPs are used by different regulatory bodies, we consider here, and recommend for adoption, the articulation of FIPPs in the Department of Homeland Security's (DHS) 2008 Privacy Policy memorandum. Compared to prior versions of FIPPs, that sometimes provided vague, incomplete, and generally weakened privacy protections,[112] the DHS framework is the U.S.-based framework that most closely follows strong international interpretations of FIPPs. It provides a robust set of modernized principles that NIST should apply to all entities collecting consumer data in the Smart Grid. These principles include:

[112] For an expansion of this critique, see CDT, *Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable*, Nov. 6, 2009, http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf, at 6-7.

1. **Transparency**: Smart Grid entities should be transparent and should provide meaningful, clear, full notice to the individual regarding the collection, use, dissemination, and maintenance of Household Energy Data.

Relevant information about the collection, use, dissemination and maintenance of Household Energy Data must be shared with the consumer. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. For example, device manufacturers should clearly provide notice of any transfer of data, such as device status being transmitted from the device to the manufacturer, which might occur with the consumer's use of a device. Further, Smart Grid entities, including utilities, third-party service providers, and device manufacturers, should also provide consumers with access to the personally identifying information collected about them, as well as Household Energy Data collected about their homes.

2. **Individual Participation**: Entities should involve the individual in the process when using energy information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of Household Energy Data. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of Household Energy Data.

The NIST draft recognizes that "new smart meters create the need for utilities to give residents a choice about the types of data *collected*,"[113] but consumer choice must also extend to the *use, transfer, and maintenance, including retention,* of Household Energy Data. To fully recognize the principle of individual participation, Smart Grid entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Initially, consumers should be required to opt in to the collection and use of Household Energy Data for any secondary purposes beyond what is strictly required for the provision of service. Without affirmative consent by the consumer, any use of data by utilities or third party service providers should be limited to purposes related to the original mission of the service or application. The opt-in consent should allow the consumer to exercise a genuine choice, meaning that it does not present high practical barriers or costs if the consumer chooses not to opt in.

In the case of utilities, this means that opt-in consent would be required for a utility to use Household Energy Data for delivering advertisements to its customers, which is clearly unrelated to the primary purpose of providing energy service. A third

[113] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12 (emphasis added).

party service provider's use of device identifiers for marketing purposes is another example of using data for a secondary purpose. As explored further in the Use Limitation principle, NIST should develop use cases that provide specific guidance on what constitutes acceptable primary and secondary purposes of data use in the Smart Grid.

Informed consumer consent should also be affirmatively required for any access to or transfer of Household Energy Data to or by third party service providers. At all points, consumers should have reasonable access to the Household Energy Data that utilities or third-party service providers are collecting and using, with mechanisms available to correct data where it contains inaccuracies and to actively manage secondary uses. There should also be parity in enrollment and any opt-out/opt-in mechanisms. That is, if an individual or household can enroll in data sharing online, they should also be able to cancel that sharing and exercise other choices about their data through the online mechanism.

3. **Purpose Specification**: Companies should specifically articulate the purpose or purposes for which Household Energy Data will be used.

The specification of purpose should fully describe both primary purposes of data use by the utility or service provider, and any secondary purposes, as described above. Consumers should be provided with this information about how their data will be used *before* the time of collection by service providers. The NIST Draft allows for disclosure "at the time of collection,"[114] but that may not provide consumers with the necessary opportunity for individual participation, which includes sufficient opportunity to separately opt in to any use of their Household Energy Data for secondary purposes.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that "Household Energy Data" will be used for the primary purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. A third-party service provider offering consumers an online interface for monitoring energy consumption may specify that Household Energy Data will be used to target product advertisements to the consumers (which, again, is likely the use of consumer data for a secondary purpose, requiring affirmative, additional consent). If the utility later changes the purpose for which the Household Energy Data is used, consumers should also opt in to that new use.

4. **Data Minimization**: Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as necessary to fulfill the specified purpose.

Generally, Smart Grid technical standards should support, and technologies

[114] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

should be capable of, appropriate data minimization. In the context of the utility, the Data Minimization principle means that utilities' collection of data for the primary purpose of providing energy use should be limited to that information necessary for billing, load management and some demand response programs—information that is "directly relevant and necessary" to the provision of the primary service. As the NIST Draft importantly notes, "only the minimum amount of data necessary for utility companies to use for energy management and billing should be collected."[115] Further explanation of the specific types of information necessary for utilities to perform these functions in a data minimizing manner should be detailed in the set of use cases developed by NIST, as suggested above. At the outset, we note that it is unlikely the utilities need to collect information about the functioning of individual appliances, or even individual houses, to implement load management or demand response programs.

Centralizing the collection and usage of Household Energy Data at the Smart Meter level would also enable such minimization. As smart meters become capable of more sophisticated computation, they should be engineered so that it is possible to aggregate the collection, use, and storage of private data at the point of consumption. Such a meter would aggregate and anonymize usage records over both time sequence and type of appliance so as to report only relevant abstractions of data such to the utility. It would also enable consumers to have their smart devices communicate securely with the HAN or other gateway without revealing the details of their smart devices, or the time of use, to the utility.[116] Designing smart meters and other devices to preserve privacy by default enables households to fully participate in the decision to share their Household Energy Data outside of the home. Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed earlier.

While there are some likely consumer advantages tied to sending Household Energy Data to the utility (e.g. a utility may offer price discounts for consumers who share data beneficial for load research), our initial research suggests that the efficiency benefits of the Smart Grid can be realized without centralizing all control of Household Energy Data at the utility. Existing meters should be updated where possible within technological constraints, and new meters should be designed, so that consumers can choose to minimize the sharing of Household Energy Data with utilities or third-party service providers. Meters with sufficient processing and storage capacity to manage demand response pricing within the home are not currently being widely marketed, but advanced smart meters such as Itron's OpenWay CENTRON meter, which has the capability for performing complex usage calculations and storing large quantities of data, already reveal that smart meters can allow for data minimization while still enabling the

[115] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

[116] Note that in the ZigBee Smart Energy Profile, customers must reveal details of their smart device to utilities in order to register and authenticate their smart devices with a home area network. An alternative design may not require so much detail about customers' smart devices in its implementation of the same function.

benefits of the Smart Grid. Where Smart Meters are already being installed without any capability for data minimization,[117] NIST should adopt technical recommendations that provide for this option, especially since devices already in the field can be updated remotely.

Applying the data minimization principle to utilities also means that current retention periods for customer records, which currently widely reflect the industry standard of seven years,[118] should be revised in light of the Smart Grid transition and attendant collection of Household Energy Data. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to the utilities in terms of decreased storage and maintenance costs.[119]

Applying this principle to third party services providing consumers with web-based visual representations of home energy use, such as MS Hohm, suggests that those service providers should not collect appliance-level device identifiers (unless a purpose such as consumer marketing was specified to the consumer and opt-in consent was obtained prior to the use, per the principle above). Third party service providers should also enable consumers with the choice to end service and terminate their accounts, including the prompt deletion of any Household Energy Data retained by the utility.

5. **Use Limitation**: Household Energy Data should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected.

In the case of a utility collecting Household Energy Data for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the utility to entities with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an opt-in regime, as detailed above. For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a utility or third party service provider, unless such use was specified to the consumer, who specifically opted in to the purpose. Similarly, third party service providers should not use Household Energy Data

[117] Utilities have already begun to deploy Smart Meters to customers. In Northern California, PG&E's Smart Meter implementation has generated controversy among customers complaining of higher bills and prompted a class-action suit. *See* Andrew Koskey, *Smart Meters Come Under Fire*, San Francisco Examiner, Nov. 26, 2009, http://www.sfexaminer.com/local/Smart-meters-come-under-fire-73831897.html.
[118] Berkeley/CyberKnowledge Report.
[119] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), http://epic.org/reports/dmfprivacy.html.

for behavioral advertising or other marketing purposes when the primary purpose of the data collection and use specified to the user was more limited.

6. **Data Quality and Integrity**: Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Utilities and other entities handling Household Energy Data, including third-party service providers, should provide consumers with tools to correct mistakes or challenge information provided in profiles.

The NIST Draft importantly noted this need to allow consumers to review and correct, where necessary, their information. Standards and technical requirements implemented by utilities and third party service providers, for example, should allow for easily-accessible interfaces which give consumers the opportunity to review and correct their Household Energy Data. This review provides the best means of ensuring that consumer data is accurate, which is particularly important given companies' data retention and transfer practices.

7. **Security**: Companies must protect Household Energy Data through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards. Reasonable security in the Smart Grid requires that any transmission of Household Energy Data must be secure and that data practices by utilities and other providers include meaningful safeguards for Household Energy Data.

For example, if a communication is sent over an open wireless connection, or could otherwise be intercepted with reasonable or targeted efforts, encryption should be required, for both organization-owned infrastructure and third-party communication services. More broadly, technical standards identified by NIST for implementation should be reviewed and, if necessary, revised to require that smart-device communications provided by either utilities or third-party service providers are truly secure, prior to any recommendations being made. For example, contrary to the Draft's requirement that "[d]emand response HAN devices must be securely authenticated to the HAN gateway and vice versa,"[120] both OpenHAN and ZigBee standards presently identified as NIST standards for implementation include scenarios (in the provided background context for relevant use cases) in which smart devices respond to open radio signals to provide demand response capabilities.[121] NIST should recommend that these standards be revised, as unauthenticated HAN devices responding to open, unencrypted signals pose a clear security risk for consumers.

[120] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at Appendix D, D.10.
[121] *See* UtilityAMI, *OpenHAN System Requirements Specification*, at 27; ZigBee Alliance*, ZigBee Smart Energy Profile Specification*, at 189.

Further, Household Energy Data collected, used and maintained by utilities or other service providers must be stored securely, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of Household Energy Data, affected customers should be notified and all reasonable steps should be taken to minimize harm to customers.

8. **Accountability and Auditing**: Companies should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use Household Energy Data and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements.

NIST's current draft recognizes the importance of this principle in stating that "documented requirements for regular privacy training and ongoing awareness activities for all utilities, vendors, and other entities with management responsibilities throughout the Smart Grid should be created and implemented, and compliance enforced."[122] As discussed above, an important means of ensuring widespread implementation of the full set of FIPPs is to develop rigorous, comprehensive use cases that reflect a comprehensive model of data flow as well as these principles, and that inform the development of specific privacy requirements against which companies can audit for compliance purposes. In expanding the next iteration of the Draft, and specifically in further developing the Privacy chapter, the CSCTG should develop or collect these use cases.

The CSCTG should also consider outlining an accountability mechanism, such as a certification programs for Smart Grid technologies and third-party services, to measure adherence to privacy principles grounded in FIPPs. Such a certification program could be helpful in establishing an industry standard for data practices by utilities or other providers that provides meaningful safeguards for the Household Energy Data. In developing such a program, California's experience in certifying meters could be instructive.[123]

## V. General Recommendations

As the exemplified in the prior discussion, crafting a comprehensive privacy framework for the Smart Grid is a complex task requiring the careful examination of

---

[122] NIST, *NIST Draft NIST Interagency Report (NISTIR) 7628*, at 12.

[123] California adopted permanent standards for meters in California Public Utility Commission (CPUC) Decision No. 98-12-080, http://www.cpuc.ca.gov/PUC/energy/Retail+Electric+Markets+and+Finance/Electric+Markets/Metering/msp_info.htm, http://www.cpuc.ca.gov/PUC/energy/Retail+Electric+Markets+and+Finance/Electric+Markets/Metering/mp_process.htm. Meter manufacturers could "self-certify" their meter products by submitting a self-certification form to CPUC, stating that the meter meets the standards for certification, subject to the review and approval of CPUC.

rapidly evolving technology and business models. While well-developed tools, such as the robust articulation of FIPPs outlined here, can be quite helpful in creating privacy principles for the Smart Grid, more work must be done to apply these guidelines to modernized Grid technologies and specifically to the full set of NIST recommended standards and technical requirements that will emerge from the standards-setting process. As a priority for future work, we recommend that the CSCTG devote energy to developing a specific set of uses cases that reflect a comprehensive model of consumer data flow related to Smart Grid technologies and services and that are informed by the FIPPs-based framework set forth above. In addition to helping companies in the auditing process, as described above, developing a rigorous set of uses cases now will provide an important mechanism for identifying further changes that need to be made to the proposed standards to protect consumer privacy, and for evaluating where additional standards may need to be created.

Finally, fully addressing the implications of utilities and third-party application providers' greatly enhanced collection and use of Household Energy Data in the Smart Grid may require more time than has been allocated in the current process. While we understand the tremendous interest in accelerating the deployment of Smart Grid technologies, we also strongly support NIST's observation in the Framework and Roadmap, 1.0 that the development process "must be systematic, not ad hoc."[124] While it is certainly true that "[l]egal and regulatory frameworks can be further harmonized and updated as the Smart Grid becomes more pervasive,"[125] it is critical to develop a full, carefully considered privacy assessment now, so that the applicable standards are crafted in a way that protects consumer privacy. We suggest that the timeline for CSCTG's work be considered, and readjusted if needed, to ensure there is sufficient opportunity for a full review of these issues, including the development of the privacy use cases described above. This may require that NIST extend the target date for the completion of the final Draft.

## VI. Conclusion

We greatly appreciate NIST's attention to consumer privacy in the Smart Grid, and encourage the prioritization of these important issues in further work to finalize the Cyber Security Strategy and Requirements document and Framework. As noted earlier, we are at a critical point in the deployment of new Smart Grid technologies, necessitating immediate attention to consumer privacy and security risks. Failure to ensure adequate consumer protections in NIST's recommended standards and technical requirements for the Smart Grid could encourage the development of technologies and services that do not adequately protect privacy within the intimate realm of the home, undermining consumer confidence in these promising new technologies. By adopting robust privacy principles

[124] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Sept. 2009, at 22.
[125] *Id.* at 84.

that recognize the sensitive nature of Household Energy Data and ensuring the implementation of these principles in its technical standards, NIST can provide much-needed guidance to the energy community about how best to safeguard consumers while still realizing the promise of the Smart Grid.

We look forward to providing any further information that may be useful.

Respectfully submitted,

Jennifer M. Urban
Elizabeth Eraker
Longhao Wang

Samuelson Law, Technology and Public Policy Clinic, University of California, Berkeley School of Law
585 Simon Hall
UC Berkeley School of Law
Berkeley, CA 94720
(510) 642-7338

on behalf of the Center for Democracy & Technology

December 1, 2009

**Participatory Sensing and New Challenges to U.S. Privacy Policy**

*Katie Shilton, Deborah Estrin, UCLA CENS*

Mobile phones have created a radical new platform for data collection, discovery, and social analysis. At the same time, they fundamentally challenge our current understandings of privacy policy and data security. Mobile phones place calls, surf the Internet, and there are close to 4 billion of them in the world. Their built-in microphones, cameras, and location awareness can collect images, sound, and GPS data. Mobile phones are more often on and carried than any previous personal technology, and because they are connected to location services and the web, they can use a wealth of web-based data as context. Participatory sensing (PS) is a new practice which harnesses these tools to collect and analyze data for use in social science, environmental and health discovery.

Participatory sensing shapes phones into ubiquitous, familiar tools for quantifying personal patterns and habits. Phones become platforms for thousands to document a neighborhood, gather evidence to make a case, or study mobility and health (Anokwa, Borriello, Pering, & Want, 2007; Burke et al., 2006; Eisenman et al., 2006; Miluzzo, Lane, Eisenman, & Campbell, 2007; Pentland, Lazer, Brewer, & Heibeck, 2009). In addition, phones can be programmed for manual, automatic, and context-aware data capture. Because of the sheer ubiquity of mobile phones and associated communication infrastructure, it is possible to engage people of all backgrounds nearly everywhere in the world and collectively, provide unprecedented access to high resolution, real time, and scalable spatio-temporal data.

An infrastructure to collect, coordinate and analyze these data will enable researchers to conduct studies at individual, community, and population scales; research that addresses socially critical issues related to human behavior, sustainability, health, and education. However, a significant barrier to adoption of this technology is the need for careful attention to the privacy issues and data practices surrounding these very personal and intimate data. The issue is particularly challenging because of the multiple stakeholders involved in these systems: in particular, end-users (participants in studies), researchers designing and conducting studies, and mobile carriers and application developers who collect, warehouse, and distribute participatory sensing data.

*Participatory sensing*

Participatory sensing is meant to enable (and encourage) anyone to gather and investigate previously invisible data. It tries to avoid surveillance or coercive sensing by emphasizing individuals' participation in the sensing process. Applications designed to enable participatory sensing range from the very personal and self-reflective to shareable data meant to improve an individual's health or a community's experience. As examples, we present three applications from UCLA's Center for Embedded Networked Sensing to illustrate the diversity of possibilities, as well as suggest data collection and sharing concerns.

**PEIR** (Personal Environmental Impact Report). Participants in PEIR (http://peir.cens.ucla.edu/) carry mobile phones throughout their day to calculate their carbon footprints and exposure to air pollution. By referencing GPS and cell towers, the phones upload participants' locations every few seconds. Based on these time-location traces, the PEIR system infers participant activities (indoors, walking, driving) throughout the day. The system maps the combination of location, time, and activity to Southern California regional air quality and weather data to estimate individual carbon footprint and exposure to particulate matter. Sensing a participant's location throughout the day enables more accurate and previously unavailable information about environmental harms people face, as well as the harms they create. To participate, individuals need to record and submit a continuous location trace.

**Biketastic.** This project (http://biketastic.com) improves bike commuting in Los Angeles, a city notoriously unfriendly to cyclists. Bikers carry a GPS-enabled mobile phone during their commutes. The phone automatically uploads bikers' routes to a public Web site. The phone also uses its accelerometer to document the roughness of the road, and takes audio samples to analyze volume of noise along the route. Participants can log in to see their routes combined with existing data, including air quality, time-sensitive traffic conditions, and traffic accidents. They can also use the system to share information about their routes with other riders. By combining existing local conditions with biker-contributed data, Biketastic will enable area bikers to plan routes with the least probability of traffic accidents; with the best air quality; or according to personal preferences, such as road-surface quality or connections with public transportation. Biketastic shares location data through a public map, though individuals use pseudonymous user names.

**AndWellness.** AndWellness is a personal monitoring tool designed to help individuals manage health conditions. AndWellness phones are programmed to prompt the user for quick input at 'appropriate times and places' during the course of their day, wherever they are. These "experience samples" are automatically time stamped, geocoded, uploaded, and stored in a database according to the prompt and the response details. Patients with conditions such as diabetes, who are struggling to stabilize their hypertension, can record frequent physiological measures (BP, BG, weight), and timing/dosage of medication. They can also document in-the-moment self-reports on physical symptoms and side effects such as dizziness and fatigue. Such data can help the clinician and patient build a picture over a week or two to inform personalization of the care plan. In addition to giving the clinician the information they need to optimize the patient's care plan, the same systems can be used to help patients with desired health-behavior changes--the notion of a personal-coach in your pocket--whether the behavior of interest is smoking, diet, prenatal care, or parenting. In order to fulfill this vision, AndWellness collects not only location, but also sensitive data about diet and habits. Individuals might choose to share this data with a support group, coach, therapist, doctor, family, or friends.

Taking participatory sensing from a possibility enabled by the mobile-phone network to a coordinated reality is rife with challenges. Among these challenges are the ethics of repurposing phones, now used as communication tools, for data collection and sharing. How can individuals determine when, where, and how they wish to participate? How much say do they get over what they wish to document and share?

*Privacy in Participatory Sensing*

Privacy—the ability to understand, choose, and control what personal information you share, with whom and for how long—is a huge challenge for participatory sensing. Privacy decisions have many components, including identity (who is asking for the data?), granularity (how much does the data reveal about me?), and time (how long will the data be retained?) (Kang, 1998; Nissenbaum, 2009; Palen & Dourish, 2003). Location traces can document and quantify habits, routines, and personal associations. Your location might reveal your child's school, your regular trips to a therapist or doctor, and times when you arrived late or left early from work. These traces are easy to mine and difficult or impossible to retract once shared. These traces also form living records that are pre-transactional: they are even less public than purchases from Amazon or web searches, or even an interaction with a doctor. And more often than not, location traces and associated data cannot be effectively anonymized.

Sharing such granular and revealing digital data could have a number of risks or negative consequences. Safety and security threats are obvious: thieves, stalkers, etc. are possible dangers. Perhaps less obvious—and probably more likely—are other social consequences. Think about how frequently individuals beg off a social engagement with a little white lie, or keep location and

activities secret to surprise a friend. Much like Facebook's ill-fated Beacon service, participatory sensing could disrupt the social boundaries we have come to expect. And if authorities such as employers or local and federal governments collect or access location data, it's possible to imagine a chilling effect on legal, but stigmatized, activities. Would citizens be as likely to attend a political protest, or visit a plastic surgeon, if they knew their location was visible to others? Large databases of location data accessible by subpoena also could become evidence for minor disputes and civil court cases.

In the United States and Europe, fair information practices are one standard for protecting the privacy of personal data. Originally codified in the 1970s, the Code of Fair Information Practices outlines data-management principles to help organizations protect personal data (*Personal Privacy in an Information Society: The Report of The Privacy Protection Study Commission*, 1977; U.S. Department of Health, Education, and Welfare, 1973).These codes are still considered a gold standard for privacy protection (Waldo, Lin, & Millett, 2007). But the principles, designed for corporations or governments rather than many distributed data collectors, are no longer enough. Data gathered during participatory sensing is more granular than traditional personal data (name, Social Security number, etc.). It reveals much more information about an individual's habits and routines. Furthermore, data is no longer gathered solely by large organizations or governments with established data practices. Individual developers or community groups might create participatory sensing applications and begin collecting personal data (Zittrain, 2008).

We need a nationwide discussion about when and how to share this new form of personal data. Currently, corporations such as mobile carriers as well as small-scale application developers are struggling with how best to provide privacy protections for participatory sensing data. One possible solution is encouraging personal tools and sensing architectures that support individual control over sensing data. Open and privacy preserving systems can create a level playing field in which public good and market innovation flourish, as we have seen in the development of the Internet. Several research labs are currently working on architectures which would provide essential cyberinfrastucture to accelerate participatory sensing while building in privacy from the outset. The commonality in these approaches individually-controlled secure data repositories we call Personal Data Vaults (PDVs). The PDV decouples the capture and archiving of personal data streams from the sharing of that information. Instead of individuals sharing their personal data streams directly with services, we propose the use of secure virtual vaults to which only the individual has complete access. The Personal Data Vault facilitates the selective sharing of subsets of this information with various services over time. Selective sharing may take the form of exporting filtered information from specific times of day or places in space, or may import service computations into the data vault and export resulting computational outputs. Tools for data owners to audit information flows are also essential to support meaningful usage, and are a critical part of vault functionality. These vaults, which could be made available to any interested individual as a public or private service, would provide secure archives of user-contributed data, and offer tools for managing and sharing subsets of that data for use by community groups, researchers, or health practitioners, according to specific filters approved by the individual on a per-service basis. The PDV construct is fundamentally a software function that (a) provides persistent, highly-available storage and management for spatiotemporally-tagged data, and (b) implements controlled sharing on behalf of the data owner.

But questions remain. Who will offer and manage data vaults? And will citizens adopt their use? Creating a business model for the data vault that does not rely on mining location data is a central unmet challenge. Regulations and mandates to encourage participatory sensing application providers to contract with vaults might be one way to support the adoption of such infrastructure. National or state financial incentives to develop and secure such vaults might be another. A second challenge is

introducing greater transparency into the world of mobile services to which personal data vaults connect. A voluntary or regulated system of application labels could help sensing participants understand levels of risk inherent in location-aware services. If an application has "best practice" data practices, it might be certified as a 'fair data' application. In much the same way that voluntary and regulated labels such as 'fair trade' and 'organic' increase the transparency of food products for consumers, labeling can help individuals contract with trusted service providers. Best practices might start with the Codes of Fair Information Practice, and grow to include anonymizing data when possible (Cheng & Prabhakar, 2004; Horey, Groat, Forrest, & Esponda, 2007), collecting minimal information (Agre, 1994), visualizing and explaining data analysis and aggregation procedures, and supporting audit trails (Weitzner et al., 2008) and data retention limits (Bannon, 2006; Blanchette, 2002; Dodge & Kitchin, 2007). Much as the process convened to establish the Codes of Fair Information Practice took negotiation between diverse experts (Waldo et al., 2007), discussion and debate will determine appropriate definitions for 'fair data' requirements.

In addition, we need legal mechanisms to protect this data and encourage individuals to participate in sensing without fear for privacy or liability. For example, diaries – currently the pen-and-paper analogy for much of personal sensing data – are discoverable. How do we build a basis for automated, prompted self analytics to be treated with a stronger legal privilege? If raw location data and experience sampling is too easily discoverable in civil litigation, individuals or entire demographics might be dissuaded from participation in this new form of investigation. A qualified privilege modeled after the trade secrets privilege strikes a good balance of protecting this sensitive data from casual and unnecessary disclosure. Wrapping the data stored in a PDV in an evidentiary privilege, similar to the non-commercial trade secret privilege, would mean that none of the data stored in the Vault could be subpoenaed or introduced into any legal proceeding. Some exceptions might apply, such as the "crime/fraud" exception to attorney-client privilege. But the protection would provide a currently unavailable promise that personal data would not harm a person's job prospects or civil liabilities. Such a privilege could be recognized by state judge application and extension of the common law. Some analogies can be found, for instance, in the recognition of a self-evaluation or self-critical analysis privilege in certain states. Alternatively, state legislatures could pass a statute creating the privilege, as some have done for medical committee reports. If this seems politically unlikely, recognize that we would need only one state to act as a first mover.

In closing, there is tremendous power in the secondary use of mobile phone and locative technologies for research, healthcare, and community building. But to recruit the participation necessary for these technologies to prosper, individuals must be persuaded that very sensitive data will be protected by both law and technology. The current privacy framework in the United States, emphasizing notice and consent and distributed, unregulated data collection, will not support such innovation. New protections to encourage participation and long-term engagement with data control are needed to encourage participatory sensing.

*References*

Agre, P. E. (1994). Surveillance and capture: two models of privacy. *The Information Society*, *10*(2), 101-127.

Anokwa, Y., Borriello, G., Pering, T., & Want, R. (2007). A User Interaction Model for NFC Enabled Applications. Presented at the PERTEC 2007 Workshop on Pervasive RFID/NFC Technology and Applications.

Bannon, L. (2006). Forgetting as a feature, not a bug: the duality of memory and implications for ubiquitous computing. *CoDesign*, *2*(1), 3-15.

Blanchette, J., & Johnson, D. G. (2002). Data retention and the panoptic society: the social benefits of forgetfulness. The Information Society, 18(33-45).

Burke, J., Estrin, D., Hansen, M., Parker, A., Ramanathan, N., Reddy, S., & Srivastava, M. B. (2006). Participatory sensing. In *World Sensor Web Workshop, ACM Sensys 2006*. Presented at the World Sensor Web Workshop, ACM Sensys 2006, Boulder, CO: ACM.

Cheng, R., & Prabhakar, S. (2004). Using uncertainty to provide privacy-preserving and high-quality location-based services. In *Workshop on Location Systems Privacy and Control, MobileHCI* (Vol. 4).

Dodge, M., & Kitchin, R. (2007). 'Outlines of a world coming into existence': pervasive computing and the ethics of forgetting. *Environment and Planning B: Planning and Design*, *34*(3), 431-445.

Eisenman, S. B., Lane, N. D., Miluzzo, E., Peterson, R. A., Ahn, G. S., & Campbell, A. T. (2006). MetroSense Project: People-Centric Sensing at Scale. In *Proceedings of the ACM Sensys World Sensor Web Workshop*. Presented at the ACM Sensys World Sensor Web Workshop, Boulder, CO: ACM.

Horey, J., Groat, M. M., Forrest, S., & Esponda, F. (2007). Anonymous data collection in sensor networks. In *Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. Presented at the The 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Philadelphia, PA: ACM.

Kang, J. (1998). Privacy in cyberspace transactions. *Stanford Law Review*, *50*, 1193-1294.

Miluzzo, E., Lane, N. D., Eisenman, S. B., & Campbell, A. T. (2007). CenceMe - Injecting Sensing Presence into Social Networking Applications. *Lecture Notes in Computer Science*, *4793*, 1-28.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. In *CHI 2003* (Vol. 5, pp. 129-136). Ft. Lauderdale, FL: ACM.

Pentland, A., Lazer, D., Brewer, D., & Heibeck, T. (2009). Using reality mining to improve public health and medicine. *Studies in Health Technology and Informatics*, *149*, 93-102.

*Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*. (1977). Retrieved from http://epic.org/privacy/ppsc1977report/

Shilton, K. (2009). Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. *Commun. ACM*, *52*(11), 48-53.

U.S. Department of Health, Education, and Welfare, U. D. O. H. (1973). *Records, Computers, and the Rights of Citizens*. Cambridge, MA: MIT Press.

Waldo, J., Lin, H. S., & Millett, L. I. (2007). *Engaging privacy and information technology in a digital age*. Washington, D.C.: The National Academies Press.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM*, *51*(6), 82-87.

Zittrain, J. (2008). *The Future of the Internet--And How to Stop It*. New Haven & London: Yale University Press.

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4905

SIIA

# COMMENTS OF THE

# SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

## on the Notice of Inquiry Issued by the Department of Commerce on April 23, 2010

## "Information Privacy and Innovation in the Internet Economy"

## Submitted June 14, 2010

---

On behalf of the members of the Software & Information Industry Association ("SIIA"), we appreciate the opportunity to respond to the Notice of Inquiry ("NOI") published by the Department of Commerce ("DOC") on April 23, 2010, requesting public comment on the impact of the current privacy laws in the United States and around the world on the pace of innovation in the information economy.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet.[1] SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

For over a decade, SIIA has worked with policy makers at the Federal and state levels in the United States, and also with policy makers in Europe, Canada and other regions, to examine the implications and operations of privacy and related laws. This has included work with the relevant Federal agencies implementing existing privacy and security regulations and policies (notably, the FTC's approach on unfair trade practices, as well as implementation of Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), and the Health IT Act; state policy makers (particularly as the myriad of state laws on privacy and data security have evolved); as well as foreign governments, notably Canada and the European Union ("EU").

---

[1] Our website can be found at: www.siia.net

Tel: +1.202.289.7442
Fax: +1.202.289.7097

www.siia.net

## PRELIMINARY OBSERVATIONS

SIIA appreciates the request for stakeholder input into the questions posed by the Department's Internet Policy Task Force.

To state the obvious, treatises could be and have been written on the topics posed in the NOI. SIIA's comments do not attempt to address each and every one of the questions posed; rather, we focus on those that are especially relevant to the mission, experience and expertise of the Department.

Thus, it is appropriate to start with the last question: 'How can the Commerce Department help address issues raised by this Notice of Inquiry?'

For at least the last ten years, since the release of the *Framework for Global Electronic Commerce*, the Department has been positioned to engage not only within the Federal interagency process, but also with our major international trading partners, on the key issues and decisions affecting electronic commerce and doing business online. For these and other reasons, it was no accident that then-President Clinton directed then-Secretary of Commerce William Daley to "work with the FTC and other agencies, consumer advocates, industry, and our trading partners to develop new approaches to extend the proud tradition of consumer protection into cyberspace."[2]

Underlying the Department's role was a fundamental truth that the qualities of the new 'digital' economy advanced by the Internet – "flexibility, innovation, creativity, enterprise"[3] – were producing historic economic growth and jobs. At the time, Vice President Gore envisioned that "by the year 2010, we can triple the number of people who can support their families because they can reach world markets through the Internet."[4] The reality of the impact of the Internet on our economy has far exceeded this vision.

As the convergence of software and information ("S&I") have combined to transform the way that users (individual consumers, government, business end users, and enterprises) access news and information, deliver products and services, and operate, the S&I industries have become strong drivers of the U.S. and global economies, and they are also driving the digital revolution across virtually all sectors of the economy. Well-known firms as well as new, emerging startups — many of which are members of SIIA — create transformative products and services at the leading edge of innovation.

By any measure, the substantial economic impact of the S&I industries demonstrates the critical role that these industries play – despite vast economy uncertainty in real

---

[2] Remarks by the President and the Vice President at Electronic Commerce Event, White House Office of the Press Secretary, November 30, 1998, available at: http://govinfo.library.unt.edu/npr/library/speeches/rmkselec.html.

[3] Ibid.

[4] Ibid.

estate, financial services and manufacturing -- in a vibrant and dynamic U.S. and global economy.[5] The S&I industries have been over the last decade and remain today among the fastest growing and most important for creating jobs and propelling continued U.S. economic growth. For instance, in 2005, S&I industry growth was up nearly 11 percent, compared with 3.2 percent for the economy as a whole, while software and information generated $564 billion in revenue. Also notably, the newspaper, periodical, book and database publishing industry segments sold nearly $7 billion through overseas affiliates in 2005, up by 24 percent from 2000.

The Internet economy today far surpasses Vice President Gore's prediction, with the economic benefits of the commercial Internet eclipsing the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[6] "And if e-commerce continues to grow annually *half as fast* as it grew between 2005 and 2010, then by 2020 global e-commerce will reach $24.2 trillion, and will add roughly $3.8 trillion annually to the global economy – more than the total GDP of Germany."[7]

As elaborated further below, the Department of Commerce – taking into account its mission, experience and expertise – should focus in the context of this NOI on the following both within the Executive Branch Interagency process and with international trading partners on the following:

- Technology and the Internet economy remain the engine of growth for the U.S. economy, producing relative high wage and high value jobs in an increasingly globally competitive marketplace.

- Cross-border flows of consumer and user data are essential to preserving the competitiveness of U.S. workers and US enterprises, and the Department should work to ensure that data protection laws do not impose barriers to trade.

- The myriad of state and Federal regimes on data protection and data security impose increasingly confusing and conflicting requirements.

- Implementation of state and Federal data privacy, data breach and data security laws have unintended consequences for consumer harm and innovation, and require close scrutiny.

- An expansive definition of what constitutes "personally identifiable information" undermines important efforts to build confidence on the Internet and produce innovative products and services

---

[5] *Software and Information: Driving the Global Knowledge Economy,* SIIA, January 2008, pg. 11, available at: http://www.siia.net/estore/globecon-08.pdf.

[6] Atkinson, et al, *The Internet Economy 25 Years After .com: Transforming Commerce & Life*, Information Technology & Innovation Foundation, March 2010, pg. 43, available at:

[7] Ibid (emphasis added).

- The notice and choice model remains essential in the global, online environment. Critical sources of public information promote confidence in the Internet economy.

## CROSS-BORDER FLOWS OF CONSUMER AND USER DATA ARE ESSENTIAL TO PRESERVING THE COMPETITIVENESS OF U.S. WORKERS AND US ENTERPRISES, AND THE DEPARTMENT SHOULD WORK TO ENSURE THAT DATA PROTECTION LAWS DO NOT IMPOSE BARRIERS TO TRADE.

The NOI correctly recognizes that a variety of domestic and foreign laws govern how companies collect, use and share data about individuals. In addition, an increasing array of domestic and foreign laws address the security, retention and even accuracy of such information. This web of laws affects individuals in a variety of contexts: as individual consumers, as employees, and as persons doing business publicly.

This is occurring as US enterprises that are at the heart of the digital and Internet economy increasingly look outward from their U.S. bases to find new customers, enter new markets, and reap the benefits of delivering online services and products without having the costs of traditional 'brick-and-mortar' localization imposed, which may mitigate the opportunity risks.[8] This is true not just for larger enterprises, also for many smaller and medium sized enterprises, which SIIA's research indicates are having larger proportions of their revenues derive from outside North America.[9]

From our vantage, the risks are not only regulatory compliance costs and contradictions, as suggested in the NOI. It is also the direct risk that, under the rubric of data protection, data security and data retention laws, governments will impose barriers to commerce on the Internet that undermine the US Internet economy and our nation's jobs.

At minimum, the Department should be especially vigilant to this risk, factor this risk into its engagement with trading partners in both a multilateral and bilateral context and continue its on-going efforts to facilitate cross-border mechanisms, as well as seek appropriate common arrangements that further this objective.

---

[8] The Task Force should recall that central to Free Trade Agreements negotiated by the US, starting with Chile and Singapore, is a strategic definition of "digital product" that is not inherently tied to either a goods or services trade law framework and does not prejudice a product's classification. By broadly defining "digital product" to include computer programs, text, video, images, sound recordings and other products that are digitally encoded, regardless of whether they are fixed on a carrier medium or transmitted electronically, the FTAs seek a flexible, but practical approach to ensuring that goods and services that combine elements of any of these items are not discriminated against. In other words, no matter how a product may be classified, these Agreements provide for non-discriminatory treatment and promote broader free trade in such products. ***The FTAs also expand market access commitments in Computer and Related Services and ensure that establishment in either country is explicitly not required for the provision of services.***

[9] See *Software and Information: Driving the Global Knowledge Economy*, discussion beginning on pg. 31.

For example, the Department's role in negotiating and implementing the US-EU Safe Harbor agreement stands as a hallmark of DOC leadership and expertise. For many members of SIIA, and other US enterprises with customers and operations in the European Union ("EU"), the Safe Harbor agreement is an essential mechanism to foster cross-border information flows and satisfy different jurisdictional regimes. In addition, the work of the USG, in partnership with US industry, has been important to provide for model contracts to satisfy EU requirements in order that personal data can flow from a Data Controller established in the EU to a Data Controller established outside the EU.[10]

In addition, efforts by the Department, working with interagency colleagues, to provide for key principles, such as those found in APEC. It will be essential, e.g., that the Department support efforts to further the success of the 2008 APEC Ministerial that affirmed the "Digital Prosperity Checklist" and recognized the need to "Promote the development and operation of data privacy frameworks that maximize both privacy protection and the continuity of cross-border information flows consistent with the 2004 APEC Privacy Framework."[11] SIIA encourages the USG to consider the opportunities afforded by efforts such as the Trans-Pacific Partnership to further these goals. In addition, the USG should explore meaningful engagements with non-EU trading partners on how to foster cross-border flow of personal data without the context of the EU Data Protection Directive.

As the Task Force carries out its work in the area of securing personal date, it will be essential to emphasize, based on global principles and the US "Safeguards Rule" the need for on-going data security plans in a manner that promotes predictability and certainty for consumers, consumer protection authorities and businesses. This is not only good policy and practice. This approach also challenges other government that may seek to micromanage technical implementation of data security obligations.

SIIA summarizes the following principles based on international principles,[12] experts[13] and existing regimes, particular the U.S. "Safeguards Rule"[14] which are all appropriate regardless of the size of the entity.

As a fundamental matter, the companies and entities that own or license sensitive personal information should develop a written information security plan that describes their program to protect such information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity

---

[10] See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.
[11] See note on the work of the APEC Electronic Commerce Steering Group, available at: http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.
[12] Organization for Economic Cooperation and Development (OECD), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (December 2005) ("OECD Guidelines"), found at: http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.
[13] "Final Report of the Advisory Committee on Online Access and Security" (May 15, 2000) ("Advisory Committee Final Report"), found at: http://www.ftc.gov/acoas/papers/finalreport.htm#III.
[14] Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. ' 6801 *et seq.*.

of the information it handles.[15] Stated another way, the promotion of on-going security plans should avoid micromanaging the details of the plans, since effective security plans will be based on risk and threat analysis, and implementation details that are unique to each entity's situation, taking into account a variety of factors that overt regulation cannot foresee or be flexible enough to adapt to in a rapid manner.

As a general matter, the experience to date suggests that each plan should include the following items, tailored to each entity's risk analysis and situation:

- designate one or more employees to coordinate its information security program;[16]
- identify and assess the risks to customer information in each relevant area of the company's operation (including, in particular) four areas that are particularly important to information security: employee management and training; information systems; detecting and managing system failures; and on-going evaluation of the effectiveness of the current safeguards for controlling these risks;[17]
- design and implement a safeguards program, and regularly monitor and test it;[18]
- select service providers that can maintain appropriate safeguards, making sure that contracts with such service providers require them to maintain safeguards, and oversee their handling of customer information;[19] and

---

[15] See, e.g., "Safeguards Rule." See, also, "OECD Guidelines", p. 12 ("Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system."); "Advisory Committee Final Report", Sec. 3.4.4. ("...adopt security procedures (including managerial procedures) that are 'appropriate under the circumstances.' 'Appropriateness' would be defined through reliance on a case-by-case adjudication to provide context-specific determinations.")

[16] "Safeguards Rule", 16 C.F.R. 314.3(a).

[17] "Safeguards Rule", 16 C.F.R. 314.3(b). See, also, "OECD Guidelines" ("Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.")

[18] "Safeguards Rule", 16 C.F.R. 314.3(c). See, also, "OECD Guidelines" ("Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.")

[19] "Safeguards Rule", 16 C.F.R. 314.3(d).

- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[20]

To emphasize the experience of our industry to date: These requirements are designed to be flexible, appropriate to an entity's own circumstances and updated on an on-going basis. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network. These principles urge that rather than promoting an overtly micromanaged legal regime, national or regional frameworks should obligate entities or companies to assess and address the risks to information in all areas of their operations and implement security plans accordingly.

## THE MYRIAD OF STATE AND FEDERAL REGIMES ON DATA PROTECTION, DATA SECURITY AND DATA BREACH IMPOSE INCREASINGLY DIFFICULT AND CONFLICTING REQUIREMENTS

The NOI correctly notes that most states have data breach laws (46 states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information) or other laws addressing the privacy of information in the private sector. However, the sources that the NOI relies on[21] in fact underestimate the web of state laws that touch on the NOI inquiry. For example, our research indicates that at *least* 9 states have enacted prescriptive security requirements (or amended their data breach laws to achieve the equivalent goal) affecting what would be 'covered information' in the Draft.[22]

The fragmentation of laws and regulations at the state level makes it nearly impossible to provide consumers with consistent notice and choice, as well as undermine efforts to mount an effective offense against pernicious uses of data (including security breaches).

The NOI, however, focuses narrowly on the question of what hurdles enterprises face in complying with different *state* laws. This lens is increasingly not the singular or significant one. Rather, the issue of enterprise compliance with the federal framework within the maze of state laws is dominating compliance and business efforts by enterprises of all sizes. As recognized in the NOI, the approach of federal statutes is sectoral; in contrast, state privacy and date breach laws, on the whole, proscribe obligations generally on treatment of an individual's data. Yet, except in limited areas,

---

[20] "Safeguards Rule", 16 C.F.R. 314(e).

[21] The NOI references the list of state data breach and data privacy laws collected by The National Conference of State Legislatures, Telecommunications and Information Technology, available at: http://www.ncsl.org/Default.aspx?TabID=756&tabs=951,71,539#539.

[22] As of January 1, 2010, it appears that the following states have enacted security obligations: Arkansas, California, Maryland, Massachusetts, Nevada, Rhode Island, Oregon, Texas and Utah.

federal law does not pre-empt to the Federal government this sphere of influence. A key area where conflicts are arising is in the area of data breach requirements,[23] as well as the securing of health care information,[24] where HHS "Guidance"[25] is inconsistent with the provisions of data security laws in Massachusetts and Nevada, to cite two specific instances.

## IMPLEMENTATION OF STATE AND FEDERAL DATA BREACH AND DATA SECURITY LAWS HAVE UNINTENDED CONSEQUENCES FOR CONSUMER HARM AND INNOVATION, AND REQUIRE CLOSE CRUTINY

In the arena of data protection, the implementation and impact of data breach laws is drawing increasing scrutiny. This is due to a number of factors, including media reports of large data breaches involving personal information and the growing challenge of identity theft. The need for such focus today is not merely related to implementation of good information practices. Rather, entities managing and collecting data face a growing array of "cybercrooks who are continually arming themselves with innovative tools and methods of attack."[26] These criminals "no longer want notoriety—they want financial gain" and their "criminally motivated attacks have more impact on businesses and their customers than the previous generation of digital vandalism and reckless hacking."[27]

In this context, SIIA offers some background that we believe is useful to examine the relationship between data security breaches and the incidence of identity theft.

Amidst the dramatic news stories of data breaches (most notably the massive breach experienced by TJX Corporation, where the public record indicates that a large number of fraudulent accounts were created as a result), several reports have documented that the instances of identity theft have, on the whole, been limited. One of the challenges is that many of the studies over time have not used consistent definitions of breach, and many do not use legal definitions in defining their parameters.[28]

---

[23] See http://www.siia.net/index.php?option=com_docman&task=doc_download&gid=2279&Itemid=48.

[24] See See comments to HHS on their proposed Guidance, available at: http://www.siia.net/index.php?option=com_docman&task=doc_download&Itemid=318&gid=1626.

[25] "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009".

[26] "Hackers open new front in payment card data thefts," *Computerworld*, April 15, 2008, available at: http://www.infoworld.com/article/08/04/15/Hackers-open-new-front-in-payment-card-data-thefts_1.html.

[27] Technical Brief: Symantec Security Response: *Handling Today's Tough Security Threats*, 2006, available at: http://www.symantec.com/content/en/us/enterprise/collateral/tech_briefs/11310863_HTTST_tb.pdf.

[28] See, e.g., the methodology used by the ID Theft Resource Center. The Center compiles an on-going list of publicly reported breaches. The Center's website indicates that "Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver's license numbers and uses

A close examination of several of the most publicized breaches illustrates the point. For example, in March 2005, a laptop with personal information on 98,369 graduate students or graduate-school applicants was stolen from the University of California at Berkeley. However, not a single case of stolen identity related to the incident was ever reported. "The laptop was recovered in September, and police believe that the thief was interested only in the computer, not in the information in its files."[29] In other cases, "it is unclear whether any breach had taken place, [although] there was the possibility that the information was accessed by unauthorized people."[30] In one recent study, it was found that "data breaches were responsible for just 6 percent of all known cases of identity theft, compared to 30 percent from incidents like losing one's wallet. The study also showed that less than 1 percent of all individuals whose data was lost later became victims of ID theft."[31]

In July 2007, the U.S. Government Accountability Office (GAO) released a report[32] examining (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. The report represents one of the more thorough investigations on the subject, examining 570 data breaches that were reported in the news media from January 2005 through December 2006. (This period did not include the TJX case, the largest up to that date).[33]

The report suggests that breaches of sensitive personal information "have occurred frequently" and under widely varying circumstances, but concludes that:

- Evidence of actual identity theft resulting from the breaches is limited. "Available data and interviews with researchers, law enforcement officials and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts," the report states.

---

it for their own personal gain." However, the compilation provided by the Center includes many incidences that appear to not meet this particular definition.

[29] "Separating myth from reality in ID theft", CNET News.com, October 24, 2005, Found at: http://news.com.com/Separating+myth+from+reality+in+ID+theft/2100-1029_3-5907165.html.

[30] Michael, Turner, *Towards A Rational Personal Data Breach Notification Regime,* Information Policy Institute (June 2006), p. 8.

[31] "Survey: Data Breaches Yield Few ID Thefts", Computerworld, September 15, 2006. Found at: http://www.infoworld.com/article/06/09/15/HNidtheft_1.html.

[32] The report was requested by members of the U.S. House Financial Services Committee (Cong. Spencer Bachus, Mike Castle, Darlene Holey, Steve LaTourette, and Dennis Moore), all of whom were co-sponsors of the bill reported by the House Financial Services Committee in the 109th Congress. The full report can be read at: http://www.gao.gov/new.items/d07737.pdf.

[33] The breaches studies involved personal data, including financial data, that could be used to commit identity theft or other related harm. GAO excluded breaches involving other types of sensitive data, such as medical records or proprietary business information.

- Of the 24 largest reported breaches between 2000 and 2005, the GAO found three of the breaches resulted in fraud on existing accounts; specifically, the cases involving CardSystems, DSW and CD Universe, a case stretching back to December 1999. There was evidence in the ChoicePoint case indicating the creation of fraudulent accounts. For 18 of the breaches studied, no clear evidence was uncovered linking them with identity theft. For the remaining two breaches, there was insufficient evidence to make a connection with identity theft.

- "Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges," the report states. The GAO said that consumers notified of a breach could take steps to reduce the risk of identity theft, such as monitoring credit card and bank accounts.

- "At the same time," the GAO said, "breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals," the GAO said. "Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether."

- "... care is needed in defining appropriate criteria for incidents that merit notification. Should [the U.S.] Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk," the GAO said in its report.

In fact, based on this report, and a close examination of reports compiled by entities such as the ID Theft Resource Center, it appears that many breaches pose no real threat to the personal information of individuals and that the requirement for public notification should be carefully crafted.

One other point deserves elaboration. Based on the U.S. experience, a significant number of breaches reported involve government agencies (including U.S. States and the military). In 2009, government agencies accounted for 35.6 % of records breached, according to one source,[34] behind those experienced in the general business category, which was high last year due to the well-publicized Heartland Systems Breach.[35]

We therefore urge that policy recognize the key role that government agencies play in promoting more effective security practices and effectuate steps that minimize the likelihood of data breaches by public authorities:

---

[34] See "2009 Data Breach Stats" published by the Identity Theft Resource Center.
[35] Of the 132,000,000 records reported breached by the ITRC in 2009, at least 130,00,000 were attributed to this one breach.

As of this writing, 46 states (plus the District of Columbia, Puerto Rico and the Virgin Islands) as well as the FTC (under the Health IT Act and through actions under its existing authority[36] for failure to maintain or disclose security practices[37]) and Department of Health and Human Services ("HHS") are implementing data breach regimes.

The following lessons, in our view, are emerging from the implementation of these regimes:

***Establish a meaningful threshold for notification to affected individuals.*** To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a ***significant risk*** of identity theft. This is the recommendation of consumer protection authorities such as the FTC, for example.[38]

---

[36] E.g., primarily Section 5 of the FTC Act for deceptive and unfair trade practices. See, also, Children's Online Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act (FACTA).

[37] To date, the FTC has brought 29 actions against companies that failed to protect consumers' personal information *See, e.g.,* See *Dave & Busters, Inc.,* FTC File No. 082-3153 (June 8, 2010); *See United States v. Rental Research Svcs.,* No. 09 CV 524 (D. Minn. Mar. 5, 2009); *Federal Trade Commission v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of CVS Caremark Corporation*, File No. 072 3119 (Feb. 19, 2009) (accepted for public comment); *In the Matter of Genica Corp.*, File No. 082 3113 (Feb. 5, 2009) (accepted for public comment); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[38] In testimony before the U.S. Congress, then-Chairman Deborah Majoras of the FTC stated the view of regulators that: " ... companies ... notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. ... the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required." Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the

A meaningful threshold predicated on a "significant risk" standard is essential to avoid overnotification of consumers. As then-Chairman of the FTC Deborah Majoras stated in Congressional testimony:

> "The challenge is to require notices *only* when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, ***notices may be more common than would be useful***. As a result, ***consumers may become numb*** to them and fail to spot or act on those risks that truly are significant. In addition, ***notices can impose costs on consumers and on businesses,*** including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[39]

In April 2007, the Identity Theft Task Force established by U.S. President Bush,[40] and co-chaired by FTC Chairman Majoras and then-Attorney General Alberto Gonzales and comprised of 17 federal agencies with the mission of developing a comprehensive national strategy to combat identity theft, reached the same conclusion: that a national standard should be established to require private sector entities to safeguard the personal data they compile and maintain and "to provide notice to consumers when a breach occurs that poses a significant risk of identity theft."[41]

*The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification.* For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications.

The concern is based on the fact that consumers are being preyed upon by bad actors following massive notifications. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists were trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already

---

United States Senate (June 16, 2005), p. 7. Found at: http://www.ftc.gov/os/2005/06/050616databreaches.pdf. (Hereinafter referred to as "Majoras Testimony."

[39] Majoras Testimony at p. 10. (emphasis added)

[40] Exec. Order No. 13,402, 71 FR 27945 (May 10, 2006).

[41] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http.//www.idtheft.gov, p. 4.

be the victims of identity theft.[42] The FTC was compelled to caution U.S. veterans in 2006 "to be extra careful of scams following the recent data breach at the Department of Veterans' Affairs (VA)," noting that "[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the phone."[43]

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, referencing recent news reports of "breaches", asking them to enter their details and account numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user's account and against the backdrop of a widely reported data breach, many users will assume that news is legitimate.[44]

***Careful coordination with enforcement authorities is essential to mitigate harm to consumers in the event of a breach.*** Based on the practical experience that where a breach occurs it is essential to act rapidly to prevent the subsequent harmful affects, a categorical requirement such as this may be inappropriate, and potentially counterproductive.

The decision as to whether or not individual notification is required in the event of a breach must be based on an analysis of the level of risk of harm on a case-by-case basis. This is absolutely essential, due to the fact that public notification of data breaches is a complex issue with signifiant implications for organization and individuals as well as law enforcement, data protection, and consumer protection authorities.

Where a breach occurs, and there may be a significant risk of identify theft, entities experiencing the breach will need to work in a time-sensitive manner with relevant law enforcement authorities who are empowered to combat computer hacking, consumer fraud and related crimes. It is essential that these vital steps are not impeded by requirements that are not as time sensitive. Moreover, it essential that coordination be required among government authorities.

***Define carefully the kind of personally identifiable information that is covered by notification requirements.*** Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification occurs.[45] Two very important points:

---

[42] See "Phishing Fraudsters Prey on Identity Theft Fears," January 13, 2006, found at: http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html.

[43] "FTC Warns Veterans to Delete Unsolicited E-mails;*Scams via E-mail and Telephone Often Follow Data Breaches*," (June 2, 2006), found at: http://www.ftc.gov/opa/2006/06/fyi0632.htm.

[44] See "Will MasterCard breach breed new wave of phishing?", 21 June 2005. Found at: http://software.silicon.com/security/0,39024655,39131331,00.htm.

[45] In general, sensitive personal information that, if breached, should be subject to notification, should include first and last name in combination with any of the following: (A) Government issued identification number used to facilitate social welfare benefits or the equivalent; or (B) Financial account number or

- It should not include a breach involving elements that are widely used in commerce to facilitate transactions.

- It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.[46]

***Avoid mandating specific technologies, while encouraging the adoption of good practices***. SIIA would urge, as part of a coherent national framework, technology-neutral incentives for businesses to take appropriate and effective steps to safeguard sensitive data. A number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction. To single out one method to secure data in legislation, such as encryption, suggests, if not an outright mandate, then a *de facto* exclusive means to avoid notification, creating a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools. SIIA strongly recommends that "securing the information by a method that renders the data elements unreadable or unusable" is recognized in policy.

***Where 3rd parties manage data, and notification is required, avoid consumer confusion.*** In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect themselves, which is the object of notification regimes.

As a final note on this point, SIIA urges the Task Force to focus its attention on a trend where NIST guidance – which was developed for use by federal agencies, and may not be to be evaluated against – is being included in legally binding obligations on private sector entities under Federal data breach regimes. Earlier this year, SIIA wrote to NIST Director Patrick Gallagher[47] expressing deep concern that "the incorporation of the NIST technical guidance and standards by HHS into a mandatory rule not only factually misstates many of their key elements, it also risks degradation of key non-binding

---

credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.

[46] It is noted that the vast majority of U.S. states that have enacted data security breach notification laws (35 of the 39 to date) have included an exception for public record information.

[47] A copy of the letter is found in Attachment A.

technical work that NIST engages in and which is of tremendous value to our industry." It is essential that NIST remain a first class world laboratory. Steps such as those taken by HHS in its "Guidance" risk making NIST a 4th class regulator.

## AN EXPANSIVE DEFINITION OF WHAT CONSTITUTES "PERSONALLY IDENTIFIABLE INFORMATION" UNDERMINES IMPORTANT EFFORTS TO BUILD CONFIDENCE ON THE INTERNET AND PRODUCE INNOVATIVE PRODUCTS AND SERVICES

SIIA appreciates that the topic of non-personally identified information is one that is the focus of rich discussion in a variety of venues. Yet, despite the robust discussion underway, there appears to be a trend to expand the scope of privacy and data protection regimes to include *non-personally* identifiable information about individual users, whether they are consumers or business associates, i.e., without regard to the context of the collection, use or disclosure of individual data. This makes compliance not only challenging, but raises serious questions about the balance of achieving meaningful privacy protections with providing essential services and innovation solutions that enhance consumers.

Nowhere is this debate more evident than over Internet protocol addresses. We note, however, that to date no data protection authority or judicial body, to the best of our knowledge, has determined that such an identifier is personally identifiable without examining *the specific context in which an IP address is used*; indeed, data protection authorities and judicial bodies have avoided categorical conclusions in this regard.

The inclusion of IP address in the definition of "personally identifiable information" also fails to recognize that it is a standard data point and absolutely necessary to deliver Web pages and content. It is not personally identifiable, as such.

Moreover, the collection, use and disclosure of Internet Protocol address data, which travels with virtually all Internet communications, is essential to the prevention, investigation and combating of all forms of online misconduct. It is particularly important to preserve the ability to collect and use Internet Protocol address data in cooperative efforts to reduce the unacceptably high levels of trademark and copyright infringement, cybercrime, denial of service attacks, and other illegal and harmful activities online. And it would be difficult, perhaps completely unnecessary – and potentially counterproductive -- to provide notice and consent to Internet users, as has been suggested in some quarters, that their publicly available IP address information may be collected for these purposes.

It has asserted that developments in the EU support the argument that IP addresses are to be considered PII. Despite press reports of high profile statements by leading data

protection authorities,[48] a closer scrutiny belies the broad assertion that IP addresses are categorically considered PII in the EU. The actual discussion of the issue revolves around the purpose and manner in which IP addresses may be associated with *other* information that is not collected from the consumer. In the recent high profile case, *Promusicae v. Telefónica,*[49] the European Court of Justice (ECJ) examined the question whether the Internet Service Provider (ISP) Telefónica should be "ordered to disclose the identities and physical addresses of certain persons who it provided with internet access services, *whose IP addresses and data and time of connection were known*"[50] in the context of a civil investigation that included a request for contact information about individuals using the KaZaA file exchange (peer-to-peer) program to exchange pirated sound recordings. Significantly, the ECJ did not conclude that IP addresses were *inherently* PII as such, because the names and addresses, which did constitute PII, were previously known and linked.[51]

SIIA urges the Task Force, the Department and the Administration to work to make sure that the long-standing availability of this information be explicitly preserved in order to detect and remedy instances of malicious and illegal conduct, including cybercrimes and intellectual property infringement.

## THE NOTICE AND CHOICE MODEL REMAINS ESSENTIAL IN THE GLOBAL, ONLINE ENVIRONMENT. CRITICAL SOURCES OF PUBLIC AVAILABLE INFORMATION PROMOTE CONFIDENCE IN THE INTERNET ECONOMY

The NOI inquires whether the notice and choice approach to consumer data privacy is still a useful model.

In short, yes, it remains essential, particularly in the global online environment where entities driving the digital and Internet economy operate across borders and in different jurisdictions. As previously noted, there is a trend to expand the scope of privacy and data protection regimes to include *non-personally* identifiable information about individual users, whether they are consumers or business associates, i.e., without regard to the context of the collection, use or disclosure of individual data. Thus, especially in a business-to-business context, whether dealing with recognized PII or non-PII of business customers, it is essential that the contours of those commercial relationships be able to be managed effectively through a notice and choice model.

---

[48] *See, e.g.*, "European Regulators Mull Protecting IP Addresses," Information Week, January 23, 2008 06:00 AM, found at: http://www.informationweek.com/internet/showArticle.jhtml?articleID=205916731.

[49] C-275.06, 29 January 2008.

[50] Ibid at para. 30 (emphasis added).

[51] See, also, *EMI Records v Eircom Ltd* [2010 IEHC 108], finding that such uses fully compatible with Irish data protection law. Available at: http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/7e52f4a2660d88408025770700350 82f?OpenDocument

The NOI inquires whether a "use-based model for commercial data privacy" could be a basis for defining data protection obligations.[52] SIIA has studied the cited document on a preliminary basis, and will discuss it further with members in light of our experience with US and global data protection, data breach, data security and data retention regimes. As an initial reaction, the paper holds some useful insights into well-established fair information practices. However, it is not clear how this would be a substitute for notice and choice, in light of the well-developed frameworks that predicate data protection on this model. In addition, it is not clear how the approach put forward could be reconciled with non-US regimes, which are based on different assumptions than fair information practices.

Regardless of the model – notice and choice, use-based, or other underlying principle – it is essential that the Task Force, the Department and the Administration work to preserve the use and disclosure of individual data that "enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy," as stated in the NOI.

A few illustrative examples are provided below.

***Whois Domain Name Registration Data***. As the Task Force is well aware, domain name registration information has been publicly accessible through "Whois" since the earliest days of the domain name system, even predating the World Wide Web.

Access to Whois data is critical to dealing with instances of phishing, distribution of malware, network attacks, and online frauds of all kinds; it is also essential to the investigation and mitigation of copyright piracy and trademark misuse over the Internet. Virtually every Internet user benefits from public accessible Whois, as public access to Whois data is essential to knowing the entity one is doing business with via the Internet.

This policy is recognized not only in the NTIA policy governing the ccTLD .us. It is also recognized in the Affirmation of Commitments that the Department concluded with ICANN last September.[53] It should also be noted that the leadership of the Energy & Commerce Committee – including Chairman Waxman, Chairman Boucher and Chairman Emeritus Dingell – wrote to Secretary Locke[54] last summer with the same vision: that ICANN would remain perpetually accountable to the public via an instrument that should:

---

[52] The NOI cites as one example of a use-based model the paper published by the Business Forum for Consumer Privacy ``A Use and Obligations Approach to Protecting Privacy: A Discussion Document," Dec. 7, 2009, http:/ /www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf.

[53] Moreover, it is essential that the Department not only work to preserve public access to such Whois data, but strengthen its oversight to improve the accuracy, reliability and timeliness of data found in the Whois service.

[54] August 4, 2009, available at: http://www.boucher.house.gov/images/icann%20letter.pdf.

"Ensure that ICANN will adopt measure to maintain timely and public access to accurate and complete Whois information, including registrant, technical, billing, and administrative contact information that is critical to the tracking of malicious websites and domain names."

It is incumbent on the Task Force, Department and Administration to make sure that this policy is also preserved vis-à-vis our global government partners, some of whom have taken the position that publicly accessible Whois is incompatible with the privacy laws of some countries. The positions of these governments threaten to cloud the transparency needed for the digital and Internet economy.

***IP Address Information***. To reiterate our concerns stated above, the discussion about what constitutes 'personally identifiable information' remains a central challenge to the implementation of data protection regimes domestically and globally.

In the context of this discussion, the collection, use and disclosure of IP addresses is extremely important to combating cyber crimes, online fraud, denial of service attacks, copyright piracy, trademark infringement, and other forms of harms to consumers misconduct carried out online.

It is essential that the Task Force, the Department and the Administration engage actively on these issues, both in the development of U.S. privacy law and policy, and in consultations with our trading partners, to ensure that that the "personal data" rubric is not counterproductively extended to impede responsible use of IP address data to detect and deal with instances of online conduct and crimes.

# ATTACHMENT A

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095


March 5, 2010

The Honorable Patrick D. Gallagher, Director
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 1000
Gaithersburg, MD 20899-1000

Dear Dr. Gallagher:

On behalf of the members of the Software & Information Industry Association (SIIA), I am writing to bring to your attention our concerns with the misapplication of NIST technical guidance and technical standards by the Department of Health and Human Services (HHS) last year when it published guidance on technologies to secure personal health information.[1] As we explain below, the incorporation of the NIST technical guidance and standards by HHS into a mandatory rule not only factually misstates many of their key elements, it also risks degradation of key non-binding technical work that NIST engages in and which is of tremendous value to our industry.

A legal safe harbor is designed to encourage good practices, not merely to avoid notification. As such, the Interim Final Rule Guidance does not achieve the purposes of the Safe Harbor by relying on inapplicable NIST documentations and processes, many of which cannot be technically adhered to in the manner asserted in the Interim Final Rule Guidance.

We respectfully request that NIST, along with your colleagues at the Department of Commerce, work with others in the Administration's interagency team implementing the Health IT portions of the American Recovery and Reinvestment Act of 2009 (the "stimulus Act") to address these inaccuracies and misapplication of NIST documents. With HHS likely to update its guidance, and a report to Congress on the health data security provisions of the stimulus bill possibly underway, we also urge the interagency review of the guidance before any report is provided by HHS as required by law.

---

[1] Section 13402 of the American Recovery and Reinvestment Act of 2009 required the Secretary of Health and Human Services (HHS), within 60 days of its enactment, to issue "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements".

Despite HHS issuing the guidance within that time frame, the substance of the Guidance proved extremely problematic. SIIA commented at two specific stages of the HHS rulemaking process, outlining the concerns were share today. At no stage did HHS address the substance of these comments. And the guidance, as published by HHS remains essentially unchanged and of deep concern.

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

## CONCERNS WITH THE GUIDANCE

SIIA raised this substantive issue in our prior comments, but HHS did not specifically address it in its analysis.[2]

***First, the Interim Final Rule Guidance conditions a legal safe harbor on compliance with documents and processes of the National Institute of Standards and Technologies (NIST) that were not intended to be used in this manner.***[3] We strongly urge that any reference to NIST in the Guidance be removed to the degree that it implies that the legal basis of the 'safe harbor' reflected in the Guidance is predicated entirely on implementation of the NIST publications and validation procedures.

All of the work done by NIST incorporated into the Guidance was undertaken in the context of NIST's statutory mandate, which is in furtherance of its responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. Thus, "NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all *agency* operations and assets."[4] As such, "This guideline has been prepared for use by *Federal agencies*. It may be used by nongovernmental organizations on a *voluntary* basis..." (emphasis added) It is inappropriate, and outside of HHS' authority, to require private entities to abide by the requirements of FISMA. This fundamentally alters FISMA's statutory mandate.

The Guidance also states in this regard, in Section II.B(a)(ii), that entities must comply with "valid encryption processes for data in motion .. [which] may include others which are FIPS 140-2 validated." The reference to FIPS 140-2 is not a focus on a "technology or methodology", but instead a reference to specific products, which is not found in the ARRA. This Guidance, in essence, selects winners and losers in this marketplace, rather than allowing the best technology to thrive. Moreover, choosing static products in this dynamic field undermines the goal of protecting health information as there is no incentive for our members to adopt newer technology that might be more secure, if to do so prevents our members from availing themselves of the safe harbor.

---

[2] HHS does state "that any further comments regarding this guidance received in response to the interim final rule will be addressed in the first annual update to the Guidance, to be issued in April 2010." However, this mention does not address the factual issue raised previously to HHS, and leaves the current Interim Final Rule Guidance faulty and inconsistent with the requirement that a rulemaking address factually substantive issues.

[3] HHS asserts that "the guidance on securing protected health information is not mandatory; it is discretionary" but recognizes that "many covered entities and business associates are voluntarily choosing to secure their protected health information in accordance with the guidance in order to avoid the possibility of having to provide breach notifications pursuant to this subpart." (emphasis added) HHS misses the mark in its analysis on this point. First, HHS provides no evidence to this effect, as we explain in our letter, the Special 800 Series are neither designed nor intended to be used in this way.

[4] "...but such standards and guidelines shall not apply to national security systems."

Finally, FIPS are developed and adopted by NIST as a standard that "is applicable to all *Federal agencies* that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106." While "this standard is available to private and commercial organizations," FIPS have never been imposed by federal rule or regulation as a predicate to a legal obligation, liability or safe harbor on commercial implementations.

**It is our view that it is beyond the authority provided in the Recovery Act for HHS, as a condition of a legal safe harbor, to impose on the commercial sector Special Publication requirements, many of which are not even mandatory to Federal agencies.**[5]

***Second, the Guidance states factually inaccurate information about a number of NIST Special '800 Series' Publications.*** The Interim Final rule Guidance asserts that the "encryption processes identified [in the NIST publications] have been *tested* by NIST and *judged* to meet this standard [the provisions of the Stimulus Act cited by HHS]."[6] (emphasis added)

This statement in the Guidance is factually incorrect. Without prejudice to the useful technical analysis that is provided in these Special Publications and the well recognized role of NIST as a facilitator with industry in this important area, *nothing in these documents has been "tested" nor been "judged" to meet a particular standard.* On the contrary, the entire "Special Publication 800-series" reports on NIST's Information Technology Laboratory's *research, guidance, and outreach efforts* in computer security and its collaborative activities with industry, government, and academic organizations." The "800-series Publications" are distinct from other NIST responsibilities which "include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems." (emphasis added) In developing the "800-series Publications", NIST has carefully refrained from labeling these Special Publications as even 'best practices.'

***Third, the Guidance incorporates documents which are not designed to be nor in fact capable of being evaluated against.*** The Guidance imposes on affected entities a virtually impossible burden: to benefit from the safe harbor, they must show they meet often inconsistent, generally designed 'requirements' found in documents which have neither been subject to comment and review, much less the requisite scrutiny that is required for 'assessments' Thus, a company may have implemented some of the

---

[5] The implication of HHS imposing these documents on commercial implementations raises profound questions about the process that NIST has gone through in the development of Special Publications. If HHS were to require, as provided in the Guidance, conformance to these documents, each of these documents would have to be opened up for a formal notice and comment process. None of these documents are the product of such a process.

[6] This language is identical to that in the earlier draft Guidance, and remains unchanged – without any explanation.

elements of the "research" that are found in the Special Publications, but not all of them, but enough to make data unusable, unreadable or indecipherable. As such, it is not clear from the language in the Guidance whether this is satisfactory.

As a general matter, SIIA is deeply concerned that the Guidance gives legal benefit only to those processes that have been tested (or, of deeper concern, *'certified'*) in satisfaction of the Guidance. Nothing in the authority given HHS under the ARRA permits the imposition of testing or certification requirements, *even if HHS could demonstrate that such conformance were technically possible using common place evaluations – which it has not, and we would add, could not be done.* Additionally, nothing in the record establishes that such tests or certification is a necessary prerequisite to benefitting from the safe harbor established in the Guidance.

We appreciate the hard work of NIST on so many fronts that are important to our industry. And we very much appreciate your consideration of our concerns. We strongly urge an appropriate adjustment to the use and characterization of the Guidance in this Rule, and a continued collaboration with NIST on the many issues of importance to our industry.

Sincerely,

Mark Bohannon
General Counsel &
Senior Vice President, Public Policy

cc: Aneesha Chopra, Chief Technology Officer, White House

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095


June 14, 2010

Honorable Barney Frank
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Honorable Christopher Dodd
Chairman
Committee on Banking, Housing and Urban Affairs
U.S. Senate
Washington, DC 20510

Dear Chairmen Frank and Dodd:

I am writing on behalf of the Software & Information Industry Association (SIIA), to express my concern that our member companies may have difficulty in accessing the public debt markets because of Section 933(b) in the *Restoring American Financial Stability Act* currently being finalized in your conference proceedings.

SIIA is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic information content for business, education, consumers and the Internet. SIIA's members include software companies, e-businesses, and information service companies, as well as many electronic commerce companies.

SIIA members have led the way in establishing and expanding our nation's information infrastructure – a key to sustained economic growth in the 21st Century. Like many new and emerging markets, our members have and will continue to depend on access to the public debt markets in order to expand the suite of innovative products and services available to American citizens. We are, however, concerned that our member companies may have difficulty in accessing the public debt markets because of Section 933(b) in the *Restoring American Financial Stability Act* currently being finalized in your conference proceedings.

Specifically, we believe there may be unintended effects of Section 933(b) because it places discriminatory liability burdens on credit rating agencies by exposing them to an unprecedented, new "state of mind" standard for securities fraud claims under the 1934 Securities and Exchange Act. These provisions would establish a standard different than that which has applied to any other market participant and therefore could force rating agencies to become more defensive in the issuance of ratings, possibly substituting litigation concerns over independent analytic judgment. They will therefore likely be less willing to rate debt in new and emerging markets, including innovative software and information technology firms. Without such ratings, our companies are likely to find it much more difficult to access the public debt markets, resulting in significant increases in capital costs that will slow the pace of innovation and economic growth.

We therefore respectfully urge that Section 933 be deleted or redrafted. The provision should ensure that credit rating agencies provide ratings that maintain strong investor protection against intentional bad faith acts without causing disruption in the quality and timeliness of robust ratings that are, and will remain, so important to our members.

Thank you for your consideration of this request.

Sincerely yours,

Ken Wasch

Ken Wasch
President

Cc: Members of the Conference Committee

Tel: +1.202.289.7442
Fax: +1.202.289.7097

Sören Preibusch

University of Cambridge
Computer Laboratory

15 JJ Thomson Avenue
Cambridge CB3 0FD

Soeren.Preibusch@cl.cam.ac.uk

---

2010-06-07

**Comments regarding the Notice of Inquiry on**
**Information Privacy and Innovation in the Internet Economy**

**Unaddressed privacy concerns lead to welfare loss**

Privacy has become a decisive factor for the success of online transactions. Whilst more recently, privacy negligence at global social networks has sparked protest form consumer associations, governments, and interested individuals, electronic commerce has been exposed to the negative consequences of careless data processing for a longer time.

According to a 2009 PayPal-commissioned study, protecting their privacy and the related protection from fraud and ID theft are online consumers' two biggest concerns when shopping online. Earlier surveys indicate that two thirds of offline-only shoppers did not purchase online because of privacy concerns; around one third of online shoppers would buy more if they were not worried about privacy/security issues; more than a quarter of shoppers had abandoned online shopping carts because of privacy reasons. My own research indicates that two thirds of online shoppers intend to cancel a transaction if prompted for personal information they are unwilling to provide. The majority of them choose to switch to an alternative, competing vendor, and approximately 30% provide false information, leaving the online retailer with untapped sales potential and latent defects in data records.

As consumers refrain from shopping online because of privacy concerns, the loss in realised trade implies a loss in social welfare.

**Naive anonymity is not the answer**

Simply reducing data collection does not provide a viable route to increase consumers' propensity to shop online.

Anonymous usage of online services is often undesirable as it forbids a persistent account with convenience features such as a transaction history or reuse of once-entered information.

Anonymity also precludes the ability to personalise offerings, a basis for recommendations individually tailored to one's needs and interests. As identity information is used in addition to the behavioural and transactional profile, socialising features amongst consumers are unlocked. Whilst there is a clear business perspective in such marketing endeavours, consumers actually value the convenience and quality of personalised services.

As we acknowledge that anonymity is not the aim, we also realise that security features such as data encryption alone are insufficient, despite being an important building block of privacy-enhancing technologies.

**Information privacy is achieved through individual control**

Privacy is an individual's ability to decide for herself who should have what information about her and also the individual's ability to effectively limit how this information is used, for which primary and secondary purposes, and with whom it is potentially shared.

Privacy reaches beyond the data item itself. Privacy requirements put personal information in context, notably through purpose-binding. For instance, whilst a consumer may decide to reveal her email address to an online shop, she may want to restrict how her email address is being used: order confirmations are acceptable, but a weekly newsletter is unsolicited. Currently, Web interfaces seldom offer even such basic methods for users to exercise choice and control.

The Notice of Inquiry uses the term "use-based rules" to describe user-driven regulation of purposes for which personal information may be employed. I argue that effective choice in privacy-related decision-making does and should genuinely encompass users' ability frame their personal details.

In some continental European legislations (e.g. Germany), companies are forbidden to tie customers' acceptance of the terms and conditions to consenting the privacy policy. Pragmatically, this leads to two checkboxes on Web forms; more philosophically, it implements the distinction between primary and secondary purposes of data usage for the same set of data items.

**Heterogeneity in privacy preferences**

The why and how of one's control over the own personal information very much depends on privacy preferences albeit the data subject's routine inability to verbalise these preferences. My own research into *privacy types* shows the difficulty in structuring a population of consumers into groups that exhibit similar concerns about revealing personal information. Consumers have fragmented preferences with regard to providing personal information online, let alone the moderating effects of trust and previous interactions at the individual level. Even fine-grained clustering achieves poor coverage of the entire online population.

This heterogeneity implies that any attempt to approach consumers with an inflexible, take-it-or-leave-it privacy policy—as it is current corporate and regulatory practice—will leave most of consumers unsatisfied.

**Detrimental inflexibility in current privacy practices**

Consumers' diversity in privacy preferences and their individual valuations of service quality levels unlocked by additional, voluntarily provided data, find little response in current data collection practices on the Web.

Today, the parameters of informational self-determination are often laid out in privacy policies, but it is hard to find user participation in these policies when flexibility or feedback channels are absent. As frustrated and disappointed customers cancel online purchases, or avoid online interaction because of privacy worries, companies are unable to learn which parts of their static privacy policy lead to rejection at the individual level and how the dependent functional service properties are valued. Consequently, the existing channels of the Web for interaction and transaction do not tap into their full potential.

**Subjective choice and objective guide**

The Notice of Inquiry contrasts "satisfying subjective consumer expectations" with "enact[ing] objective privacy principles" as design goals for regulation. These goals are not mutually exclusive, all the same. Subjective satisfaction is achieved as consumers make individual choices. To the extent these choices are guided by appropriate risk assessment, i.e. privacy decisions really reflect informed consent, they translate an objective principle. Regulation could encourage effective support tools, increase the salience of privacy risks, make implicit data collection explicit or mandate privacy-friendly default settings.

**Privacy Negotiations**

The relationship between privacy and personalisation has been labelled as a trade-off; however, this term ignores the rewarding ability to also tailor data protection to the individual customer.

In *privacy negotiations*, consumers and service providers establish, maintain, and refine privacy policies as individualised agreements through the ongoing choice amongst service alternatives.

Negotiable privacy policies put an end to the paradigms of take-it-or-leave-it and one-size-fits-all. Privacy policies become a matter of personalisation themselves. Privacy negotiations provide customers with the ability to choose the level of data protection they deem appropriate and desirable at that very moment. This principle of choice, which can happen implicitly as services are consumed online, is advocated in most culturally motivated data protection principles, such as the Fair Information Practice Principles.

By breaking down the opt-in process to single data items or other privacy dimensions such as secondary purposes, the retention period, and sharing with third-parties, privacy negotiations also follow the spirit of the European Privacy Directive. Disagreement on a single aspect of the privacy policy no longer implies that the customer is forced into a data collection scheme against her will or to cancel the transaction; instead, the user may singularly choose not to provide a data item.

Offering rewards for specific data items expands the negotiation space and thereby makes reaching an agreement in privacy policy negotiations with higher levels of data disclosure more likely. In *incentivised privacy negotiations*, the transaction partners may additionally bundle the personal information collection and processing schemes with monetary or non-monetary rewards. Live examples include discount codes attached to a newsletter opt-in.

**Privacy negotiations are a win-win for consumers and corporations**

Privacy negotiations allow consumers to effectively find, for themselves, a balance between their privacy concerns and their appreciation for online services, for which voluntary data disclosure potentially unlocks more advanced features. In embracing the diversity in privacy preferences, fewer consumers are deterred by subjectively worrying privacy practices. Companies may offer incentives to stimulate voluntary data revelation as mandatory collection is phased out.

The exchange of personal data items for rewards does not conflict with the nature of privacy as a fundamental human right which excludes it from being traded. Privacy negotiations do not contravene the human right to informational self-determination. Consumers are not rewarded for renouncing their privacy, but agree on a price for personal information, which is an economic good. As a privacy-enhancing technology, incentivised privacy policy negotiations lift this price above null compensation.

Companies, in turn, may realise that consumer-friendly privacy practices attract new socio-demographic milieus. My research provides evidence that a company charging slightly higher prices, but collecting less personal details may sell commodity products at an average unit price of 80% above its competitor's price, effectively turning privacy into a competitive advantage.

**Mechanised enforcement generates trust**

As a result of privacy negotiations, combinations of data items agglomerate to amorphous data records. Even similarly filled data records may be governed by different privacy policies. This poses new challenges for the back-end data processing algorithms. Consequently, stronger assurance must be given that not only some, company-determined static policy is respected, but that every user's own privacy configuration is diligently adhered to.

The Notice of Inquiry asks how "privacy-related technologies and business processes [could] enhance consumer trust in Internet commerce." Privacy seals are the most salient advertising of

careful processing of personal information; if vouched for externally, certification often involves scrutiny of the companies' data processes. However, the degree of formality of such assessment remains low with code inspection being rare and mechanised analysis even rarer. Therefore, seals are only as reliable as the laborious manual inspection. Their costs also make privacy checks less frequent than changes to the functionality of the Web site, resulting in potential divergence between the certified state and the actual state. Further empirical and theoretical research is needed to bridge between empirical research into the economics of privacy and formal *privacy calculus*.

**Before the**
**Department of Commerce**
**Internet Policy Task Force**

| | | |
|---|---|---|
| **In the Matter of the Request for** | ) | |
| **Comments on Information Privacy and** | ) | **Docket No. 100402174-0175-01** |
| **Innovation in the Internet Economy** | ) | |

---

# COMMENTS OF THE STATE PRIVACY & SECURITY COALITION

---

Jim Halpert
Adrian Copiz
DLA Piper
500 Eighth Street, NW
Washington, DC 20004
(202) 799-4000

**June 16, 2010**

**June 16, 2010**

**FILED ELECTRONICALLY**

**National Telecommunications and Information Administration**
**US Department of Commerce**

**In the Matter of the Request for Comments on**
**Information Privacy and Innovation in the Internet Economy**
**Docket No. 100402174-0175-01**

# Comments of the State Privacy & Security Coalition on Information Privacy and Innovation in the Internet Economy

## I. INTRODUCTION

The State Privacy and Security Coalition very much appreciates both the Department's undertaking this NoI and this opportunity to submit comments.

### A. Description of State Privacy & Security Coalition

State Privacy & Security Coalition ("the State Coalition") members include a broad cross-section of the US technology and media industries – companies and trade associations who are vitally concerned with barriers to innovation posed by conflicting state privacy, security and e-commerce regulation: Amazon.com, AOL, AT&T, Cisco, Comcast, HP/EDS, Facebook, Fox Interactive, Google, Monster.com, Reed Elsevier, Skype, TimeWarner Cable, Verizon, and Yahoo!, the Entertainment Software Association, Internet Alliance, the NA*i,* NetChoice, Technology Association of America, and TechNet.

Our Coalition has a wealth of experience in the issues raised in the State portion of the NOI. Its focus is on state privacy, security and e-commerce proposed laws and regulations that would create barriers to doing business on a nationwide basis.

At the same time, most of its members do business internationally and are strongly supportive of the Department's efforts to reduce barriers to innovation posed by conflicting international regulation.

The State Coalition was formed in the wake of passage of a sweeping California opt-in spam law with $1,000 per message class action exposure and an overbroad Utah "anti-spyware" law that imposed broad notice and consent download restrictions on a wide array of routine, beneficial software programs that are not spyware, including parental controls software. The

first law was preempted by Congress through the CAN-SPAM Act[1], before it could take effect. The second was enjoined by a Utah state court on First Amendment and Dormant Commerce Clause grounds.[2] However, both these narrow misses highlighted the threat to Internet innovation and growth posed by disparate and overbroad state privacy and security regulation. These laws underscored the need for technology and media companies and trade associations to join forces to work proactively to manage these significant risks to innovation.

A white paper from the Department or the White House explaining potential barriers to innovation caused by disparate state privacy and data security regulation would be very helpful. State policymakers, many of whom are part-time legislators, are well intentioned, but often make law in a climate of suspicion of new technologies and without full information about the often complex issues raised by new technologies.

**B. The Significant Threat to Innovation Posed by State Regulation -- The Large Volume of State Regulation and Near Misses**

In recent years, state legislatures have enacted over 100 state privacy and data security-related laws. This includes security breach laws in 46 states plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, 10 data security laws for the protection of personal information, data disposal laws in 19 states, RFID privacy laws in 13 states (with multiple laws passed in Washington, California and New Hampshire), phishing laws in 22 states, spyware laws in 15 states, 37 spam laws, 24 online sexual predator laws, 2 recent credit history privacy laws, and 3 online privacy laws.

The NOI asks only about laws. It is important to recognize that every year, but for the efforts of affected stakeholders, including the technology industry, privacy advocates, and civil libertarians, there would be dozens of additional state privacy and security laws that would make it exceedingly difficult (if not impossible) to operate in the Internet environment and provide commensurate levels of privacy and data security to all users. State barriers to innovation are a significant threat. Policymakers at the state level are actively seeking to regulate in this area, even if relatively few laws are ultimately enacted.

For example, In 2004, Utah enacted a "spyware control act," H.B. 323,[3] which imposed detailed notice, consent and uninstall requirements for any software that triggered an advertising based upon user activity if that advertisement obscured any part of a webpage or advertising on a webpage. Trademark owners, website owners, and advertisers could all sue under the law for $10,000 statutory damages per advertisement displayed, plus attorneys' fees. The law was phrased sufficiently broadly that it reached a wide variety of other software downloads that presented advertising when a user's browser was open, exposing software distributors to lawsuits for significant statutory damages

[1] 15 U.S.C. § 7707(b).
[2] *WhenU v. State of Utah*, (June 22, 2004), transcript available at http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf.
[3] Available at http://www.benedelman.org/spyware/utah-mar04/bill.html.

In 2007, both North Carolina and Connecticut came very close to enacting unworkable age verification mandates for a broad range of websites that bills in these states defined as social networking sites. Neither bill passed, and a Berkman Center Report on child protection issued the following year highlighted privacy and security flaws in the age verification approach, which had been advocated by several vendors.[4] This year, a California bill, S.B. 1361,[5] would prohibit including an address and phone number field in online profiles of users known to be under the age of 18.

In 2009, Maine passed a teenage marketing law, L.D. 1183[6], that had the effect of extendeing the federal Children's Online Privacy Protection Act (COPPA) to 17 year-olds and to offline collection of either personal information or de-identified health information. The law also barred any transfer of personal information or de-identified health information about a minor to any other party, even if transferred with parental consent. Third, the law barred any use of personal information or de-identified health information about a minor to recommend any course of conduct with regard to a product or service (including health or safety recall warnings or advice about the safe use of medicine). The law made no reference to activities in Maine and purported to apply nationwide; there was no feasible way to identify and segment Maine minors on the Internet, unless (ironically enough) companies collected and retained more personal information about individuals. Several coalition members, represented by DLA Piper, sued and obtained a consent order that raised serious questions about the law's constitutionality. As a result of the consent order, the Maine legislature repealed the law this spring.

Both Massachusetts' and New Jersey's security breach laws gave state regulators the authority to impose data security regulations. Both states initially proposed technology mandates that required the use of encryption, and only encryption, as a data security solution. The New Jersey regulations went further, mandating a long list of specific information security measures appropriate for medium-sized business. Both these technology-mandate approaches were withdrawn.

Law enforcement-related mandates are an equally serious threat. In particular, several states (including Nevada, Colorado and, last year, Maine) have come very close to imposing IP address data retention mandates on ISPs and other Internet companies. In a less dramatic but similar vein, Minnesota imposes a hard deadline for complying with any law enforcement subpoena from that State. Other states (New Jersey and Wisconsin) have considered rigid, short deadlines for compliance with all law enforcement subpoenas from their states that would create inevitable conflicts with federal and other state law enforcement priorities. In the end, these bills were changed to remove the hard deadline.

Even state breach notice bills, for which state-by-state compliance is in principle workable, typically pose significant compliance problems as introduced. For example,

---

[4] John Palfrey et al., *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States* (2008), available at http://cyber.law.harvard.edu/pubrelease/isttf/.

[5] http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1351-1400/sb_1361_bill_20100419_amended_sen_v97.html.

[6] Pub. Law c. 230, codified at 10 MRSA c. 1055, § 9551 *et seq.*

Mississippi this year became the 46th State to enact a breach notice law.[7] Despite having 45 other states to follow, the Senate sponsor proposed a series of different requirements that contained several unworkable features that would have:

- required double notice to state residents by both the data owner and the vendor when a vendor suffered a security breach;
- required notice whenever an employee accessed a database containing personal information in good faith for legitimate work purposes that nevertheless exceed the employee's authorization;
- prohibited electronic breach notice by Internet companies to state residents even if their only communications with these state residents were by electronic means, unless the Internet company had obtained E-SIGN compliant consent for electronic notice; and
- required consultation with federal, state *and* local law enforcement whenever a company determined that a breach did not pose a risk to State residents in the event of a breach.

The Attorney General's office strongly supported the Senate approach. Only in a House-Senate conference on the bill were these outlier provisions removed.

### C. Potential Solutions Where State Barriers Arise

#### 1. Preemption

Preemption can be an extremely valuable tool in curbing state barriers to innovation. For example, the preemption provision in the CAN-SPAM Act was critical to preserving the viability of non-deceptive commercial email advertising following passage in 2003 of California S.B. 186.[8] That law created $1,000 per email message statutory damage class action liability against advertisers, senders, and list providers for each commercial email message sent to or from California without opt-in consent. Congress passed the CAN-SPAM Act shortly before the effective date of the California law, averting a huge chilling effect on the use of email as a means of advertising and averting a rash of lawsuits under S.B. 186.

Given the very large volume of state legislation and enormous interest among state policymakers in imposing privacy and security regulation on a conflicting, state-by-state basis, when Congress regulates in these areas, it should do so by adopting uniform national standards. While we recognize that some in Congress are reluctant to preclude innovative state approaches to regulation, once an issue ripens to the level that it is addressed in congressional legislation, preemption is necessary to avoid conflicting state and federal standards.

It is important that the Department's report stress that where Congress regulates in a privacy or data security area affecting the Internet or other areas of innovation, Congress do so by establishing a fair, uniform standard, empowering State AGs to enforce that federal standard,

---

[7] Mississippi H.B. 583 available at http://billstatus.ls.state.ms.us/documents/2010/pdf/HB/0500-0599/HB0583SG.pdf.

[8] http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0151-0200/sb_186_bill_20030924_chaptered.html.

and preempting state law that addresses the same subject matter, while preserving state unfair and deceptive trade practice statutes..

To date, with a few exceptions discussed below, the State Coalition has been successful in opposing state laws that would create inconsistent privacy and data security standards. We are not suggesting that federal legislation is needed in any of the areas discussed in these comments. However, if Congress decides to legislate, it should do so preempting state law.

**2. Dormant Commerce Clause/First Amendment:**

The Dormant Commerce Clause and First Amendment have served as the other legal bulwarks protecting innovation across state lines. It would be very helpful if the Department's report specifically cited the important limits that the Dormant Commerce Clause places on state regulation of interstate commerce over the Internet and other communications networks. and that the First Amendment places on state restrictions on expression on the Internet by teenagers and adults and on state restrictions on advertising.

For example, a host of decisions have struck down state "harmful to minors laws" that attempted to regulate Internet content.[9] The 2004 UT "spyware contract act" was enjoined on Dormant Commerce grounds.[10] Last year, DLA Piper, counsel to the State Coalition, represented several State Coalition members in a lawsuit that resulted in a consent judgment declaring the Maine teenage marketing law, L.D. 1183[11], discussed above on pp. 2-3, likely unconstitutional on First Amendment grounds (the court did not reach plaintiffs' Dormant Commerce Clause theories).

**The Dormant Commerce Clause** guards against barriers to interstate or foreign commerce. The Dormant Commerce Clause doctrine flows from a power affirmatively and exclusively granted to the federal government in U.S. Const. Art I., § 8, cl. 3: to regulate interstate commerce. Because the federal power is exclusive, states and localities may not enact laws or impose regulations that impede the free flow of goods and services across state lines.[12] The doctrine prohibits both protectionist laws that discriminate against commerce from other states in favor of the enacting state as well as state regulations that, although facially nondiscriminatory, unduly burden interstate commerce.[13]

States may regulate commerce that occurs solely within their borders, and, to a limited extent, interstate commerce that affects their citizens. However, the Dormant Commerce Clause prohibits state laws or regulations that:

---

[9] *Johnson v. ACLU,* 194 F.3d 1149 (10th Cir. 1999); *PSINET, Inc. v. Chapman,* 362 F.3d 227 (4th Cir. 2004); *American Booksellers Foundation v. Dean*, 342 F.3d 96 (2d Cir. 2003) ("*Dean*"); *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997).

[10] *WhenU v. State of Utah*, (June 22, 2004), transcript available at http://www.benedelman.org/spyware/whenu-utah/pi-ruling-transcript.pdf

[11] Pub. Law c. 230, codified at 10 MRSA c. 1055, § 9551 *et seq.*

[12] *See Lewis v. BT Inv. Managers, Inc.*, 447 U.S. 27, 35 (1980).

[13] *See Kassel v. Cons. Freightways Corp. of Del.*, 450 U.S. 662 (1981).

(1) directly regulate a means of interstate commerce that by its nature demands uniform national treatment[14]; or

(2) have the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction[15];

(3) would risk "inconsistent legislation arising out of the projection of one state['s] regulatory regime into the jurisdiction of another State"[16]; or

(4) regulate interstate commerce only indirectly, but imposes burdens on interstate commerce that are "clearly excessive" in relation to the law's asserted local benefit.[17] A state statute that burdens interstate commerce will be invalidated in this context if the legitimate local purpose "could be promoted as well with a lesser impact on interstate activities."[18]

Most importantly for state Internet regulation, a string of cases addressing state Internet content restrictions has held that where a state imposes age-screening restrictions that apply to out-of-state websites and the websites must apply them to all visitors because they cannot be sure which visitors come from the regulating state, such regulations violate the Dormant Commerce Clause.[19] This line of authority is very significant in the current Internet environment because IP address-based geo-location is inaccurate in a significant number of circumstances. For example, all blackberry users have IP addresses indicating that they are from Canada and all AOL ISP subscribers have IP addresses indicating that they are from Virginia. Thus, websites that do not collect street addresses cannot be sure whether they are dealing with a resident from a state that imposes onerous regulation. Thus, state laws that apply to the Internet and impose restrictions regardless of whether the defendant is aware of the state of residence of its users have the practical effect of requiring out-of-state commerce to be conducted at the regulating state's direction.[20]

**First Amendment** curbs on state regulation of speech over the Internet are typically better understood. The Supreme Court has made clear that speech over the Internet medium deserves the highest level of First Amendment protection.[21] First Amendment case law also makes clear that the government may not, in advancing its compelling interest in protecting children, reduce adults to receiving only expression suitable for children if less restrictive alternatives would be at least as effective in achieving the government's legitimate purposes. *See, e.g., Communications of Cal., Inc. v. FCC,* 492 U.S. 115, 126 (1989).

---

[14] *See, e.g., American Library Ass'n v. Pataki,* 969 F. Supp. 160, 168 (S.D.N.Y. 1997).
[15] *Healy v. Beer Institute*, 491 U.S. 324, 335-40 (1989).
[16] *American Booksellers Foundation v. Dean*, 342 F.3d 96, 104 (2nd Cir. 2003).
[17] *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).
[18] *Id.*
[19] *Johnson v. ACLU,* 194 F.3d 1149, 1161-62 (10th Cir. 1999); *PSINET, Inc. v. Chapman,* 362 F.3d 227 (4th Cir. 2004); *American Booksellers Foundation v. Dean*, 342 F.3d 96, 102 (2d Cir. 2003); *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 177 (S.D.N.Y. 1997).
[20] *Healy v. Beer Institute*, 491 U.S. at 335-40.
[21] *Reno v. ACLU*, 521 U.S. 884 (1997).

The First Amendment provides strong protection for freedom of expression against state content-based or speaker-based restrictions on speech, and guarantees older minors the right to communicate and to receive information. It acts as an important counterweight against privacy laws that would prevent older teenagers from speaking on the Internet without parental consent.

The First Amendment also protects against overbroad or selective restrictions against advertising over the Internet and other communications media. *See, e.g., Greater New Orleans Broadcasting v. F.C.C.*, 527 U.S. 173 (1999); *Verizon Northwest v. Schowalter*, 282 F. Supp. 2d 1187, 1194(W.D. Wa. 2003) (invalidating state opt-in requirement for use of CPNI).

It would be particularly helpful if the Department of Commerce report explained and discussed the importance of these theories to provide guidance to states in avoiding creating barriers to innovation and freedom of expression.

## II. Responses to Specific Questions in the NOI on State Privacy Laws)

Our comments now turn to supplying what we hope are helpful answers to the Department's specific questions regarding state privacy laws.

The Department's very thoughtful preamble actually understates the volume of state privacy laws. As mentioned above, almost every state has both data breach and at least several other sectoral privacy laws. California alone has more than 20 such laws[22].

### "A. What, if any, hurdles do businesses face in complying with different state laws concerning privacy and data protection?

The largest hurdles typically arise with regard to four types of state laws:

(1) State laws that impose liability in class action lawsuits for statutory damages for non-intentional conduct. These create significant insurance risks and greatly complicate negotiations of arrangements between business entities that touch or secure the data at issue.

(2) State laws that impose hard or soft technology mandates – for example, to implement a specific Internet safety solution, to use encryption, and only encryption, to protect personal data, or an exception for encryption, and only encryption, from breach notification. These distort the market for technology, freeze technology developments, and force some companies to switch to different product or service offerings.

(3) State laws that require a *sui generis* state-specific notice or website configuration, or protocol for handling data.

(4) Widely divergent or incompatible state requirements regulating or imposing liability for the same activity.

[22] For a helpful overview, see the website of the California Office of Privacy Protection, http://www.privacy.ca.gov/privacy_laws.htm.

More generally, simply tracking the huge variety of state regulation is both expensive and burdensome, and for that reason beyond the capacities of small businesses.

**"B. Is there harmonization among state laws governing data protection? Please describe any significant differences among the states"**

**General Data Security Laws:** Specifically with regard to data security laws, until 2008, there was very positive harmonization of state laws (requiring use of "reasonable security measures").[23] This changed with the Massachusetts data security regulations and Nevada data security mandate law.[24] The Nevada law is a particularly sharp contrast. It imposes a technology mandate to use encryption, and only encryption, to protect the type of "personal information" that would trigger a breach notice obligation under Nevada law. The law requires encryption at all times that the personal information is transported or stored outside the premises of a business. It also includes a vaguely worded mandate to comply at all times with the Payment Card IndustryData Security Standard for protection of payment data.

By contrast, in Massachusetts, the legislature left room to authorize other data protection technologies beyond encryption, and eventually the regulator who issued the regulations moved to a technology neutral approach. *See* 201 C.M.R. § 17:00. That state's other requirement to have a comprehensive written information security program if companies maintain personal information about Massachusetts residents may not be understood by many state businesses, but it is well-intentioned and technology neutral.

While Massachusetts' data security statute is technology neutral, the original version of the Office of Consumer Affairs and Business Regulation's regulations to implement the law allowed only encryption as a technology protection measure. These rules were repeatedly stayed, then amended last year to allow other technology protection methods. Nonetheless, this spring, a State Representative attempted to add an amendment rider to the State budget that could have had the effect of restoring the encryption mandate.

For its part, the New Jersey Division of Consumer Affairs initially drafted very problematic, highly specific data security standards to implement the state's data security and identity theft statute, P.L. 2005, c. 226. These draft rules, first circulated in 2007, were based upon medium-sized business data security best practices, but not adapted to small or large organization approaches. Those regulations are still under consideration, but the Department of Consumer Affairs withdrew them in 2008 before they took effect, and has not reinstituted them.

**Payment Card Data Security Laws:** This year, Washington State enacted a much better considered, technology-neutral payment card data security law. The law provides for safe harbors from liability for a breach of payment card data, if a merchant either passed a PCI audit

[23] *See, e.g.,* ARK. CODE ANN. §§ 4-110-104(b), CAL. CIV. CODE § 1798.81.5(b), CT. GEN. STAT. § 42-471, MD. CODE, COM. LAW § 14-3503, ORE. REV. STAT. § 646A.622, R.I. GEN. LAWS § 11-49.2-2(2), TEX. Bus. & COM. CODE § 521.052, and UTAH CODE ANN. § 13-44-202.

[24] *See* MASS. GEN. LAWS CH. 93H.; NEV. REV. STAT. CH. 603A.

within a year of the breach or protects data using encryption (or another comparably effective method based on how encryption was defined in the bill). H.B. 1149, amending REV CODE WASH. CH. 19.255. By contrast, in 2007, Minnesota enacted a different requirement that all merchants delete magnetic stripe and CCV code data within 48 hours or else face strict liability for a data breach involving payment card data. REV. MINN. STAT. § 325E.64. Other proposals have been considered in many states (e.g. CA, TX, IL, WI, CT) and they remain a significant potential barrier to innovation.

**Data Destruction Laws:** State data destruction laws are somewhat harmonized but not totally so. Some states (at least California and Connecticut) require secure data destruction for any personally *identifiable* information, while others require secure destruction for a smaller subset of data elements that are more sensitive. Imposing a secure data destruction requirement for ordinary name and address information is burdensome and expensive.

**Medical Information Laws:** More dramatically, the California Medical Information Act (CMIA) at California Civil Code § 56.36, contains a provision that creates huge ($1,000 per act of release) class action liability for breaches of medical data that involve negligence. This provision creates significant liability risk for the promotion of electronic health records, which is a significant American Recovery and Reinvestment Act and Administration priority. As class action lawsuits brought under this provision proliferate, they risk raising insurance costs for electronic medical records.

**Security Breach Notification:** State security breach notification laws are far more effective than data security mandate laws and can significantly benefit consumers by providing them with information about security breaches that pose some risk to them. Breach notice laws differ from other (more problematic) state laws in that data holders can normally identify individuals who reside in individual states and send them notifications that comport with that state's security breach notification law.

That said, the 46 state security breach notice laws (plus laws in the District of Columbia and Puerto Rico) also contain a fairly wide array of variations in factors that make a difference for compliance (e.g. the event triggering the notification requirement (acquisition, access or acquisition, or access and acquisition), timing of notification, content of notification, regulatory entities that must be notified, when regulator notices must be made, and the content and method of notifying). In particular, it is necessary to draft different notifications for Maryland and Massachusetts, which have unique content requirements for resident notifications.

These variations raise costs and delay notifications without significantly enhancing protection of state residents from identity theft and fraud. While not in themselves a reason for enacting a federal breach notice law, when and if a federal private sector breach notice law is enacted, it should preempt all state notification laws and laws imposing liability for data security breaches.

In addition, a minority of state breach notice laws also contain disincentives to innovation in data security by creating "encryption only" exceptions to breach notice.[25] These exceptions disqualify other technologies that protect personal data from an exception for notifying data subjects and thereby make those technologies less desirable to use in protecting personal information. Encryption may actually make data less safe when keys are stored with the encrypted objects and create significant network security problems because encrypted objects flowing through Internet networks are impossible to screen for viruses and other security threats. In reality, the definitions of personal information in breach notice laws, by requiring that a name be obtained "in combination with" a sensitive data element, also recognize data segregation as providing an exemption from notification. However, this is not commonly understood, and other effective methods, such as access control technologies, do not receive an exception from notification. This sort of "soft" data security regulation distorts the market for security technologies and hinders innovation.

**"C. How does complying with multiple states laws affect organizations' business activities and ability to operate online?"**

**&**

**"E. What approaches do companies take to comply with privacy laws in multiple states?"**

Generally, simply tracking the huge variety of state privacy and security regulation in other states is costly and burdensome, and for that reason beyond the capacities of many small businesses.

Typically, organizations that have the resources to follow the multiplicity of state regulation in this area face a choice. They can segregate and localize data collected from particular states and ask users to confirm their addresses, for example creating variations of their website based upon the response. The compliance alternative is to comply with the most restrictive combination of state standards. For efficiency purposes, organizations almost always choose to comply with the most restrictive state laws. Moreover, there is also some risk that organizations will be found to be negligent in other states if they do not live up to standards required in the more restrictive states.

However, in some cases, where state standards are incompatible in some ways, businesses are forced to expend resources to implement a state-by-state compliance approach – for example, in the breach notice context.

In other cases, businesses decide not to deploy a particular service in a difficult or high risk compliance jurisdiction – for example, a state with *sui generis* data security mandates.

[25] *Compare, e.g*, California Civil Code § 1798.82 (requiring notification of a breach that involves "unencrypted personal information; Del. Code § 12B-101(1) (defining a "breach of a security system" to include the "unauthorized acquisition of unencrypted computerized data . . . .") *with, e.g.,* IND. CODE § 24-4.9-2-5 (technology neutral safe harbor for encrypted data and for data that is "secured by another method that renders that data unreadable or unusable.")

In the case of laws, such as state recording statutes, that reach interactions with websites or consumers in a particular state, they may forego entirely deploying an innovative service that is lawful in most states because of litigation risk in a minority of outlier states that project their law outside of their states.

**"D. What types of existing state laws have the greatest impact on companies business models?"**

Technology mandates or technology preferences are the most problematic for innovation. These laws prevent or strongly discourage innovation to find better methods for securing and storing data. The Nevada data security encryption mandate law and the strong preferences for encryption in many breach notice laws are prime examples.

Laws that impose class action exposure for statutory damages or multipliers or criminal penalties have a particularly strong chilling effect. Even if conduct is very likely legal, legal uncertainty is usually enough to deter companies from innovating in the area.

Laws that apply outside of the states' borders also have a major impact. The Maine teenage marketing law (now repealed) placed sweeping restrictions on the collection and transfer of personal information about minors without consideration of how the law could logically be enforced just in Maine and without any consideration of its unintended consequences for free expression. The breadth and exposure of this law were so broad that they left in-state and out-of-state businesses little choice but to sue to enjoin the law.

More generally, in an era where for efficiency purposes data may be stored or delivered in many different states, state-specific data security laws are an impediment to innovation. It is many cases unworkable to know where personal data will be stored, and creating varying risks on a state-by-state level introduces an element of risk and legal uncertainty that is a barrier to innovation.

**"G. What future directions in state law are anticipated? Does the variety of technology-specific state laws help individual Internet users exercise their rights, or does it create confusion for consumers?"**

Based upon our experience following state privacy and security regulation over the past decade, we expect future developments in at least the following areas:

- Regulation of social networking sites
- Smart grid regulation (see the next paragraph)
- Online marketing to teenagers/children

- Mandates to use specific technologies or methods to protect data security (particularly for payment card data)

- Privacy regulation of IP addresses

- Requirements to retain or quickly furnish evidence to law enforcement.

Smart-grid technologies are a new technology development that is at prime risk for inconsistent regulation. Only recently, the California Public Utilities Commission released a proposed decision adopting requirements for smart grid deployment.[26] Noting that there are subtleties and complexities to privacy protections, the Commission stated that further comments and deliberation would be required, which would occur after adoption of the proposed decision. Nonetheless, in its conclusions of law, the Commission provides a preview of the extensive range of privacy protections that it is interested in, by stating that "[i]t is reasonable to determine the current state of privacy actions by asking utilities, as part of their Smart Grid deployment plan, to answer the following questions concerning the data of customers:

a. What data is the utility now collecting?
b. For what purpose is the data being collected?
c. With whom will the utility currently share the data?
d. How long will the utility currently keep the data?
e. What confidence does the utility have that the data will [be] accurate and reliable enough for the purposes for which the data will be used?
f. How does the utility protect the data against loss or misuse?
g. How do individuals have access to the data about themselves? And
h. What audit, oversight and enforcement mechanisms does the utility have in place to ensure that he utility is following their own rules?[27]"

Other than breach notification, which is self-activating, it is far from clear that state-by-state regulation in these areas will help consumers to exercise their rights, as consumers have little awareness of state privacy requirements. For example, in 2006, a new "Shine the Light Law" went into effect in California empowering Californians to obtain a full list of third party entities with whom companies had shared Californians' personal information for marketing purposes. *See* Cal. Civ. Code § 1798.83-.84. Many businesses changed their business practices to conform to this requirement, yet receive almost no requests. Uniform federal standards tend to be more broadly understood and therefore more effective for consumers.

**"H. Have technology specific state privacy laws affected online innovation and business development and, if so, how?"**

As discussed above in these comments, encryption mandates have affected innovation

[26] Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, Rulemaking 08-12-009, California Public Utilities Commission (May 21, 2010).
[27] *Id.* at 114-115.

and business development. Both hard mandates and soft encryption preferences – for which some encryption vendors have lobbied – have played a key role in making encryption the standard data security solution for businesses. We believe that they have discouraged investment in other solutions.

Similarly, recording statutes have slowed innovation in metrics solutions for online services and have stopped network-based behavioral advertising in its tracks. State two-party consent recording statutes are a huge barrier to innovation in wireless and wireline communications services. Two-party consent is typically impossible to obtain in the Internet context. These laws were typically drafted before the Internet was widely used as a means of communication, and carry criminal penalties and contain exposure at $1,000 per violation in class action lawsuits. However, whether they apply depends upon whether courts will interpret capturing, for example, URL destination information, as intercepting contents. The laws create legal uncertainty, for example, for services that conduct network-level metrics on Internet usage. These laws should be preempted if Congress addresses online privacy legislation.

We are also concerned that as lawsuits under California's CMIA, Civ. Code § 56.36, proliferate, they will raise the insurance costs for electronic medical records solutions.

## III. International

Barriers to innovation flowing from non-U.S. privacy and data protection laws are significant. Three technology-related examples are as follows:

**Data Transfers:** Even using model clauses approved by the European Union, it is both expensive and slow to effectuate compliant data transfers from all the E.U. member states to other parts of the world other than the handful of jurisdictions deemed to provide "adequate protection" or to the U.S. under the U.S.-E.U. Safe Harbor Agreement. Half of E.U. jurisdictions require prior approval of the clauses and some take as long as four months to finish their reviews. Israel, Hong Kong and Mexico will all likely require different contractual provisions to comply with their laws. Even in Europe, there is no one-stop-shop filing option for these agreements, and filing and translation requirements vary widely among E.U. member state jurisdictions. This adds significant cost and delay to cloud computing, global IT help desk support and a wide range of other services that require trans-border data transfers.

**Social Networking:** The laws of many E.U. jurisdictions require the consent of all individuals in a photograph before a photograph may be posted on a social networking site or photo-sharing site. This has the effect of mandating take down obligations for all such photos posted on public sites. It also complicates employer use of collaborative work social networking applications that permit posting of photographs, since employers must require employees to obtain the prior consent of all individuals in the photo before posting.

**Online Advertising Analytics:** On their face, European opt-in consent requirements require not only notice, but also the affirmative consent of Internet users. However, entities in the Internet advertising eco-system that do not have a direct relationship with consumers are

unable to obtain consent. They depend upon the website owner, advertiser, or network advertiser to obtain consent. While Data Protection Authorities in E.U. member states have not enforced the opt-in requirement aggressively in this context, this relationship creates significant uncertainty for advertising companies that locate with in the E.U.

**Concern About U.S. Government Access to Data Stored in the U.S.:** There is also significant concern, particularly among foreign governments and data protection authorities, about allowing their data to be stored in the U.S. because of (unjustified) concerns that the U.S. government will secretly obtain access to that information. This impedes sales of some U.S. technology solutions, including hosting and data center solutions, abroad.

**What Models for Protection of Privacy Rights Across Borders Have Proven Effective?** The International privacy barriers to innovation are an area where the Department can play a critical role. The Department already has a strong track record of success in this area through its work on the U.S.-E.U. Safe Harbor Agreement, which is the single most helpful international privacy harmonization agreement for businesses achieved to date. Every year, the Safe Harbor saves U.S. and European companies hundreds of millions of dollars in compliance costs. It drives U.S. companies to implement a larger range of fair information practices and is fully enforceable by the Federal Trade Commission.

The Department is a critical representative of business and economic considerations in international data protection *fora*. The U.S. private sector does not have standing to participate effectively in these discussions and while it appreciates the FTC's work in these *fora*, the Commerce Department's presence has been missed.

**How might privacy regimes in the U.S. and other jurisdictions across the globe be harmonized?** The Department's tireless efforts to nurture the APEC privacy framework are very valuable both to demonstrate the diversity of privacy solutions in the world and to show the effectiveness of a multi-national system where data receiving organizations commit to follow an accountability framework. They show a diversity of solutions for data protection and avoid isolation of the U.S. approach to privacy.

Harmonization of substantive laws appears very unlikely and impractical, although a globally harmonized approach should be the ideal way forward.. It is important to recognize that full harmonization has not occurred even within the E.U. data protection regime. Requirements vary among member states. While the mutual recognition procedure for Binding Corporate Rules applications is a welcome step forward for companies that can afford to undertake that process, only 19 E.U. member states currently work jointly on BCR applications[28], and several EU member state DPAs refuse categorically to recognize them.

Because nations will not jettison their national legal regimes, a gradually expanding mutual recognition model may hold promise in extending the safe harbor approach to other jurisdictions. The best hope for reducing the significant barriers to innovation caused by

[28] These are Austria, Belgium, Bulgaria, the Czech Republic, Cyprus, France, Germany, Ireland, Iceland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovenia, Spain, and the UK.

conflicting international privacy regimes is to work toward cross-border recognition of compliance initiatives, along the lines of the ground-breaking U.S.-E.U. Safe Harbor Agreement.

Like the Safe Harbor Agreement, receiving entities would make enforceable commitments to follow the framework, subject to enforcement if those representations were false. This way, data protection commitments could follow personal data wherever it travelled, preserving the privacy guarantees that data subjects reasonably expect. At the same time, the costs and inefficiencies of the current data transfer model would be avoided and national boundary barriers to cross-border innovation would be reduced significantly.

Respectfully submitted,

_____
Jim Halpert
General Counsel

Adrian Copiz
Counsel
(202) 799-4000

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Monday, 7 June 2010

To: **The National Telecommunications Administration** at
U.S. Department of Commerce, 1401
Constitution Avenue, NW., Room 4725,
Washington, DC 20230.

Re: **Information Privacy and Innovation in the Internet Economy**
**Call for public comment**

This letter is written in response to the call for public comment made in the [Federal Register: April 23, 2010 (Volume 75, Number 78)], [Page 21226-21231], [Docket No. 100402174-0175-01].

We note the following text from the above call:

> *This Notice of Inquiry seeks comment on the impact of the current privacy framework on Internet commerce and innovation, both from the commercial and consumer perspective, as well as ways in which it may be necessary to adjust today's privacy framework to preserve and even enhance innovation and privacy in our new web-centric information environment. The questions below are intended to assist in framing the issues and* ***should not*** *be construed as a limitation on comments that parties may submit.* ***The Department invites comment on the full range of issues that may be presented by this inquiry.***

Thank you for making this important call for public comment. We would like to respond to this call by providing 6 files of input in 3 bundles. The title of the 6 files is as follows:

**INPUT 1)** http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html
**INPUT 2)** http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html
**INPUT 3)** "Part 4: The need for the EC to fund the development of an electronic requirements management process to support the conversion of existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified requirements model that also supports national and regional variations."
**INPUT 4) "**Part 5: A) The need to evaluate the effectiveness of data depersonalisation techniques and it's impact on the community; and B) Measuring the wider impacts of unauthorised information."
**INPUT 5)** "Part 6: A) Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments, and B) We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems."
**INPUT 6)** "Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks"

**Before describing Synaptic's input, I would like to provide some context.**

Synaptic Laboratories is a **micro** Private Technology Company managed by Australian citizens with Directors in Gozo, Malta (Europe) and Australia. We are operating internationally on a 'virtual' basis with ten years of completed cross domain research and design. Our core business is cutting edge cyber security solutions for Today's Internet (and the Future Internet).

We are active in the US Federal Cybersecurity initiatives:

- having made submissions to the NITRD Cyber Leap year public Requests for Input[1]
- having participated at the 'by invitation' NITRD Cyber Leap Year Summit where 6 of our proposals were carried forward in the Participants Ideas Report[2]
- having presented further information on these proposals[3] at the peer reviewed Oak Ridge National Laboratory 6th Annual Cyber Security and Information Intelligence Workshop (CSIIRW)[4] held in April 2010 and also at the IEEE Key Management Summit held in May 2010, where we were a sponsor[5].

Specifically Synaptic Labs are focussing on Global-scale Identity Management and Cryptographic Key Management (IdM/CKM) along the lines called for by the U.S. Department of Homeland Security in their Nov. 2009 "*A Roadmap for Cybersecurity Research*" publication[6], and on next generation Internet protocols with privacy enhancing features as published in the NITRD NCLY 2009 Participants Report[7].

Synaptic Labs was one of the few foreign participants invited to the NITRD National Cyber Leap Year Summit, and we have been acting as a bridge between US and European Government Level security initiatives, seeking to bring to the attention of the other overlapping initiatives where synchronisation and international normalisation may be possible.

Synaptic Labs has made submissions to European Calls that correspond with or are the equivalent in most regards with the subjects of your Call. Unfortunately, due to work pressures and lack of time we are unable to repackage our European submissions to specifically address your Call, however we are forwarding now copies of our European submissions trusting that you will easily find the content relevant or your purposes. We have previously forwarded at least one of these submissions to our contacts at NIST and Miles Smid (Orion Security, formerly at NIST) had this to say [quoted with permission]:

> *"I think that this is an interesting idea and indicates how standards requirements will need to be managed in the future."*

---

[1] http://synaptic-labs.com/resources/synaptic-publications/104-input-to-ec-and-us-funded-ict-initiatives/348-pub-synaptic-labs-3-inputs-to-nitrds-call-for-qleap-aheadq-ideas-2009.html

[2] http://synaptic-labs.com/resources/security-bibliography/105-security-organisations-projects-and-calls/331-bibliography-us-nitrd-ncly-security-summit-2009.html

[3] http://synaptic-labs.com/resources/security-bibliography/106-security-conferences/340-bibliography-us-ornl-csiirw-6-2010.html

[4] http://www.csiir.ornl.gov/csiirw/10/index.html

[5] http://2010.keymanagementsummit.org/ and http://storageconference.org/2010/Presentations.html#KMS

[6] http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[7] See our extracts from this report here: http://media.pqs.io/pub/papers/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

## SYNAPTIC LABS' FIRST BUNDLE OF INPUT INTO YOUR CALL

The first bundle we are providing is simply a copy of the deliverables from a European Commission funded project that we expect you will already be aware of, but just in case, we provide them now. The project we refer to is called Think-Trust[8] and it was tasked with issuing a Call for public input on very similar subject matters as your Call. These deliverables are available to the public and we believe you will find them relevant and of interest. Synaptic Labs actually made extensive inputs to this European project (See second bundle below).

Think-Trust (FP7-216890) is a project funded by the European Commission's 7th Framework Information Society Technologies (IST) Programme, within the Unit F5 ICT for Trust and Security. It is investigating Trust, Security, Dependability, Privacy and Identity from ICT and Societal Perspectives. Think-Trust is a Co-ordination Action (CA) project. It started on January 1st 2008, receives funding of 580,000 Euro and has a 30-month duration.

Think-Trust produced a list of research challenges which need to be addressed to work towards a trustworthy ICT environment. Think-Trust's deliverables make comment on a wide range of issues on information privacy and the Internet and these, in our opinion, directly relate to your call on "Information Privacy and Innovation in the Internet Economy".

In this letter, Synaptic submits the Think-Trust's two deliverables D3.1A and D3.1B **as input into your process.** Please find the two documents freely available for download here:

> **INPUT 1)** http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html
> **INPUT 2)** http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html

## SYNAPTIC'S SECOND BUNDLE OF INPUT INTO YOUR CALL

As previously mentioned, Synaptic Laboratories is a MICRO research and design company. We are actively participating in US and EU security initiatives, however our resources are inherently constrained.

We kindly ask for your understanding with regard to our second bundle of input. We have thoughtfully selected a subset of 3 out of our 6 submissions to THINK-TRUST's D3.1A and D3.1B call **unmodified**. We have carefully chosen these submissions as they are most relevant to your call.

We ask the "Information Privacy and Innovation in the Internet Economy" study group to kindly consider the CONTENT of the arguments found in these publications on their own merit, in respect to your activities, even though they are not framed directly in response to your call. We note that our submissions to Think-Trust made extensive reference to US Federal Initiatives and possible areas of international overlap.

Please find the three documents, **as input into your process:**

**INPUT 3)** "Part 4: The need for the EC to fund the development of an electronic requirements management process to support the conversion of existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified requirements model that also supports national and regional variations."

> (Also available at: http://media.pqs.io/pub/papers/TT/20100127-TT-D3-1b-P4.pdf )
>
> **Relevance**: As noted in your call "*Small and medium-sized entities (SMEs) and startup companies face the same data protection laws and guidelines as their larger counterparts, but with fewer resources.*" This proposal suggests that relevant privacy laws, national and international, such be unified in an electronic requirement model, enabling small organisations to quickly identify what

[8] http://www.think-trust.eu/

requirements they must satisfy in their software and business processes. Many other benefits are outlined.

Miles Smid (of Orion Security, formerly of NIST) had this to say about this proposal:

> *"I think that this is an interesting idea and indicates how standards requirements will need to be managed in the future."*

**INPUT 4) "**Part 5: A) The need to evaluate the effectiveness of data depersonalisation techniques and it's impact on the community; and B) Measuring the wider impacts of unauthorised information."

( Also available at: http://media.pqs.io/pub/papers/TT/20100128-TT-D3-1b-P5.pdf )

**Relevance**: Your call asks for information on data depersonalisation and re-identification technologies. This is excellent. In section A) we propose that a formal Government level study is required to evaluate the state-of-the-art, study the behaviour of the market in using depersonalised data, and to use that data to set guidelines and best practices. In section B) we call for a study to measure the cost of unauthorised information disclosure. This information is required to help establish "appropriate levels" of security protection appropriate to the damage of privacy exposure to the relevant stake holder(s).

**INPUT 5)** "Part 6: A) Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments, and B) We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems."

( Also available at: http://media.pqs.io/pub/papers/TT/20100129-TT-D3-1b-P6.pdf )

**Relevance**: Your call asks for information on New Privacy-Enhancing Technologies and Information Management Processes. This is excellent. As you are no doubt already aware, the EU is a strong proponent for privacy-enhancing technologies. In section A of part 6 of our input to Think-Trust we draw out a point that certain privacy enhancing technologies should be rejected if that proposal acts as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed. In section B, we take a broader look at privacy and accountability in security systems and observe that there is a need to explicitly require all stake-holders to be equally accountable and protected in all information processing and security systems.

## SYNAPTIC'S THIRD BUNDLE OF INPUT INTO YOUR CALL

Another European organisation Synaptic has participated with is ENISA.

The European Network and Information Security Agency (ENISA) is an agency of the European Union. ENISA was created in 2004 by EU Regulation No 460/2004 and is fully operational since September 1st, 2005. The objective of ENISA is to improve network and information security in the European Union. The agency has to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market.

In 2009-2010 the European Network and Information Security Agency (ENISA) www.enisa.europa.eu made a call for **Scenario Proposals on Emerging and Future Risks**.

Synaptic Labs' proposal to ENISA was selected for study in 2010 in the area of Trust and Privacy. In this area ENISA was looking for proposals to identify major risks in the area of trust, security and **privacy** posed by new and emerging technologies and applications. ENISA restricted scenario proposals from including proprietary technologies, and we complied with this restriction. Synaptic participated in this Call with a scenario focused on the risks associated with the global dependency upon Public Key Cryptography (PKC)

and Public Key Infrastructure (PKI). Synaptic's publication outlined **90 different threats and issues** under 8 headings identified within the submission. It has a 3 page executive summary and a further 56-page supporting document including extensive references.

This publication touches on the **known** future risks of widely anticipated **complete privacy failure** due to continued use of public key technologies (on account of Peter Shor's Quantum Algorithms and their derivatives), issues of single point of trust failure in the civilian certificate authority that **allow identity fraud** to be performed (which can **result in privacy loss**), and also raises serious concerns of **data ownership and personal control over biometric data** which is traded internationally (and protected using known at risk Public Key Technologies).

Our publication outlines how these issues collectively **impact the individuals' fundamental rights** and opportunities for development in the community. It also shows how this negatively impacts the public interest because **self-determination is a necessary condition for the functionality of a liberal democratic polity** which is based on its citizens' ability to act and to participate.

Please find the following document, **as input into your process:**

**INPUT 6)** "Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks"

( Also available at: http://media.pqs.io/pub/papers/ENISA/20100330-ENISA-FR-Synaptic.pdf )

Thank you again for a) making the call for input and b) for your understanding in our resource constraints that have limited our ability to re-frame our input specifically to your process.

Yours sincerely,

Benjamin Gittins

Chief Technical Officer
Synaptic Laboratories Limited
June 4, 2010

*Grant agreement number:* 216890


*Project title*

# Think Tank for Converging Technical and Non-Technical Consumer Needs in ICT Trust, Security and Dependability

*Instrument*

Coordination & Support Action

*Deliverable reference number and title*

D3.1a Recommendations Report (interim), including Annexes on WGs

| | |
|---|---|
| *Start date of project:* | 1st January 2008 |
| *Duration:* | 30 months |

*Organisation name of lead contractor for this deliverable*

Ecole Nationale Supérieure des Télécommunications (Télécom ParisTech)

*Editor*

Michel Riguidel
michel.riguidel@telecom-paristech.fr

# Contents

# Introduction and Background

The **Think-Trust** project is a Coordination Action whose main aim is to bring together the European R&D community in the field of Trust, Security and Dependability (TSD) and other important non-technical stakeholders that have an interest in the area and can contribute in a meaningful way, in the development of present and future programmes of Research and Development for ICT for Trust, Security and Dependability.

The approach taken in the Co-ordination Action is:

1. To consult with the users themselves, with those responsible for facilities and services, and with the researchers and developers providing the technologies, through a sequence of well targeted workshops with preparatory contribution and comment via our web-site; this stage will agree an outline framework that allows common understanding of requirements and of possibilities for solutions;
2. To set up a ***Think-Tank*** (RISEPTIS Advisory Board) of experts and representative voices to analyse and review the requirements and potential responses, which will ultimately lead to initial recommendations and options;
3. Take these back to the constituencies through workshops and web-based consultation process;
4. Compile final recommendations for future European R&D and for preparatory actions in other areas critical to long-term acceptance and satisfaction in the Information Society.

This Deliverable sets out the interim findings of the project concerning the main challenges and key research priorities in the area of Trust Security and Dependability. Section 1 of the document sets out the main issues relating to Security and Trust in the Future Internet: Section 2 sets out the main Security and Trust Challenges and Section 3 identifies four key research priorities :-

1. Security in (heterogeneous) networked, service and computing environments
2. Trust, Privacy and Identity Management (metasystems) Infrastructures
3. Underpinning Engineering Principles and Architectures that support Transparency / Accountability Architectures and Measurement
4. Data, Policy Governance and Socio-Economic aspects

The Deliverable focuses on detailing the TSD research agenda which has been outlined in the report currently being drafted by the RISEPTIS Advisory Board. The Deliverable elaborates in more detail the four areas above, which will be identified in that report. This is an interim recommendations report and will be further refined and developed during the remainder of the Think-Trust project.

This interim report sets out the scope of the challenge of providing **Trust and Security** in a new age of information processing in daily tasks, and a vision that identifies the areas where research, development and deployment of technologies will be necessary. An outline of accompanying measures in non-technological areas is also given. The final version of this report will provide specific recommendations and priorities for future work.

# 1. Security and Trust Context of the Future Internet

This section provides background information on a broad range of key issues that need to be considered when discussing Security and Trust in the Future Internet, providing a context for the challenges and research priorities in sections 2 and 3.

## 1.1 Ubiquity of the digital kingdom

### 1.1.1 IT evolution: Moore law, interconnection and usages' appropriation.

Progress in microprocessor technology, new paradigms in communication technology and the emergence of groups of networked sensor-actuators enable a vision of a new age for information processing in daily tasks.

The values of modern civilization are inevitably moving towards a more immaterial virtual world. Continuous electronic miniaturization, the acceleration of communication networks' performance and the inexorable deployment of computing infrastructures is creating a digital urbanization where everything appears closely connected, facilitating inter-communication and access to services and information. The imperial conquest of digital technology in all areas is accelerating the rate of expansion in the volume of computer data and of the massive integration of software into our daily lives. This computerization process is further accentuated by the widespread interconnection of networks and by digital convergence, which is making computing, telephone and audiovisual information increasingly compatible and interoperable. Progress in wireless technology has made possible the popularisation of mobile communication and has very substantially changed the way that businesses operate. Seamless digital technologies, i.e. the establishment and interoperation of the three complementary ubiquitous environments of computing (information stored, processed and presented here and now), communication (access anytime, anywhere, using the available best channel) and storage (collected, stored, described and displayed information and knowledge, available anywhere, anytime) will gradually surround individuals, creating a tight mesh and a digital built-environment, changing usage and having a profound impact on civilization's values. The value of digital possessions may soon exceed that of material ones, for individuals, businesses and state institutions.

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context.

Furthermore, networks and future communication systems will have to move on from the obsolete concept of end-to-end connectivity (as in the current Internet) and embrace situations in which nodes are devices which cooperate freely and spontaneously in the absence of centralized services. Ubiquitous communication systems will demand new architectures based on the independent devices, connectivity reduced to fragments and spatial awareness of the nearby environment and local data through different nodes in the network.

The concept of end-to-end is not in itself, obsolete. As long as single, point –to-point communications exist (unicasting), so will end-to-end. Unicasting would even seem to be the favoured mode of communication, both in the Internet and social sense. What is new, and constitutes the added value of the digital environment, are the new cooperating devices (instead of a centralized service) and the procedures for the establishment of these end-to-end connections.

### 1.1.2 The two frontiers: infinitely small (tiny objects) and large (complexity).

IT research must today address the two opposite aspects of the new boundaries of the immaterial world:

- Computing of the derisory: minuscule, sometimes invisible objects, with rare resources (in Watts, Mips, Bytes, Bits per Hertz and per second), possibly non-identifiable but only traceable , will be the terminations of a network with no longer a few billion capillaries, but rather several Tera nodes. Research on nano-architectures, nano-applications, and nano-protocols, will transform the new network suburbs. Undoubtedly, end-to-end will no longer

mean anything, and traditional protocols - IPv4 (and even less IPv6 !) will not withstand such brutal economies in computing and communication resources. New computing models will become necessary. We will have to segment models for computing, storage, and communication, which will only be applicable within a certain technological niche. Computing is not fractal!

- Computing of the gigantic and inextricable: poly-infrastructures (Internet, GRID, GSM, 3G, Galileo/GPS, the Internet of objects, Earth observation satellites) will be the new worldwide constructions of the (Violent) Virtual Village: interconnected, compatible, yet gigantic, inextricable, barely controllable and extraordinarily fragile. Computing of the gigantic means new services (Internet Telephony, Skype, etc.), which are also tools for surveillance, anticipation, crisis management etc.

### 1.1.3 Two structuring paradigms: virtualisation for the global and embodiment for the local.

In practice, these two opposite aspects complement each other and result in a duality, since the infinitely small strengthens gigantism, and vice versa. The mass of connected manufactured items that surround us will result in an environment characterized by excess. These extremes are addressed by two fertile, yet opposite, computing notions: virtualization and embodiment.

#### 1.1.3.1 Virtualisation.

**Virtualization** is a powerful technique that has developed from its early use in large CPUs in the 1960s. It enables the construction and operation of composite *virtual* computing entities with desired properties and functionality from available *real* or possibly other virtual entities. It involves juggling with computing entities of various orders to create other, more effective, computing entities, by reducing the complexity of a system whose handling has been changed by applications and services. Just as the object approach has changed the way software is manufactured, the virtualization approach has transformed the treatment of computing architectures. Virtual memory has changed the writing of memory hungry applications; the Java machine has made it possible to encapsulate computer programs in HTML web pages, which has determined its success. Virtual private networks have generated digital trenches in public networks, which has created a certain privacy in a global no man's land and allowed companies to operate over the Internet. VLAN technology has made it possible to dissociate the logical LAN infrastructure from the corporate network and the physical infrastructure, which has largely contributed to the success of these networks. Virtualization enables the frontiers between two hardwares, or between a hardware and a software, to be abolished, the forms and standards between two databases to be erased, domains that differ in terms of management policy to be crossed, packets to be routed differently, and borders between technologies and heterogeneous networks to be crossed. Above John von Neumann's hardware and software subdivision, a virtual plain is in the process of settling permanently throughout computing architectures. All overlay structures, all superposition networks are also paradigms derived from this virtualization operation.

#### 1.1.3.2 Embodiment, adaptation to the immediate environment

**Embodiment** is a notion contrary to virtualization that remains little used. While virtualization aims to annihilate figures that are rebellious to transparency and to a seamless world, embodiment makes it possible to design and reveal dynamic forms and, at the same time, creating intelligence locally, where there was none. Artificial intelligence and robotics are renewing themselves. While they proclaimed premature success in the 1980s, a new effective and pragmatic school is emerging with the fundamental notion that knowledge is not a result of information or computing. Intelligence is not only about computing, it demands a body (in the physical sense). The first successes are in the field of robotics recognizing their surroundings, understanding situations, and assisting individuals in everyday tasks. It goes without saying that this powerful concept will have considerable applications in the distributed world of sensor networks, of middleware, in security to supervise scattered situations and in computing in general.

While nowadays we have distributed systems and embedded systems, in the future we will supplement this range with overlaid systems (corresponding to virtualization) and embodied systems (corresponding to embodiment).

## 1.2 The three periods of a digital roadmap

### 1.2.1 The architecture- and format-cleaning period

This decade, digital technology has experienced a setback, namely, digital convergence, i.e. an ad hoc re-allotment of both architectures and formats. This attempt at realignment has consisted of cleaning up, retouching computers, televisions and telephones to make them interconnectable and interoperable. Digital technology has little connection with physical reality: few sensor networks, few robots (only 1 million in existence in 2008). Information technology is still operating behind closed doors. However, even a web in tatters, these interconnecting networks will conquer other territories and could absorb the telephony, 3G and television infrastructure. In its original, pioneering form, the web was an electronic whiteboard (the term web in fact comes from the acronym Wide Electronic Board), which became fragmented into pages scattered across different sites during the 1990s, which search engines attempted to classify and then recover; it is now in the process of transforming itself into a series of dynamic sheets of personalised information, virtually attached to every nomadic citizen. Thus the torn fabric of the internet is already showing its seams, stitches and hems: the search engines pick up these stitches, patches and hems which connect web-pages with links, peer-to-peer file download applications link processors and discs of adjoining computers in clusters to calculate and exchange in an evenly-distributed manner.

### 1.2.2 The ebullient period of reconciling virtual and physical realities

This retrenchment should change as the system evolves towards a reconciliation phase in which the virtual and physical, links between technology and reality, are reconciled. We are seeing an emergence of contactless smart cards and radio-frequency recognition labels (parcel logistics, pet tagging, etc), networks of sensors in towns (multiple-window cameras), in the countryside (forest fire and earthquake detectors), in businesses (real-time warehouse inventory, mobile vehicle fleet sensors), networks in our homes and cars, personal assistance robots, telediagnostics etc. Whilst the current internet has connected 500 million computers and mobile phones have connected 2 billion people, the Internet of Things should connect 1000 billion objects. Malfunctions and attacks on these networks could cause widespread chaos.

With globalisation, China's increasing openness and new actors emerging onto the international scene, digital networks (which are a geostrategic challenge) are in danger of being structured around language and culture, exposing new models, counter-models and alternative models, whilst avoiding the providential solution of a model which is both unique and pseudo-universal. The future cyberspace is in danger of being structured around navigation and positioning infrastructures (GPS in the US, Galileo in Europe, Glonass in Russia, Beidou in China). The natural fragmentation around these new continental plates will create a digital tectonic which is likely to see the pull of regional standards drawing a new set of decentralised networks.

### 1.2.3 What lies beyond the horizon: IT at atomic level

In the future a new digital era of Nano, Bio, Info and Cogno (NBIC) will dawn, in which humanity will be working at atomic level (nanotechnology), with living tissue (bio-geno-technology) and photons (quantum computers). This will radically change civilisation. Bits of information technology will be able to pass between the cells and atoms of living beings in order to manage and control this invisible world. A completely new level of vulnerability and threat could arise from this nanoworld: Nano warfare, the trading of living cells, quantum warfare for breaking State secret codes; in short, a new confrontation at atomic level.

### 1.2.4 21st century science and information technology

Those countries that wish to remain in a pre-eminent position will have to learn to master Angström ($10^{-10}$ m) technology at atomic level, and attometer technology ($10^{-18}$ m) at quark level. Having taken on board the Einstein-Minkowski space-time theories, humanity should now be able to move beyond our 4-dimensional view, and begin to accept theories of a universe which comprises more than 4 dimensions (some of which are nanoscopic), and more than 4 forces. T Kalusa's first theories date from 1921! They remained in obscurity for over 50 years. String theory, branes and supersymmetries should come into their own within the next twenty years.

Information technology will become an integral part of everyday life, running through the very veins of reality and nature, creating a new thinking machine on a planetary scale, a new realm, alongside the animal, mineral and vegetable kingdoms. The new information technology of the 21st century will organise this invisible artificial world, this vast ubiquitous world. It will be a world away from the current internet, with its primitive architecture and which is so wasteful of energy and fuels the digital divide.

## 1.3 The fragility of the digital world

### 1.3.1 Threats and vulnerabilities

Despite the unquestionable success of digital technology, the resulting information systems are vulnerable because it is in the nature of their construction that the digital content is independent of its physical support. The digital environment is thus volatile: it can easily be duplicated or destroyed, stolen or falsified. Furthermore, since digital documents are read and written with equipment that uses software, and software nearly always contains errors or bugs, the possibility of some kind of malfunction is ever present.

In this way as society becomes increasingly dependent on digital technology, the environment provided by the technology becomes increasingly fragile. A major risk is inherent because our daily environment is determined by these complex systems that can break down or be paralyzed by malicious action, accident or failure. Since these systems are interconnected and interdependent they are exposed to domino effects that can quickly spread malfunctions in the operation of each system. Our attachment to these tools, which in the case of the Internet and mobile phones sometimes approaches addiction, does not help this situation of dependence on digital structures.

Lastly, let us not forget that the future of ICT raises human and social issues. What type of digital systems should we consider for daily lives that are compatible with our values; how should we view the relationship between knowledge and the capacity of physical persons and their cultural and emotional requirements? What are, what will be and what should be the social implications of the development, deployment and use of such systems? The evaluation of technology on a precautionary basis should guide the design of tools for the construction of ICT, ultimately not purely driven by the evolution of technology, but with a basic objective of improving the quality of life.

### 1.3.2 Is the Web about to unravel? The Internet is broken

Over the last few years, the very fabric of the internet has started to come apart, distended by new usages, pulled in opposing directions by successive hordes of new arrivals and defaced by the cyber-delinquents who exploit the web's pseudo-anonymity with impunity. The Internet, the network of networks, was never designed to be used on such a vast scale. Its size has been grossly overextended by the power of its services and the performance of its high-speed connections, which are inundated with increasingly voluminous content. 1.4 billion Internet users generate a monthly traffic volume of 10 exabits, requiring connections which can download 100 gigabits per second, to run such popular applications such as Skype, eBay, YouTube, Facebook, Amazon, BitTorrent, SecondLife, etc. The strength of the internet lies in its ability to have stood up to this new context, but its weakness is that is that it is unable to change its fundamental nature.

The hard-line internet extremists continue to trot out the dogma of network simplicity and performance, intelligence at both ends, free usage, transparent architecture and protocols and ease of connection. These properties have diminished over time such that we now see false simplicity with patches and spot repairs, inflexibility and over-sizing to absorb the multimedia

tsunami, complexity within the core of the network, a false idea of free access as, for example, someone has to fund investment in such innovations as fibre-optics etc., software obscurity, aggressive usage of standard protocols, the inability to manage mobility, partiality of governance, security lapses through identity fraud, a disregard for personal data protection, following insidious surveillance or even digital inquisition. The old internet model has coped with all of this.

The current Internet was unable to adapt either to mobility, or to modern security. The Future Internet (FI) will be polymorphous, created on the basis of different infrastructures. Therefore, it is necessary to incorporate into the Future Internet the split, the dynamic and evolving nature of digital systems and a strong holistic security design.

Our current information technology paradigms are in the process of being dissolved. The dichotomies between computer and networks, between hardware and software, between applications and services, between the logical and the virtual, between software and information, are in the process of being blurred or, more precisely, the terms of the division are radically changing meaning. Consequently, the security paradigms need to progress at the same rhythms as IT evolution.

## 1.4 Sovereignty and dignity (individuals, groups, states)

The values of modern civilization are inevitably moving towards an immaterial world. Continuous electronic miniaturization, the acceleration of the performance of communication networks and the inexorable deployment of computing infrastructures is creating a digital urbanization which facilitates communication and access to information.

Gaining control of information and its transport, enforcing the protection of owners' intellectual property, protecting teenagers against illicit acts and ensuring the security of stored, processed or conveyed data are becoming the major challenges of our countries in Europe. Protection of sensitive digital commodities (in the form of data, documents or other creative work) belonging to responsible entities (their authors or owner organizations) represents the new challenge of the administrators of the networks being woven and deployed all around us. The freedom of individuals, the survival of companies and the future of countries in all the fields of endeavour, whether in private or public life, in the civilian world or in the defence establishment need to be considered.

The digitization of the developed world is in progress, and the digital universe is intruding into all sectors of activity: industry, trade, finance, defence, administration, health, education, justice and environment as well as personal and social. The stakes of information security at the dawn of the 3rd millennium raise questions of sovereignty such as ownership of transport and storage of information over national territory, economic questions such as costing of on-line distribution of contents, sociological questions such as establishing citizens' trust in digital structures (the Internet, but also mobile telephony, banking or logistic digital labelling networks), as well as ethical questions such as recording, without their knowledge, the computerized data of people.

Digital personal data, which are recorded without the subject's knowledge, are for example, successive bank account transactions, geographical position within a telephone relay cell at the telecom operator, connections on the Web servers at te Internet access provider, appearance and behaviour on the cameras installed on public highways, the radio label (RFID) on clothing.

The security of the digital world has become a fundamental stake for the citizen with respect to individual freedom and protection of computerized identity and privacy, for the company with respect to the protection of its computerized industrial assets, the security of its business transactions and the trust level of its information networks, and for the state with respect to the reliability of operations and the reduction in the vulnerability of large and critical infrastructures : power and water distribution systems, transport communication methods and means, and information and communication systems pertaining to these infrastructures.

### 1.4.1 Sovereignty: Geo-Strategic Aspects

Digital security has assumed major importance in the civilian and business environment over the last decade. Security is closely related to geo-strategic, as well as to political, economic and social issues. Indeed, entire facets of daily life, of the economy and of administration are highly dependent

on information technology: transportation (management of the railway and air traffic), communications (telephony and Internet), the stock exchange, the trade system, the banking system, the health system (the social security smart card, the computerized medical records) and the defence system are examples of sectors relying on about a hundred computer servers. Rendering these servers secure is of critical importance as an attack against these computerized fortresses may result in the disclosure of vital information to the attacker or may paralyze an entire country or region.

It is therefore crucial for users, companies and the state to preserve their dignity, liberty and sovereignty, yet these rely on the control of the digital systems they use and the security of their operations and related information security.

### 1.4.2 Revaluation of the Digital Asset Base: The Economic Aspect

Individual, corporate and government assets are increasingly taking a dematerialized form, as the storage of digital data is becoming equivalent to productivity gains in all respects. The volume of data doubles each year and the value of family, company and government assets is increasingly derived from or encapsulated in this digital, cultural and industrial asset base. This is true for some new economy companies, whose industrial assets are already almost exclusively in intangible form (databases, computing programs, manufacturing secrets), overtaking in importance the buildings and possibly even the personnel administering it. However, this phenomenon will become a reality for the individual users as well. Archiving, restoration and search of personal databases, rerunning older software, replay of data, will become current practice among our countrymen. The government should take into account this essential aspect of the lifecycle of data from their creation through obsolescence and destruction, via utilization and reconstruction. The birth of the concept of digital assets represents a genuine rift that has much wider implications than information management in general: it includes management of Intellectual Property Rights (IPR), Digital Rights Management (DRM), copyrights and online sharing of information.

The security objectives related to the digital assets base are expressed in terms of confidentiality (non-disclosure to unauthorized persons), integrity (non-alternation of content by hackers) and availability (the ability of authorised users to access and use these assets without being hindered by unintentional or malicious acts).

### 1.4.3 Building and Maintaining Trust in Digital Infrastructures: A Sociological Issue

Large digital infrastructures are set in place all around us: mobile telephony, communication satellites, computerized banking networks, the emergence of digital television, smart tag logistic systems (RFID). Some personal digital objects have become irreplaceable (credit cards, mobile telephones) or sometimes indispensable (portable computers) or convenient to use (PDA's, digital cameras).

All citizens should embrace this digital world, without, however, abandoning the dropouts by the roadside (the social rift here is rather of a digital nature). Due to its highly complex and diverse nature and to its rapid development, the digital world can no longer be mastered: computer science has accustomed us to bugs, while software or products that work poorly if at all are hardly a rare occurrence. All these reinforce the sense of mystery in the minds of laymen.

Information security is related to the level of trust. If we wish all citizens to share these conveniences and adopt the new technologies, we must establish and/or restore the trust of individuals, companies and government. To this end, the concept of "digital governance" exercised by the international community has become necessary, as the digital world can no longer be left to the will of market forces.

### 1.4.4 The duality between digital privacy and collective security: digital dignity

This illustrates the subtle relationship between the methods designed to preserve our privacy and the legal procedures to ensure it, and the practices intended to protect the rest of the world against our potential malicious or accidental actions, and the means that are being implemented to confine

them. Creating a climate of mutual respect and trust is not contradictory to devising and setting up mutual defence procedures.

Open and transparent dialogue should make it possible to negotiate the rules and subscribe to clear and harmonious security policies. Such digital dignity is achievable and required to preserve the democratic values of our civilization.

### 1.4.5 Confidence in the security offered: digital sovereignty

It is crucial that the security operating rules are open, transparent and well understood by everybody without the presence of hidden solutions of which people are unaware and that are out of their control. We must be offered tangible security that is verifiable or verified and certified by a trusted (state) authority in order to get confidence in the host of security tools we are offered. It is therefore important to insist on the guarantee, the certification, or the qualification ensured by a trusted entity and its experts. If, for example, security is designed in the dark and concealed in a black box, it will be impossible not only to analyze any residual weaknesses and vulnerabilities, and therefore to trust the system, but also to intervene in the event of an attack. Security specifications implemented could not therefore be an absolute industrial secret[1]. Moreover, (security) service providers should not establish a dominant power play between themselves and their users that would cause the latter to become sorts of "trusting slaves". For example, a trusted third party accepted by both could appreciate the technical measures and validate the actual levels of security implemented.

Today, ICT has reached a planetary dimension and is used by a broad section of public that handles and processes myriads of potentially vulnerable data. Security should then be perceived as a state of vigilance that ought to be implemented through a set of actions that is very well thought through: we need to anticipate problems and solutions rather than considering attacks like an unavoidable phenomenon of modern times and healing, at the end of the chain, the damages caused by cyber-crime. This is the challenge that we must face in order to gain the trust of citizens and companies and encourage them to use these technologies in a fruitful manner.

## 1.5 Creating a user-centred system

### 1.5.1 Focussing activity on three issues: who, where and when?

To specialist observers, the Future Internet, and more generally, tomorrow's communication networks (for we cannot discount the **coexistence of different forms and methods of communication**), look to have one overriding feature: it will be focussed squarely on the individual (the citizen, the end user, the consumer). This vision is, at this stage, neither optimistic nor pessimistic, as the aim of all future R&D programmes will be to influence the nature and scope of this central position:

- Will the individual passively occupy this central position, a mere consumer at the hub of immaterial radii? Or indeed,
- Will individuals be active in the sense that they can construct their own relationships, using an array of technical, functional and societal tools and specifications?

Put another way, this issue touches on our freedoms:

- Does "being central" mean being observed (even monitored, spied upon) by the surrounding system?
- Or does "being central" mean, conversely, that one's choices will interact with and influence one's environment?

So the issue is twofold: what rules will govern relations between future systems and individuals, and who will write these rules?

[1] Kerckhoffs' principle: a system should be secure even if everything about the system, except the keys, is public knowledge (Shannon: *The enemy knows the system*)

It is not enough however to maintain the primacy of the individual if we then ignore a parallel trend which both weakens and puts into a different perspective the aforementioned vision: the centre will potentially be everywhere, for everyone:

- The ubiquity of information technology and the supply to its access points;
- The dissemination of information (both spatially and thematically);
- The capacity to join spatially disparate sources of computing power;
- The rapid expansion of potential locations from which individuals can assert their presence via actions conducted over the network (relayed communication, remote function operation, etc).

The unity of a situation is often defined in the same way as the three theatrical criteria: unity of time, place and action (or person). How are we to ensure that these unifying factors continue to prevail in the future, if time (through programming activity) and place (through the multiplication of remote access points) are no longer reliable indicators?

**It is incumbent upon future research programmes to restore spatial and temporal system guarantees (the where and the when, with sufficient certainty to ensure continued confidence), if we are to avoid seeing it diverge from this.**

### 1.5.2 The postal model

What we shall call the **postal model** would be interesting to apply in at least five of its aspects:

- The Postal Service is a trustworthy infrastructure.
- The possibility of senders being able to transmit messages anonymously (unless they actually give their details on the back of the envelope).
- The impossibility of maintaining anonymity in postal services frequently used for official purposes, such as recorded delivery.
- Guaranteed dispatch point, thanks to the postmark (this does not indicate the sender's final destination).
- Date guarantee; this has a recognised value, since the postmark "authenticates" it (the postmark does not necessarily match that on the letterhead, nor the date on which it was placed in the post-box, as there may be a day or two's disparity).

**Based on this postal model, it might be possible to draw up a set of technical specifications which could lead to concrete security policies and technical solutions for electronic exchanges.**

With regard to the aforementioned third criterion of unity through action and person, it is worth highlighting the importance of the issue of identity: how can any person or object be reliably defined whilst respecting the need for relative anonymity or privacy as well as transparency? More prosaically, how do we avoid identity fraud or theft?

**What we shall refer to as "unity of person" should be preserved by both legislative and technological means.**

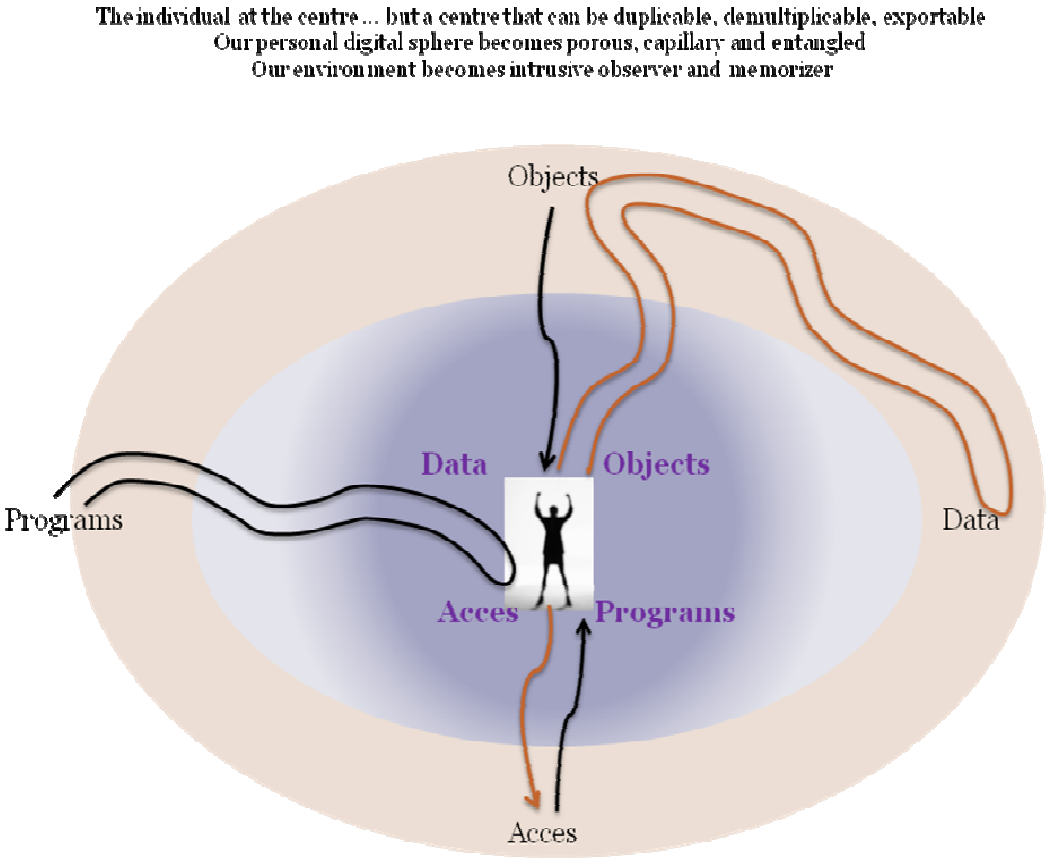



**Figure 1: The individual will become the centre, but the centre will become duplicable, multipliable, remote-capable. Our own personal digital domain will become porous, capillary and disordered. Our technological environment will become one of intrusion, surveillance and record-keeping.**

## 1.6 Security issues for business and society

The internet is a public space in which the security of infrastructure security for operators, and the security of software and data security is, for both their authorised users and owners, a guarantee of reliability. Despite the architectures deployed to ensure greater reliability and service connectivity and despite the anti-piracy measures taken to protect sensitive data, it is clear that computer systems regularly fail or are subject to malicious attacks.

Architectural security (future internet) and data security (software and data) represent key challenges. The digital world is one which is open to all: on the web, everyone is technically more or less free to post and to upload content, publish whatever they want online, write what they want to whomever they want; essentially to do whatever they please on the system which they choose or stumble blindly upon. The first phenomenon which everyone has experienced is the receipt of viruses via various entry/exit methods (networks, USB keys, CD-ROMs, etc), on the back of which the antivirus software market has experienced tremendous success, not necessarily justifiably, and the invasion of spam messages against which operators offer a filter to weed out this proliferation of inappropriate advertisements, which ultimately performs rather poorly.

Then there are more pernicious phenomena such as fraudulent and criminal acts which can be conducted over the networks. These include such acts as the theft of credit card details and sexual offences as well as sensational fraud and the propagations of ideas which call in to question the whole notion of democracy and respect for others. One of the challenges in guaranteeing a democratic world (as the internet does not recognise national boundaries), is to put in place a rigorous system of regulation on the one hand and effective policing of the network on the other. It would also seem to be imperative that the means of combating cyber-fraud be dealt with at national level, and that regulations governing business (access providers, software publishers, and hosting

companies) and the State be drawn up to ensure there is adequate legislation covering the issues of cyber-fraud and consumer protection.

## 1.7 Privacy issues for citizens

### 1.7.1 Protection of privacy

Logged by operators who run the digital systems and picked up by sophisticated sensors in monitoring systems, the digital trail left by everyone, wherever they go, can make far more detailed data files than the traditional files compiled by bureaucratic administrations.

With these techniques we reach a whole new level and individuals can no longer keep in their own possession information about them which they do not wish others to see. Surveillance and GPS tracking techniques pose formidable problems when it comes to protecting personal privacy.

Objectively verifiable data was previously compiled and managed with specific and known purposes in mind. Now, however, the data-gathering system operates greedily and indiscriminately, grabbing data from each and every source. This opens up new possibilities for tracing, monitoring, shadowing and digital inquisition, with the possibility of registering and following every move of every object and processing and cross-referencing this data.

### 1.7.2 The right to opacity, omission and disengagement

Everyone should have the possibility of retaining an area of obscurity, in which they are able to remove all traces of themselves, to disconnect from the network, to disengage from infrastructures. Faced with the possibility of exposure of parts of their existence which they do not want revealed, everyone should be able to assert their right to a certain protective opacity. Currently data is being disseminated, supported by social networking practices and legal or pirate copies of data between sites. This dispersal makes it impossible to erase all traces. However, each individual has the right to opacity and to erase data in accordance with the known data retention period.

Indeed, web-based monitoring, the possibility of being traced via mobile phone signals, and, in the future, the monitoring of objects through radio-frequency tracking devices or through new internet-based functionalities expose the individual without them even necessarily being aware of it. Automatic identification, using IPv6, will allow everything to be registered, movements followed, and communication with others organised, so long as there are suitable sensors and interfaces. This opens up an infinite universe: the internet of objects. To forearm themselves against the undesired usage of their persona data, everyone should be told what data has been collected on them, what happens to the traces they leave behind, and whether they can be erased or retained. Certainly our contemporaries, particularly the younger generation, have little awareness of how potentially dangerous this irrational immersion in the digital universe could be.

**Think-Trust encourages work to be done on technical solutions which will allow everyone to protect data relating to them. It also encourages Europe, and its constituent States, to strengthen the independent data protection authority that institutes and ensures compliance with regulations, in the same way that those governing road traffic allow us to travel in the best possible conditions**.

### 1.7.3 Managing the life cycle of information and secure data formats

Through the information society, individuals constantly generate this raw material, information, relating to themselves, their past, their career, etc. Even as creators of this information they do not, however, acquire any rights or guarantees over it. It is at once held, managed and controlled; it is potentially shared with third parties, who may variously be a single entity, easily identified or may be an unknown quantity, or potentially a multitude, and may go so far as to be freely available on the digital network.

**This change calls for personal control by everyone over their data, at all stages in the life cycle of this information. One approach could be a dedicated, personal, over-writeable network, in which everyone would be able to control data concerning them. Another perfectly feasible solution would be to create tools capable of destroying (or "putting in the**

**trash can", to borrow a current computing analogy) personal data about us which may be on the information network and thus exposed to all third parties. From the point of view of the data lifecycle, tools would therefore be needed which can deal with data at the end of its life cycle, through a personally-appointable collector.**

### 1.7.4 The security of personal (hardware, software, data) cybersphere: the digital objects' life cycle security.

The scenario of nomadism (see 1.8 below) reinforces the need to achieve a mastery of the life-cycle of information and its secure media. An individual becomes, through the information society, a constant producer of this raw material: information on him, his past and his life-path. Being a creator of information does not give control of a personal cybersphere, neither automatic nor guaranteed. There is an involuntary sharing that results in loss of the creator's control of retention and management of dissemination, access and usage. It also results in unaccountability where the *shared* information may be attributable to an identifiable third party, possibly reduced to a single actor, or to a misidentified third party, or to a unspecified multitude, up to a situation of free access across the digital network

This evolution requires for a check by each on their data, at anytime during the life cycle of information. One way could be a personal dedicated overlay network, of which each person would have control. A potential solution would be also to provide tools (such as garbage collection in computer memory for object oriented language) that could go and destroy (or "put in the trash," by analogy to our computers) the information that is private but exposed to any third party. In a lifecycle perspective, it would thus be tools capable to ensure the final phase of the information cycle by a garbage collector activated at will.

### 1.7.5 Clarifying the roles played by ICT players.

This move will better determine everyone's respective responsibilities and duties with regard to security (telecommunications operators, network managers, content and service providers, etc).

The more of these players there are, the more support there will be for providing sufficient mutual or collective security.

**One possible option is the virtualisation of everything which is currently represented by packets, routers, lines, bandwidth, sessions, etc.**

A second key issue is that the balance of power between provider and user needs to be restored, especially when it comes to the individual user. It is currently very unequal, as the provider has a power which, in law and in social terms, could be described as an opposition force. Any failure to restore this balance in favour of the users, their usage, their access and their control over their own digital domain and the network will impede the effective development of practices, including any future commercial power.

We need to be able to devise viable forms of governance for the individual's infosphere: forms which can support their growth during mass deployment, and can extend to hundreds of millions of users. This includes the management of our data and the traces we leave behind us on the network, and also brings into play any solution based on the ability to audit what happens on a network to identify movements and entry points, whilst mainlining sufficient levels of digital privacy for all.

## 1.8 Mobility issues in a scenario of nomadism

### 1.8.1 User security here and now: its fragility, its dependence and the "big brother syndrome" in locating individuals.

Nomadism (intermittent connection and session from various locations) or mobility (continuous connection to a digital infrastructure and activity during the move) destabilize the perennial framework within the personal cybersphere security when the position is static. The security of mobility requires an anchor of geography and time. Nomadism and mobility especially emphasize the logic of a spatiotemporal security framework based on the *hic et nunc* (Latin for "here and now).

The concept of geographical territory, where legislation applies, retains its relevance in the sense that it remains necessary for the common safety, to report, through it, an act committed by an identifiable author, but also at the point of entry space from which the actions have been initiated originally.

The "now" introduces and facilitates an *in vivo* (Latin for “within the living") environment, which corresponds to the ICT specificities: capacity of near-instantaneous, customization capability, interaction or adaptation to a person.

In order to protect this volatile mobile digital life, made in real time and in vivo, several axes are possible:

- Protect our secrets and our identities in terms of identification and authentication, with tools and components such as secure USB keys, smart cards, SIM cards. It is to secure on the one hand, the individual, and on the second, the digital instruments of the person. This would be very useful for those who are engaged, while nomads, in connection with a playful or collectively online videogames with multiple players or multiple parties.
- Develop a contextual security, ambient intelligence, to deal with problems such as:
- Tracking, monitoring and traceability of people on a territory, according to their trajectories, refined observations of behaviour (eg through a crosschecking between input position and images of networks of urban cameras). This monitoring may be as much a source of protection, to validate remote access by an individual by introducing identity requesting such verification, a source of insecurity if violating for her privacy;
- Usability of security tools, awareness of the security of the user, the definition of a fair level between a sophistication need of protection in order to make its activity dependent on an awareness of its user, with capacity for him to disengage or configure these functions at will and desire of that user to a transparent, simple to the extreme, without activation. The good level of usability requires an arbitration with both technical and citizen orders;
- Mastery of consequences arising from this extension of itself that is the computer science tool, when this tool is likely to breakdown, malfunction or malicious taking control. There is a risk in the situation of dependence on both physical and psychological integrity of an individual to keep this tool a part of its memory, its links with the past, with the outside world, and particularly in need of communication, in crisis situation, etc.
- Provide tools and means to ensure privacy around personal objects: this affects in particular the Internet of things, and the fact to delegate our security to external entities: robot, micro-robots (medicine, digital prosthesis) or other artifacts. It raises the question of delegation (to whom, for what) for objects of our daily lives such as our car, in a multiparty situation (vehicle owner, repairman, car manufacturer).

**For these objectives, it seems possible to prefer a type of trust infrastructure, rather than of a security infrastructure.**

### 1.8.2 Redistribution of responsibility in the chain of actors involved in exchanges

In a situation of mobility, it is necessary to facilitate and clarify the roles between actors of ICT, to better identify the responsibilities and duties of each player (telecommunications operators, network operators, service providers, content or service providers, etc.). The issue of maintaining a mutual or collective security should be strengthened, as the number of these players tends to grow.

One possible way should be through security at the virtualization level: virtualization of all the paradigms (packets, routers, channels, bandwidth, sessions, applications, etc.).

A second key point relates to the necessary rebalancing of the relationship between supplier and user, including the individual user. This unequal and unfair face-to-face relationship is today marked by a strong asymmetry, where the provider has a power, in law, which results, in social terms, a power imbalance. A shift in this balance resulting in the enhanced usage, access and control of the user over their digital sphere will ensure development of uses, including their commercial viability.

It is important to achieve sustainable forms of governance of the user's infosphere : forms capable to support growth in the massive deployment, to the scale of hundreds of millions of users. This comprises the management of our data, the traces left on the network. This pertains to any solution based on an ability to audit what is happening on a network to identify trends and points of entry, while maintaining a sufficient digital privacy for everyone.

However, it is questionable whether the in vivo might not lead to a creeping form of *in vitro* (Latin for "Within the glass"), in the sense that the digital space of a person may raise as much of a field of freedom, by a form turning to his disadvantage, a field of monitoring and observation of facts, gestures and movements, even our opinions.

## 1.9 Identity

### 1.9.1 An initial classification for identity and personal data

The main issues might be analysed on the basis of a breakdown of functions or tasks likely to be carried out by computer systems. The following list is neither exhaustive nor set in stone. It gives us the opportunity to rethink the basic functions of computer systems which are ubiquitous, constantly connected and endowed with a diverse memory capacity.

- Personal data, in the sense that it can reveal the name or other identifying information about a person (or even an object), such as address, date of birth, etc. It may also include banking (account no, etc.), professional or other information.
- Information which identifies an individual's existence: they may remain anonymous but are still acknowledged to be an existing entity. (For example, in our daily lives we do not need to know the name of a person we might encounter in the street to confirm the evidence of our own eyes and to start to form an opinion on them, decide whether we find them either helpful or unhelpful, decide to make a friend or enemy of them, etc).
- Information which defines them in terms of their consumer, philosophical, political preferences, etc.
- Information which tracks them spatially, without necessarily knowing who this person or object is (I may not know the name of a traveller, but I know where he or she has been, thanks to swipe-card, date-stamping and ticketing systems).
- It is worth mentioning that one could also previously speak of temporal traceability, which may involve looking at our educational record, our youthful opinions, etc.

The functions may therefore be summarised as: naming, designating (tracking without naming), psychological or behavioural profiling, following.

The current problem with legislature and data protection authorities is that they focus exclusively on the first issue only (nominative data), whilst the others seem to be growing as a result of interconnecting files, and data aggregation and collection facilities. Web2 and the most recent developments support this trend towards transferring private personal data into digital formats and in an open environment.

It is worth noting the position held by several German officials who have seen fit to tighten legislation governing the trading of files containing personal and similar data, often even threatening to outlaw it altogether. These decisions also extend to increasing the severity of fines for illegally trading data. This case also saw an embryonic atypical "economic model" proposed, with a minister suggesting that a company pay back any profits derived from this kind of activity.

### 1.9.2 Identity à la carte

There seems to be a broad consensus on the desire for flexible identity systems. This could take two possible forms. Individuals could have an "à la carte" choice regarding the sending and receipt of data streams:

- The ability to decide on the level of security of data streams concerning them (sent or received);
- The ability to decide the level of anonymity of these data streams.

- The ability to choose from several possible connection types, according to the desired level of anonymity.

At each of these levels, only the aspects of identity required for that particular connection are revealed.

Following the accountancy model, based on a reliable identity, to be attached to an initial territory-based registration, it would be possible to temporarily abandon this reliable identity for a particular data stream or connection, but without being able to divest oneself of the rights or facilities which the recipients or operators might require from these same streams attachable to a trusted identity.

### 1.9.3 Examples of à la carte identity

There have been various proposals made regarding identity relating to the “just enough” approach to information transmission.

- A data stream/sender could be issued with a ‘travel pass’ type document, based on the idea of a transport ticket:
- for buses, it shows the destination.
- for trains, it shows, destination, seat, time.
- for aeroplanes, it also shows an identity, validated (cross-referenced) on presentation of a passport.
- Identity certification could also be based on ID-card-type processes (driving licence, passport, etc), which do not necessarily contain the same information.

These various approaches are often governed by the principle of sending to the recipient or intended recipient only what they actually require for their own part. For the other elements, they will be informed of the authority to which they should apply to obtain possible confirmation or further information.

### 1.9.4 Current example: secure electronic identity in Germany.

The recent development of social networks and blogs on the internet has led to a huge proliferation of personal data on internet users. Each of them has to manage a genuine “digital identity” made up of their contributions and the traces they leave on the web. The growing use of the internet by individuals, businesses and government entities raises the question of information security and personal data protection. In addressing this issue of authentication technologies, users are given the confidence they need to use the internet as a tool. To this end, the German government has decided to implement an electronic ID card system for all German citizens, starting in November 2010. This is meant to be able to prove an individual’s identity and to be able to give proof of objects and products, as well as guaranteeing intellectual property using innovative procedures such as watermarks and digital signatures. German R&D has initially been focussing on the following issues:

- Secure reciprocal proof of identity through the use of an electronic ID card;
- How will electronic identities influence how the average citizen organises their daily life?
- Secure identity: transparency and authenticity in the real and digital worlds;
- The use and administration of secure electronic identities;
- Long-term security and quality of official electronic documents using the leading smart-card reader family Infineon;
- Display technology for multipurpose cards;
- Time-stamped digital signatures;
- Digital signatures for VoIP communication;
- Digital watermarks for the authentication and protection of digital media.

## 1.10 Accountability

There are two options which seem especially promising and coherent:

- Base the demand for traceability and accountability on global accountancy-type principles, which can encompass all networks, and such that reliable and more or less exhaustive incoming and outgoing accounts can be drawn up.
- Reintroduce, on a lower network layer, a "territorialisation" of facts and participating parties. The aim is to ensure that people and places can be guaranteed within the current communications system, whose weakness stems precisely from the difficulty in identifying and authenticating these parties, as well as actions in terms of time and place.

By partially moving system control towards establishing data either a priori or a posteriori, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows.

Other approaches have been suggested, and are worth looking at in greater detail; however, the two principal options mentioned above seem to have immediate unifying and organisational potential.

This two-pronged global accountancy and re-territorialisation approach could offer an alternative to the mutually opposing laisser-faire/network policing options. It could also buck the network trends towards ubiquitous practices, nomadism and varying identities.

On a more general level, a similar approach might consist of implanting time/space marker points into the system.

- The spatial could borrow from IBM's vision of an existing physical relationship between an internet user and an administration (or any ad hoc interlocutor) which could validate their real identity in a permanent, stable and guaranteed manner.
- With regard to the chronological dimension, the accountancy approach would require the temporal dimension to be implanted into the functionality of future tools. This is inspired by existing accounting practices, in which the principle of chronologically recording facts is not enough, and is completed *a posteriori* through the re-use of the same data in an incomings-outgoings system which has to balance up (all incomings and outgoings must be entered with their complement on the assets-liabilities balance sheet or as receipts-expenses on the operating account: this is known as double-entry book-keeping and guarantees, *a posteriori*, that the chronological records are accurate, that nothing has been omitted or added - inversely, the chronological record validates the overall balance sheet).

### 1.10.1 Towards a chain of "certainty" or "trust"

The chain principle is useful inasmuch as the need to continuously access excessive information (who, where and what?) is replaced by the knowledge of just one of these elements; access to the other elements then requires recourse to other parties and/or public (and also thus visible) procedures.

One of the potential applications of the chain system is the initial 'territoralisation' of the individual (e.g. the territory in which their passports was issued for real, physical travel). If the individual sends an email on the network from another territory, they can use this identity, which ensures they can be traced back via the entity in charge of registering their existence and issuing their digital identity.

### 1.10.2 Preliminary questions: the cost of insecurity.

By posing two preliminary questions we can start to define a framework for discussion of the two weak points in personal data protection, i.e. the lack security and of service quality.

1. How do we define what is intended by the term "reduction"? Is it a matter of eliminating undesirable situations, reducing them, or rather absorbing the cost of them without actually eliminating them? The logical extension of this would be to divide out the cost using an intelligent incentive-based system, although this attempt to effect behavioural change

applies just as much and for just as long to the drawing up of rules and regulations. The other term of "weakening" covers a range of possibilities: do we weaken the situation or its effects? In computing terms, this dilemma is very familiar: who negotiates between the effort to prevent a dangerous event occurring (the likelihood of it happening) and the effort to reduce its consequences (loss of data, delays, damage to reputation, etc)?

2. How is the exact cost of it to be calculated? Are we to have recourse to systems of measurement and evaluation on the basis of subjective or objective criteria? This issue highlights the difficulty of defining the notion of damage: what is it worth? Who is in a position to evaluate this? Should be down to the victim, the accused service provider, expert third parties in the courts, or insurance company experts? Estimating the immaterial dimension of damages is also a subjective process: justice has managed to reintegrate this point in its "economic model" as it is able to define fair financial compensation. Can we therefore do the same thing through other means such as amicable settlements and standard market ratings? Similarly, costs could perhaps be estimated through a supply and demand model, based on past records (historical cost accounting). Operating according to market regulations presupposes that "rational expectations" include future costs in the current price, but counter examples reveal the existence of weaknesses or loopholes which can be exploited by some economic operators. In a reversal the process of calculating costs based on past accounts data, what criteria will govern the conversion of future costs to current value?

**All of these considerations point up the fact that superficial thinking will not suffice if we are to formulate a price-setting system which is honest and efficient from a socio-economic point of view.**

## 1.11 A legal continuum between the material and the immaterial

Faced with this new situation, technological or political decision-makers have two choices:

- To consider that we are entering a world so new that the usual rules of society, including legal regulations, are inoperable therein.
- A second view is that all technological evolution, both materially and through the fact of it becoming a "social object", quickly becomes embedded in the existing social conventions, as largely dictated by: laws, conventions, recommendations, the rules of social engagement, moral condemnation of actions which impinge upon others' interests, etc.

The latter option, although it may not be immediately adopted, relies on three observations:

1. Observation of the material nature of the ICT sphere

Philosophically, those who posit a break with the old technological and legal world often rely on the notion that ICTs constitute a purely virtual world, which is not in fact the case, as the electrons, photons or electromagnetic waves which transmit this information are real, the magnetic devices on which information is stored is tangible; the "immaterial" (knowledge or identity) will long have need of the "material" in order to exist and to translate into a culture communicable to others. Legally speaking, a bit of information has an owner, even though it may not always be that of its repository (one can store ones property in a bank vault, without necessarily relinquishing ownership of it).

**Will areas of absolute or relative non-ownership come to exist? Or perhaps we will see the emergence of co-ownership, or the subdivision of property into subsidiary elements in the same way that immoveable property is legally defined in terms of usus/fructus/abusus (that is, respectively, the discrete rights to use, profit from or destroy or sell an item)?**

2. The premise of there being no legal caesura between the real and the virtual

The broad principles of law in no way prevent its application in the so-called "virtual world", as one finds therein legally well-defined ideas such as harassment, destruction of property (albeit digital) and intrusion of privacy. These approaches to the issue might tend to blur this virtual/real caesura,

for as far as the law is concerned, when it comes to judging damages and responsibility it is irrelevant whether data is written in ink or stored in magnetic form. This point leads to one of the subjects to which the Think-Trust is to contribute, namely, to what extent will the future internet be an essentially lawless zone?

**Will there be areas in which the law does not apply, in either absolute or relative terms, or areas of co-regulation, as currently exist for ships outside of territorial waters, or satellites in space?**

There seems to be nothing in the current legal apparatus which prevents its application in the so-called virtual domain. However it is inevitable that there will be a phase of adjustment, perhaps even experimentation, whilst the law gets to grips with the specifics of the future internet. We might attempt to classify these specific characteristic in the following way, which, albeit reductive, serves to throw the main issues into relief:

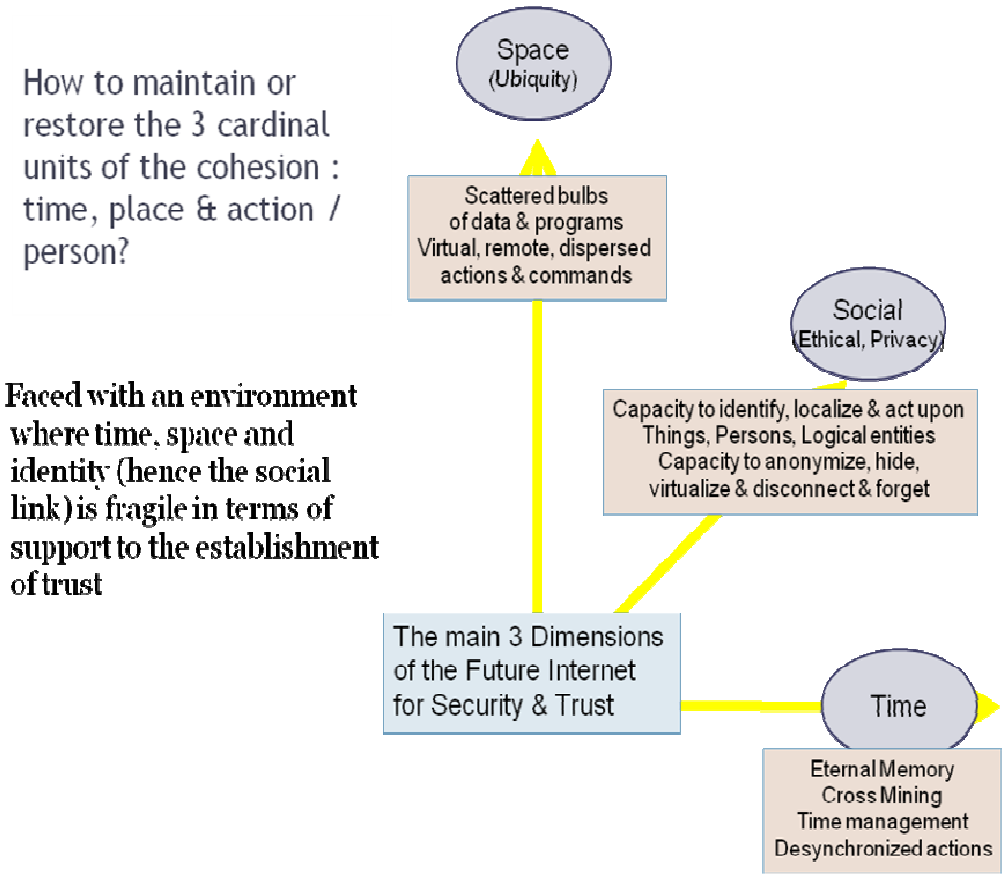



**Figure 2: The three dimensions of the Future Internet**

This diagram shows that the law may for example apply to uses relating to immediacy and spatial dispersal (e.g. an individual based in one country but possessing electronic data in another, or having programmed an action from a third). This does not necessarily require new laws, but rather working with case law to apply the fundamental principles of law to technological applications which make actions quicker, more disparate or fast-moving, and whose origins are less easily attributable to a specific entity.

3. The trend towards the normalisation of dissident actions over time

The hypothesis of the “normalisation” of the internet over time is borne out by observation of previous technological revolutions: the Gutenburg press gave rise for over a century to multiple copyright infringement actions, one notable typical example being the fact that the French writer Corneille saw numerous pirate copies of his works published during his lifetime, one by a Dutch

publisher which is still in existence today and which is now a law-abiding market operator. Similarly, cinema in its initial format (film), was initially subject to numerous copyright infringements; this was indeed the case in the 1910s, for example, to the detriment of European films shown in American cinemas. The film industry has now become a fervent defender of the law. We can expect to see a similar trend with the internet, so long as there is support for it.

It is on these means of support and assistance that the Think-Trust is to focus. To this end, we consider it useful to initially create a set of "conceptual tools" which can be used to draw up general technical specifications for future communications systems.

### 1.11.1 Forming new concepts before defining legal and technological solutions

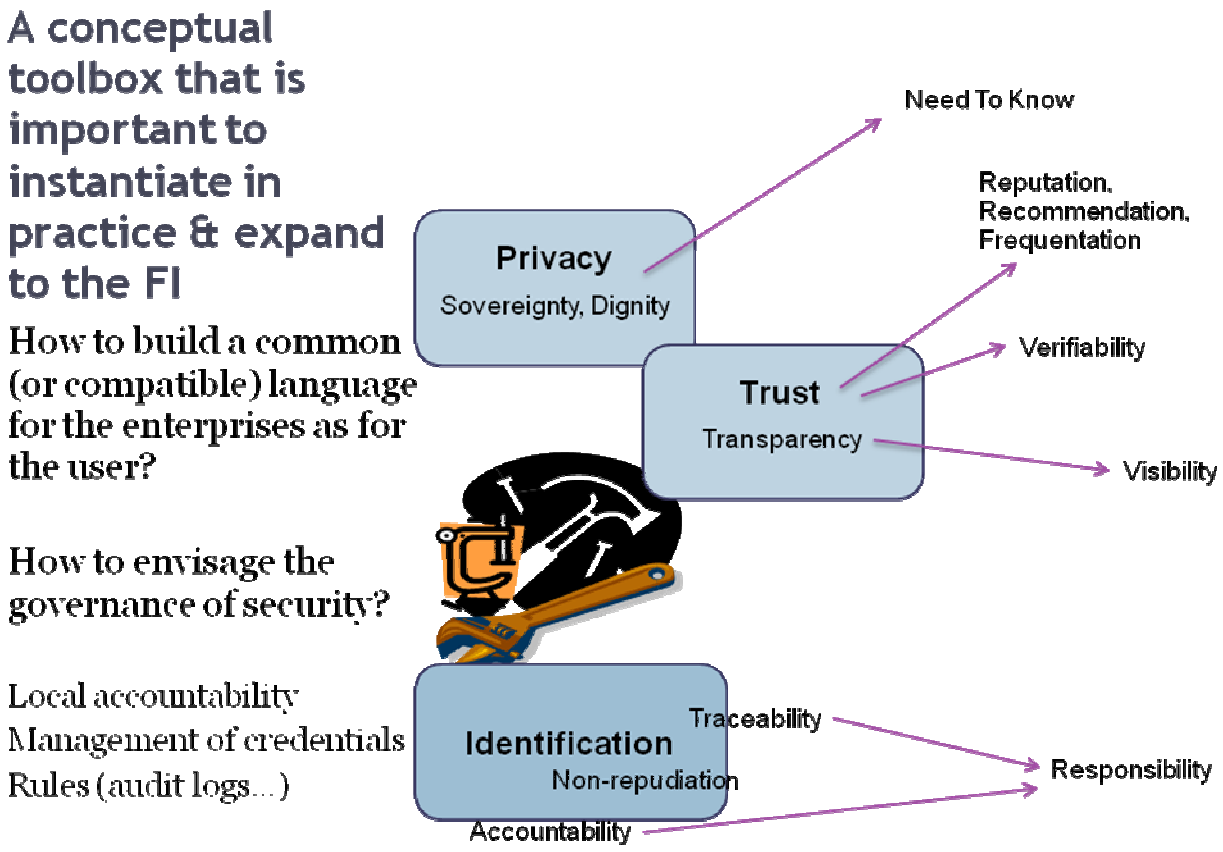



**Figure 3: A conceptual toolbox**

Several of these "conceptual tools" are already well-known: notions of privacy, confidence, accountability, transparency, individuals' right to privacy and personal data protection (with the personal digital domain itself liable to become spatially disparate, aggregated or superimposed with other personal or business domains, e.g. online management by software publishers of certain programs installed on our computers). The term "domain" implies that we are dealing with a homogenous, concentric entity, whereas it might be more accurate to describe it as sprawling, capillary or porous.

#### 1.11.1.1 Modest beginnings inspire confidence

It may be possible to combine these "conceptual tools". Similarly, by making the connection between confidence and transparency, it is easier to then define the idea of "visibility": exactly how

visible can any citizen's interlocutors, equipment or connections really be said to be, (in terms not only of security but also the relationship between appearance and reality)? Visibility is different to transparency in that the latter is supposed to be exhaustive, posited as an ideal, whereas the former is more concerned with ensuring a sufficient level is reached to inspire confidence: is the visibility of other individuals or equipment sufficient to inspire my confidence and allow me to communicate with them?

This idea of visibility leads to the need to attain certain thresholds, in two senses:

- How much and what kind of information do I need on my interlocutor or equipment to "function" in the sense of having enough confidence to interact with them?
- Conversely, how much and what kind of information do my human interlocutors or hardware interfaces need about me to "function" with me?

This focus on "thresholds" can lead us in a number of different directions, often influenced by cultural factors. In the Anglo-Saxon context of interpersonal and private contracts, it might be a matter of reciprocal and comparative thresholds: which of the two correspondents agrees to the greatest effort to become effectively transparent but simultaneously not demand too much unnecessary transparency from the other? Who assumes greatest responsibility in the event of a mistake (such as losing a file containing personal data on a partner with whom one has corresponded) or a breach of confidentiality (for example the selling on of collected private data). From this point of view, a threshold would partially become a relative value, both in relation to that of the other and from the point of view of fair distribution of effort. It would be best described in English as a "fair" situation, in which there would be an element of accounting to accurately assess the situation, particularly so as to be able to quantify each party's contribution. This would thereby calculate any possible deficits on either side.

There are a number of other possible approaches, which might involve the formulation of either a subjectively-determined minimum confidence threshold (independent of the other party's threshold or any possible effort on their part if they start from a low level), or a desire for objectively-calculated thresholds. This would require recourse to adjudicating third parties and would constitute another version of what is known as the "social contract": I defer to a designated third party who will defend and represent my interests and then determine the rules instituting rights and obligations for all, including me.

Both the private interpersonal contract and the social contract will undoubtedly be very much a part of the ongoing debate on the future internet.

Visibility demands a definition of how this is to work. There are various possible solutions:

- One approach proposes a straightforwardly declaratory method: a site or software publisher will make public their security policy, ethical and behavioural policy, and how it is implemented in their products and services. This nevertheless implies the existence of a favourable environment:
    - The existence of moral pressure on the declaring party, emanating from civil society and pushing the criteria for honest disclosure to a higher level. There are a number of considerable cultural disparities on this issue. The USA, for example, favours this overall approach, placing as it does greater cultural importance on public declaration (contrition, repentance, pardon, declaration of good faith, swearing before a jury, the grand jury principle, etc). The quasi-Biblical attitude behind this does not exist or is markedly less prevalent within other cultures, which value more individualistic behaviour, or, at the very least, are less communitarian in the Pilgrim Fathers' sense of the term. Of course there are also certain countries which are influenced by criminal organisations but which are home to many good software publishers as well as pirates.
    - Generally speaking, this approach has no other value than that contained within the declaration "I swear to tell you the truth by declaring that I shall not lie".
    - An effective and deterrent system of sanctions in the event of fraud. Currently, those cultures which place little value on the public declaration lack such sanctions.

    - A system which informs users of the existence of fraud, and gives them adequate "publicity".
- An intermediary model, in which the declaratory principle is set within a framework of technical specifications stipulated by independent bodies. However the inadequacies inherent in the previous system are also seen here, as the question of veracity, sincerity and moral obligations remains the same.
- Another intermediary model is based on joint or corporative structures, as much to enact constraints on declaration as to add an additional level of professional verification and sanction (in the same way that health insurance companies employ examining doctors). However this presupposes the existence of organisations which are virtually non-existent in the current IT environment, despite their prevalence within such self-regulating professions as law and medicine in various countries.
- Other approaches go beyond the declaratory model to suggest direct user verification or having intermediary private or public bodies perform this function (as exemplified by the certifications provided by private control bureaus for oil tankers, although they have been seen to carry the risk of complicit circumvention).

#### 1.11.1.2 The optimal adjustment of mutual recognition for all parties

The "visibility" philosophy links to a whole range of pre-existing concepts, one of which is taken from strategies for "just in time" or "just enough" manufacturing logistics, viz: it is as unnecessary to deliver (items or information) in too great a quantity or too early as it is too little or too late. Applying this concept to network data, the issue might be summarised thus:

- What is my personal confidence and communications threshold?
- What is the confidence and communications threshold of my partners, suppliers and other relevant socio-economic parties?

In many respects, this idea relates to the "need to know" principle, which is similarly based on the notion that total disclosure is not necessary for an action to be carried out or contact made. This calls for a more precise theoretical definition of transparency (e.g. legislative and legal) and for it then to be specifically applied, thereby making it operational.

Opening and holding this debate presupposes the need to define key concepts, foundations for future decisions:

- How do we define the idea of digital capital?
- More generally, how do we define digital citizenship?

## 1.12 Trust

### 1.12.1 Instilling trust in the digital ecosystem and keeping it in a robust condition

The galloping digitization and computerization of the modern world is pushing towards the generalization of networks; this generalization is carried along by new concepts such as pervasive networks, and ubiquitous computing or ambient computing. These new tropisms are highly heterogeneous both in terms of policies and technologies deployed.

From the security point of view, this heterogeneity tends to increase the complexity of the main security functions, like identification, authentication, access control and data protection. The implementation of these functions usually follows objectively from a trust model in the form of a trust infrastructure, itself forming the basis of the security architecture. Trust is thus at the heart of the security because the necessity and pertinence of the deployment of some other security mechanism depends on its existence and on its level or characteristics, and reciprocally.

The absence of a measurement of trust in digital systems is one of the major obstacles in the maintenance of networks and telecoms infrastructures in a controlled state, both in terms of security and reliability of operation.

The lack of trust in ICT infrastructures shows itself at every stage in their life cycle: during operation, because these systems have to confront intentional attacks or cope with accidental breakdowns, and at the design stage because security or robustness are often not included in the system's specifications.

Communication infrastructures and systems involve thousands, even millions of nomadic devices and the implementation of virtual constructions (virtual networks, overlay networks) which operate both on the hardware and the software, and on the network and the servers.

Security architecture constitutes a beginning in the treatment of security in heterogeneous networks. The completeness of the specification of this architecture remains an objective to be reached; an objective of which the satisfaction is dependent on the raising of a number of questions and limitations.

Beyond the security of the trust model which has proven to be an essential element conditioning the security of the overall security architecture, are other questions, likely to put this architecture at fault. All the aspects and questions broached represent stages to be cleared or at least to be dealt with, in the achievement of a platform simulating our security architecture.

It is advisable to automate and make the trust infrastructure more dynamic through interaction with the security infrastructure, so that authorizations, exceptions and the general security management are carried out by the system itself. Such is, in substance, the objective of this trust platform. The objective is to accompany and strengthen the security and reliability of the cyberspace, the ICT infrastructures, networks, services and systems. Research will be interested by trust models in general:

- the definition of trust: total, partial and assigned trust;
- protocols for instilling trust;
- the range of trust models (based on reputation, frequentation or surveillance, on security or redundancy mechanisms) with regard to a system, a service, a network, a hardware or software component, or an architecture.
- the variables to measure trust in real time in a system;
- the estimation of trust by a user, an operator.

The construction of a trust framework must offer a hybrid trust model for heterogeneous networks (heterogeneous primarily though policies) in which one leans in particular on its distributed consonance; a consonance inspired by the social trust model and based in its formalism on heuristic mathematics. One will thus be able to experience the contours of a new security architecture with a design crystallized by its close links which unite, without dissolving or mixing them up, the trust infrastructure with the security infrastructure. Furthermore, this new architecture will take into account the heterogeneity of technologies as well as the heterogeneity of policies. The searching of data or rather the communication of various data relating to an entity of which one wishes to gage the "trust" can also play an important role. In everyday life malicious people are often betrayed by "shady" details which they have forgotten, or have not been able, to mask.

### 1.12.2 Trust versus security

#### 1.12.2.1 The distinction between Security and Trust

We have to distinguish between the various following ideas:

- Security is a non-functional property of a component, a system or a service;
- Security assurance of a component, a system or a service, which is the quality of the design and operation of this property, is the degree of trust in the system's security, but not necessarily the degree of trust in the system;
- Trust (or distrust) expresses the quality of the relationship between two entities; these entities can be persons, physical items (components, equipment) or intangibles (virtual machines, software or data files).

Certain titles (trust infrastructure, trust operating system, trust module etc) confirm the confusion by mixing up the two concepts of trust nod security, or more frequently the concepts of trust and security assurance, which in no way helps in understanding for non-specialists.

For example, so-called trust infrastructures such as PKI are generally not trust infrastructures but rather secured infrastructures (for key management). Indirectly, through authentication of the entities, they can instill trust in a digital system in which no one knows with whom they are in contact. Such infrastructures generally have good security assurance (they bear a quality approval), which does not mean they must necessarily be trusted.

"Trusted OS" are secure operating systems that properly execute the tasks they have to carry out, usually through compartmentalization. They do this with primitive security functions that can be used by the applications. Their guarantee is security assurance. However, they cannot necessarily be trusted.

For marketing purposes, the TCPA alliance has been called "trusted", but the specifications in no way provide trust for the user. On the contrary, these are systems the user should fear, because they take away from the user sovereignty over his system and data. Similarly, the TPM (Trusted Platform Module) of a user's PC's motherboard can be assessed using the EAL3 Common Criteria, which does not mean one can have trust in one's own "personal" computer.

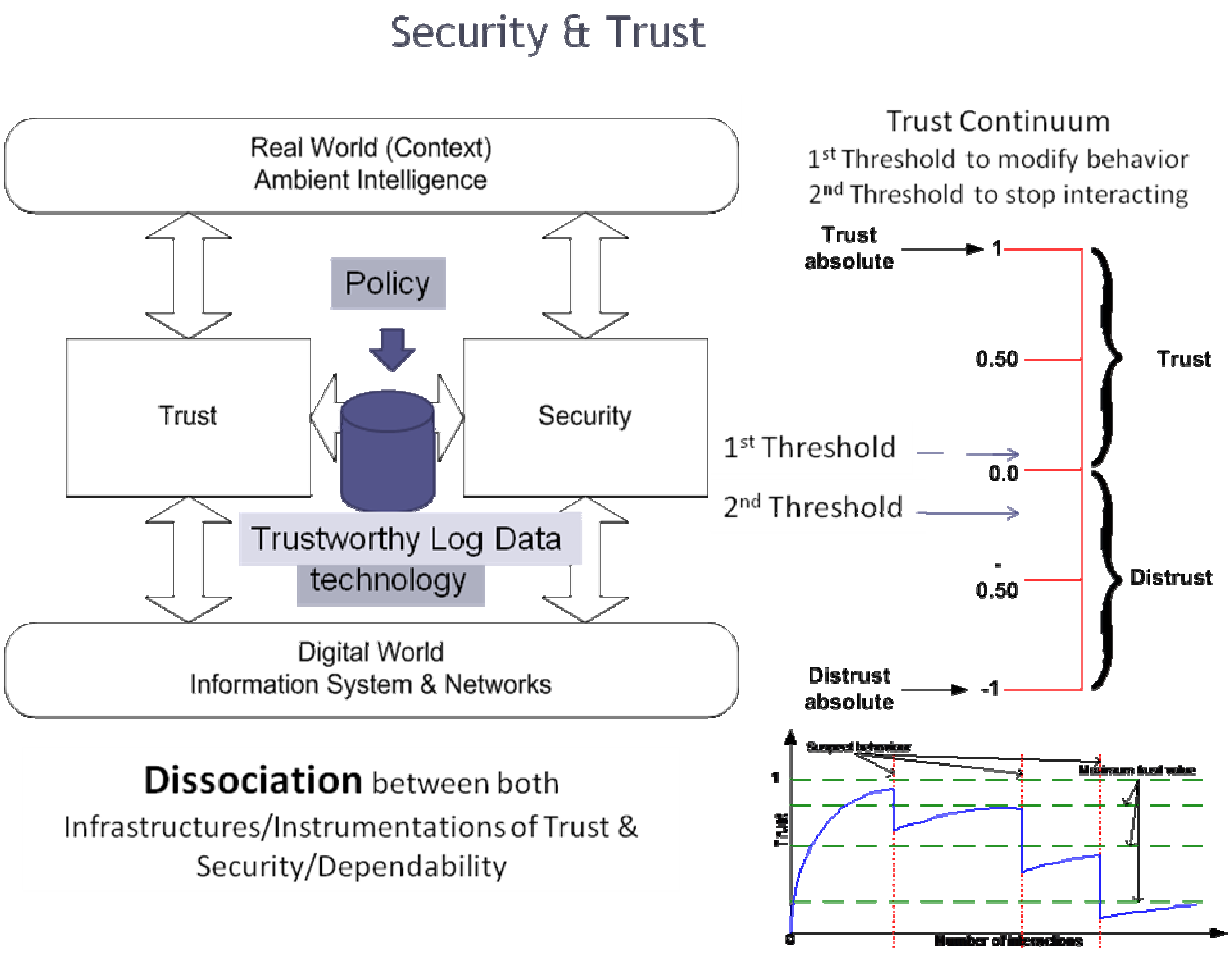



**Figure 4: The Distinction between Security and Trust**

### 1.12.2.2 Security functions associated with an entity

The following, various functions must also be distinguished, which are frequently badly defined, poorly understood and wrongly interpreted in security literature:

- The identity, name of the entity or alias (and the associated authentication, accountability and non-repudiation functions),

- The anonymity, masking of identity, unawareness of the person's name, and thereby the absence of responsibility, because it feels authorized to do everything (spread viruses and spam);
- Traceability (and the related functions of reporting, flagging and surveillance),
- Disappearance of the entity (drops out of sight) and the loss of identity; the entity and its name have been destroyed or have simply melted into the immensity of the IT magma, to reappear at a given time.

There is sometimes confusion between the use of identification and the operation of authentication. The latter can prove the identity of a person or prove the tracking of a flagged but anonymous person, or the behaviour of a software entity that has been flagged but for which the relationship or link to a responsible person is unknown.

More than the function of identity, the traceability function is increasingly important in this mobile universe. Anonymous persons can be traced. Accountability and responsibility are crucial in this digital world.

#### 1.12.2.3 Reminders about security and security assurance

Operational security can take the form of models for protection, dissuasion, survival, deception, disinformation, crisis management and attacks.

Faced with threats (limited or vague, known or unknown), operated by enemies or attackers, faced with breakdowns and the fragility of the system (due to poor design or sensitive operation), and with a view to get the most out of the IT assets (services, software, files, brands on the web etc), a manager (either a person or a body) defines a security policy that is implemented using security functions. Security functions (identification, authentication, access control, auditing, data protection, communications protection etc) are implemented to achieve security objectives that can be expressed in terms of confidentiality, integrity and availability.

Security assurance is a measure of quality (in the general meaning of the term) of the implementation of this security, in the design, operation and use of the system. It is an assessment of the strength and correctness of the mechanisms implemented, measured by taking into account the entire life cycle of the system, from design to destruction.

#### 1.12.2.4 Trust consideration

Trust is a different concept. Generally it has nothing to do with the security of a system, even though of course there is a relationship and a link between the two concepts.

The security of a system is an intrinsic, non-functional property, outside of any other entity, like upgradeability, flexibility and manageableness.

Trust in a system or its various sub-systems is a property of the relationship with an entity (for example, myself) that does not belong to the system or this subsystem Trust is a binary relationship between two entities that are going to interact, not necessarily in the same manner. This entity is a person but can also be software, or a virtual entity.

The degree of trust or distrust in a system will define a strategy of thought, decision and action in respect of the system.

In practice, everyone defines their confidence based on trust models. It is a mutual relationship that depends upon the context, and frequently on the history of the relationship between the two entities. It is possible to define this trust relationship between two entities using a mathematical function. The underlying trust model is a relationship built on:

- Ontologies (by definition and construction of the entities, they satisfy the trust function that varies as a function of time, space and context);
- The construction of entities based upon one's physical inspection (I have examined the software source code, it does not necessarily do what the specifier wanted, it does not necessarily do what is stated in the documentation, but the software is on the one hand not

aggressive and on the other hand not vulnerable, meaning it can resist certain attacks, but will not be able to resists in such and such a context such and such a menace.

- Experience (following a history of interaction, through behavioural analysis I believe that a trust factor can be calculated and inferred);
- Acquaintance (I have used it for a long time, it works and has never let me down, so I can trust it in the future);
- Reputation (many people that I do not really know have told me that I can trust it);
- Recommendation (not many people, but they are trustworthy, have told me I can trust it).

#### 1.12.2.5 Measure of trust

Trust is a non-reflexive, non-symmetrical and non-transitive relationship. Mathematically it is a lattice that does not create a total relationship but only a partial one. Within this group of values there exists a greatest lower bound, a least upper bound, but in general it is not possible to compare two trust relationships.

Trust in a meta-system, within a system, an infrastructure, a service, an application, software or hardware, a product or a component, thus depends on the trust policy that one has defined for oneself and that develops as a function of time, space, context and history. Trust functions are very characteristic functions in terms of time (trust has difficulty growing fast, but in general decreases very quickly, for example following some event). Having been let down, the entity will have difficulty building trust back up quickly and it will not reach the level it had been at, unless there is an element of forgetting involved.

Trust varies from –1 to +1. Negative trust (distrust) is relatively common: one does not have trust, but the policy says that one can act in any case. Positive trust (>0) facilitates acting more or less. Blind trust (=1) is dangerous. The exact assessment of the degree of trust is not very important. What counts are the two basic thresholds in this gradation. What counts in trust is less the absolute value of this trust than the two thresholds, C1 and C2.

- The first threshold, C1, is a value below which one will change one's behaviour by being careful and vigilant. From threshold C1 I change my view of the system and I will act differently.
- The second threshold, C2 is a smaller value, below which of one's own free will one puts an end to the relationship (for a certain period of time). From this other threshold, C2, downwards, I stop interacting with the system.

Depending upon whether one is optimistic, aware, in a hurry or pessimistic, paranoid etc, these two thresholds vary. These thresholds vary as a function of a sometimes uncertain context: an atmosphere that can be described as warm, courteous, suspicious, malevolent, hostile, according to which one has with the other complicity, a well-intentioned attitude, perplexity, a careful attitude, increased vigilance, a violent reaction.

In a commercial context, for small stakes, I make fun of the trust I can have in the system: happen what may, what counts is what I do, because if what I do is seen, falsified or stopped it is unimportant, it makes no difference. The risk is worth it, I need to act.

In a highly sensitive context, what counts is to do something, but fully secure (in terms of confidentiality, integrity and availability): the message must not be divulged, it must arrive at its destination complete and correct, and the route must not be blocked or interrupted.

In an open world, what counts for the user is sovereignty over his digital universe, over his personal domain.

In a malevolent and even hostile world, what counts for the user is the dignity of software and content.

#### 1.12.2.6 The composition of trust

Measuring the trust of a component or a system is not easy for two reasons:

1. Firstly, it must do what it is meant to, and develop this function through use;
2. Then the difficulty is to accumulate these trust values within an IT structure.

In IT the vulnerable objects are in general composites. Is this the case, for example, with a session? A session is quite an abstract ontology with the servers, the OS and the network for support. How do you put together the atomic values of trust to calculate the trust of a session?

In IT, objects are dependent on each other. If trust in the network is 0.8, 0.9 in the application, 0.7 in the operating system and 1 in hardware, what is the end-to-end trust of the service. On the one hand the trusts C1, C2, C3 …Cn must be considered, and on the other hand the dependence between mutual trusts C12, …, Cn-1, n.

If an application (C=1) operates on an OS (C+0.5), what is the trust of the entity being the application on the OS? The minimum or center of gravity [C= (C1 + C2)/2]? Unfortunately, the commonly held idea that the trust (or security) of a system is equal to the trust (or security) of the weakest link, is in general false. We in fact create system architectures, made up of related entities, exactly in order to increase trust in the whole (through redundancy) or to filter the dubious parts: the reason an institution has procedures is to clean up the items created and the output that lacks trust. An individual can make a mistake, which is not the reason his or her institution will endorse the decision or output of its employee. A real time system produces results, which does not mean that the system will take at face value every statement of this entity.

So trust depends a great deal on the topology and geometry of the system.

Thanks to routing protocols and network architecture, we can greatly increase trust that we have in a system, even if its internal components do not necessarily have high trust (a virus attacker implements a multi-part policy to create denial of service: statistically this will end in success for him).

#### 1.12.2.7 The instrumentation of trust

The idea therefore is to weave a trust infrastructure over the digital system to allow each user or every sub-system that interacts with another to decide in full awareness whether the interaction can take place, So we are going to calculate a network that at each point will calculate the trust to be obtained, In the light of this, each person will decide if they can act or not.

### 1.12.3 Security policy and trust policy

There are interactions between security and trust. If trust reigns, security measures can be lighter. If everyone has trust, the security policy will be to do nothing and protect nothing. If there is no trust in anyone or anything, there will be tyrannical, ostentatious security, which will simultaneously react and (perhaps) create trust in the system, at least at the beginning, but then things deteriorate because entities do not adjust well to dictatorship or terror.

If security measures are strict they might be effective, and then trust can be created; or they might be ineffective (it means nothing, it is just the manipulation of public opinion) and in that case there is trust but it is overvalued and places the citizens in danger.

In general there is a dynamic relationship: security measures increase trust in the system, and a relationship built on trust will lower the security measures. There is thus a dialectical adjustment to minimize costs and the disturbance caused by the introduction of security measures.

#### 1.12.3.1 The link between security and trust

We must accordingly distinguish between the two concepts of security and trust. The two infrastructures, the systems and the instruments must now be separated, those that serve security and those that serve trust. Now in the networks and the systems there will be tools and algorithms to create, manage and maintain trust in a system. And by the way, protection systems will always be created (encryption of content to protect semantic content, a firewall that protects access to a system's frontiers through access control), as well as security (digital tattooing of content to dissuade a pirate from copying and using software).

Obviously, and here things become complicated, there must be, in the traditional way, security assurance for the security infrastructure (these are the classic assessment methodologies for security such as ITSEC and CC), and the trust infrastructure must be secured. However this is a less important aspect of our thesis, because it simply involves securing one service like another, with good service assurance.

IDS and IPS are often systems in which security and trust are mixed together. Data is collected and the variables calculated, which facilitate deciding according to behavioural models (normal, not normal) whether or not an operation is legal. This in fact involves the underlying introduction of a trust factor that facilitates deciding yes or no, about performing a transaction or certain traffic over a network.

### 1.12.4 The security crisis: the parade of trust

Today we know that it is not possible to protect a large, open, interconnected system with mobile components. Thus to secure it, other means of protection are employed. In place of protecting there is prevention, repression, user awareness, attackers are dissuaded and tricked … and the law will try to do the rest.

You cannot wrap every mobile object in armour, all the more so since in general there is a reduction in IT energy at the periphery of networks. So it is preferable to save resources for positive functions or ones with added value, rather than to waste them on counter-productive defensive measures.

Faced with this crisis of security tools that is more favourable than that of a closed club that has to open up to the open, mobile, interconnected world, the idea emerging these days to make progress is to improve the Defence process with a more complex and more local decision-making algorithm, to substitute the idea of security that defines the state of a place with an ersatz Defence, namely the idea of trust, which will feed and support the decision-making and action process of the entity that is acting on the system. Instead of protecting the system, we will measure the trust that can be had throughout the system, or at least in the sub-systems with which we plan to integrate.

## 1.13 Economical aspects

### 1.13.1 Integrating weaknesses and the cost of their reduction within a coherent economic model

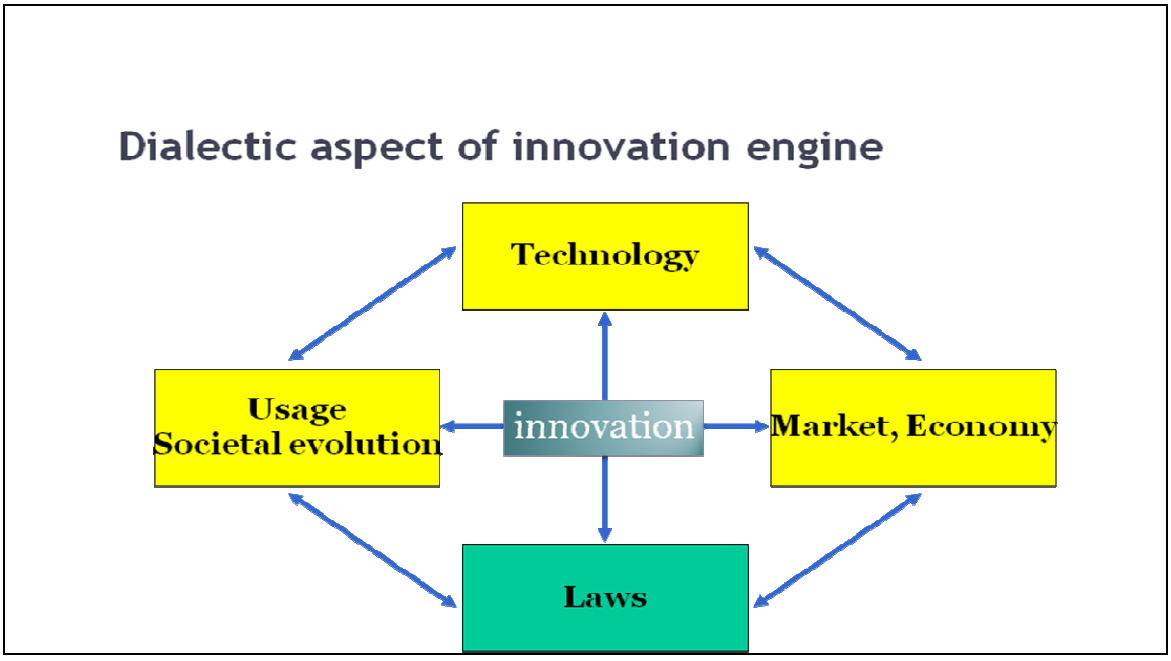



**Figure 5: Dialectic Aspect of An Innovation Engine**

Firstly, it is commonly observed that it is difficult to incorporate security, in the broadest sense of the word, into a suitable and practically-applicable economic model. Clearly safety is not usually enough of a selling point (or unique selling point), and is even less persuasive when it means putting up the price of a product.

Nevertheless this analysis is based on faulty logic, based on a social misunderstanding: consumers do not refuse to pay the price of security, but consider to have already paid for the product or service and thus fully expect it to function as it should, without malfunctioning, without latent defects and without hidden functions. It wouldn't be logical for a manufacturer of tinned foodstuffs, having agreed a price with the client, to then present them with a second invoice for certification that these same goods were suitable for consumption. It is not that the security market shows poor accounting practices, but that security is just one of a mass of competing commercial requirements and products, making it difficult to isolate.

When considering a future economic model it is worth bearing in mind that the current one is weakened by this uncertainty as to whether security and service are already included in the purchase price. Moreover, the current consumer trend towards open source or free software indicates that consumers already consider software to be expensive enough, even with the supposed inclusion of security. The suggestion that consumers should pay more for security could only boost this trend.

Inversely, making this security visible and manifest to the consumer would add value to the software industry: with users having been left disappointed by promises which were not kept, this economic sector is showing falling customer numbers. In short, users feel they have already paid for security and over the next few years they are likely to spurn further purchases if, for the same price, they do not ultimately get this security (in its widest sense) in a way which is visible, manifest and verifiable by them (or by a trusted third party), or even partially configurable on request and to suit their own requirements.

If security can add some commercial value, it will be less in the hope of increasing software prices or sales but more to avoid the gradual exodus of disappointed consumers. With this issue, there are two vital criteria:

- The first, as previously mentioned, is visibility;
- The second is verifiability: something must be done so that customers and users can verify for themselves the functions offered and the way in which their personal data is used. Lest we forget, we are talking about rights already covered by various laws, as citizens often have the right to access or change data held on them. Without necessarily having to verify the source code, users could ensure that software running on their computers is doing what it is supposed to do, and nothing else.

Verifiability (and even the possibility of configuring certain functions) also relates back to those aforementioned ideas of minimum trust thresholds.

### 1.13.2 Ambiguous aims: to care or to cure?

Once the framework is in place, the debate can focus on determining whether the aim of the economic model will be to care or to cure. However we should not be fooled by the apparent simplicity of the caring/curing dichotomy:

- Are we to rely on incentives or penalties? It seems likely that a mixture of both will be necessary, but we need to define both proportion and content.
- Do we want a system which (whether it provides incentives or penalties) acts before or after the facts: the idea that there is an automatic link between incentives and prevention is often false, as exemplified by the additional insurance premiums (whether as an incentive or deterrent) which businesses or individuals must pay, *a posteriori*, for previously-committed errors. Inversely, repressive measures can often be implemented before the facts, as exemplified by speeding fines, which are imposed before an accident has occurred but which indicate how strong a possibility it is.

This point leads us to another unavoidable question: do we want to tackle errors and dangers which have already actually occurred; or rather, do we want to focus on high-risk behaviours? In the case of the latter, it is not that a matter of accident-prevention, but of acknowledging that an individual or economic entity put itself in a position to have caused an accident, regardless of whether it actually happened: should we then penalise the running of risks, or wait until the risk becomes an accident?

Are we therefore looking at curing bad behaviour or its consequences? Often, it is a matter of striking the right balance between the two.

### 1.13.3 Economic players linked to various economic models.

We need to look at what kinds of parties will be judging or arbitrating in these situations. There are a number of broad schools of thought on this issue: the law (which sets down limits or rules), the market, historical cost accounting etc.

#### 1.13.3.1 The market

The market can be divided into various subsections:

These can take the form of quotation or securitisation of risk. These mechanisms have recently come under the media spotlight due to the recent financial and banking fallout. More generally, there is a particular contradiction in the case of ICTs, for which one of the desired criteria is transparency in being able to judge how secure or harmless retail products are. Pure economic theories currently suggest, amongst the basics of a liberal economy, that there should be transparency of products, players, and supply and demand mechanisms (and its corollary, the absence of any disparity in information between economic players) before any rating can be made. There would be a serious contradiction in demanding that a market list degrees of transparency, although this same transparency, at a more general level, is necessary to the accuracy of the assessment on which this quotation is determined. This leads back to the need for a result which, a priori, has its own source and method.

Can the market alone provide the basis for an economic model which includes security, privacy, transparency, etc?

If so, how do we restore the transparency required for it then to be judged itself? The principle of ratings agencies has recently been subject to criticism, which, without rendering the concept null and void, weakens the argument for it in an unregulated form.

Does perfect competition currently exist?

It is worth noting another important weakness here: economic theory stipulates that a market is only perfect under certain conditions (we have already seen the indispensable criteria for transparency and the absence of any disparity in information). These conditions provide a total competition situation, which itself refers to the atomicity of supply and demand, the absence of any barrier to entry or exit of the market.

The software market does not currently enjoy such conditions. Lest we forget, European authorities have taken up several emblematic cases, with legal proceedings and record fines. It would make little sense to rely on consumer reactions in the face of a lack of service provider security, if their ability to change is limited by commercial or contractual motives, or by a lack of individual technological skills.

The same goes for their ability to judge security levels, something which is not appreciable by the uninitiated.

There is a second branch of this area of the market which relies on insurance industry techniques, which are already used to gauge risks and to spread the cost of them out amongst the insured parties either a priori or *a posteriori* based on the possibility of a risk occurring or its actual occurrence.

- The anticipatory system is based on insurance premiums calculated on the basis of risks incurred, attitude, and the means and mechanisms available.
- Bonus/surcharge systems, in addition to the basic anticipatory system, also include *a posteriori* measures, which distributes the cost of insecurity (or for ICTs also a lack of privacy) based on observations of facts and individuals.

It is worth noting that the French authorities are currently looking to promote this bonus-surcharge system, and to extend the list of eligible products. This covers environmentally-rated products but such practices could also work in terms of ICT hardware and software security policies.

This initiative is being promoted as part of a "true environmental cost" initiative, which aims to encourage manufacturers to develop energy-efficient models with low consumption of raw materials and resources. These approaches are completely or partially transferable to criteria such as security.

Could a good economic model be created based on the insurance system, incorporating security, accountability, privacy and transparency?

The insurance industry, with its system of trust and visibility guarantees would also offer some useful reference points with regard to interlocutors who do not have the time or skill to make detailed checks on other interlocutors or systems. This domain would, then, work along the same lines as the existing accreditation and certification system.

#### 1.13.3.2 The law

The law can be seen as an integral part of an economic model, as the various parties involved include in their potential expenses the cost of such items as fines for copyright infringement, convictions for offences, or even the cost of loss of freedom (those involved in computer piracy do measure, at least unconsciously, the profitability of a financially-motivated act by balancing it against the probability of spending a number of months in prison, counted as a liability.

Proposals have been made to consider various forms taxing the lack of security and personal data protection (in relation to the minimum required levels of data to be collected), etc. This approach could be either unilateral (a financial penalty for poor products, thereby generating additional charges compared to good products, and conferring to the latter a price advantage), or bilateral (taxing the lack of security, but redirecting money raised from such charges to those who have made efforts in this area).

This latter approach is partially compatible with the insurance company notion of bonuses/surcharges, in which the aim is not for individuals to support their competitors' injurious acts, but on the contrary to confer an advantage on those who adopt good practices. Here a choice has to be made as to whether we want these systems of either penalty or reward (through cross-compensation) to be governed by the law, the market or even by an insurance industry-type system. And moreover, to what extent public and private bodies will play a role in this.

#### 1.13.3.3 Accounting costs

As reputation can be seen as a constituent part of individual or corporate capital, it can also be considered as a part of an economic model, as a company can judge the negative impact of adverse publicity over the intrinsic qualities of any of its products. This approach would therefore support the emergence of systems which disseminate information on known malfunctions and the risks inherent in certain software and hardware products.

There are then two questions to be asked: by what technological means is this information to be disseminated (which media) and by whom? The how and who could be based on spontaneous initiatives, co-operative movements, word-of-mouth/viral internet transmission, etc. There could also be public bodies, such as product ratings agencies, along the same lines as current electronic goods efficiency ratings (for electrical, water efficiency consumption, etc.). A similar type of authority also rates vehicle pollution emissions.

Accordingly, one of the major weaknesses of the present system is that consumers do not have enough information on exactly how safe currently-available products are and what potential

dangers they may pose. This lack of information stems from an almost identical problem on the part of the authorities.

It is worth pointing out that information can be collective (in which anyone can find out about the qualities and weaknesses of any product or interlocutor), as well as individual: the digitisation of communications paves the way to a ratings agency dealing with data flows, e.g. in the form of data flow authentication stamping readable by the recipient. This already exists in antivirus systems, which use a system of icons or pop-up boxes to indicate their status rating for a particular message or attachment.

# 2 Security and Trust Challenges

This section sets out the main Security and Trust Challenges for the security design of the Future Internet. A series of key security problems and issues that form the background to the research priorities, are discussed

## 2.1 Background

### 2.1.1 Two key structural vectors

The issues addressed include Security and Dependability challenges for the design of architectures, protocols and environments that will constitute future large-scale and globally networked ICT systems. Specifically, these focus on the upcoming future internet; cloud computing; the "Internet of things" (IoT) with mixed mode environments consisting of diverse computing, communication & storage elements; and, global e-Service infrastructures. The desired characteristics of dynamic, adaptive, scale-free, autonomic control are attractive in abstraction, though as global scale systems develop, heterogeneity (in design, resource types, operational policies, etc.) is often the pragmatic key attribute making systematic end-to-end security a challenge.

When considering the future research challenges and orientations, we need to take cognisance of the direction of these two dynamic vectors in the coming years:

1. **Ambient security continuum** : security technology will be everywhere, at all scales, in all layers, in the infrastructures, in the networks, the servers, the services, the content, the physical objects or in any sort of temporary virtual constructs (virtual private networks, dynamic software service coalitions, virtualised communication, computing or storage resources):
    a. Architecture and protocols: security is everywhere, spread throughout organizations, administrative domains or even national borders, particularly with governance of secrets and identity management;
    b. Core network: crypto at 1 Terabit/s, robust protocols between Autonomous Systems;
    c. Edge networks (3G++ but also IoT): decentralized, heterogeneous domains, and numerous scarce resources, where cryptography is difficult to implement;
    d. Content and services: multimedia downloading, distribution control, proof of ownership, illicit computations; insecure composite services and mash-ups;
    e. Critical infrastructures: resilience is everywhere. In particular there is a need to deploy critical infrastructures that can reconfigure and deliver under severe attacks, damages or human errors;

2. **Proactive security paradigms**: security paradigm evolution is essential if we want to move with the paradigm evolution of IT (virtualization, massive content, multiparty exchanges within social networks or within business value chains). This will require:
    a. Innovative security and trust models which better fit to the actual IT situation:
        i. Security and trust in the design of communication (other than store & forward) and cooperation (Web2, P2P, Internet of Things);
        ii. Security (stochastic), trust (reputation, recommendation, frequentation);
        iii. Contextual privacy with pervasiveness and location.
    b. Security and trust metrics to avoid qualitative biased judgments:
        i. Measurable variables for benchmarking, quantifying security validation (before and in operation);
        ii. Composition and meaningful aggregation of variables at all scales, in all layers, for assessing security status and enabling informed decision making.

c. Approaches to secure or protect the new representation and configuration of software, services and content.

### 2.1.2 Security needs

The future needs are:

1. Support for better identification, and accountability:
    a. must handle layers/domains: could be based on virtualisation;
    b. need policy-awareness as an architectural property;
    c. need observability as an architectural property;
2. Support for security monitoring:
    a. logging, log access, traceability;
    b. providing incentives for security data sharing: typical traffic mixes, current traffic snapshots, virus and worm signatures, typical attack signatures;
    c. fostering collaborative "environmental situation" establishment, collaborative anomaly detection and classification. States could create trustworthy, closed platforms for such practices.
3. Support for dynamic, contextualised trust:
    a. implies dynamic, contextualised policies;
    b. need tools/models for trust assessment and verification;
    c. need to support the full lifecycle;
4. "Everyware" security
    a. anywhere with transcontinental applications (compute here, store over there, access there)
    b. anytime with contracts
    c. anyhow with multi-models (societal, business).

### 2.1.3 Security principles

In order to solve these problems, and to overcome some contradictory or conflicting issues, we need to put forward:

1. A fair balance between transparency / visibility versus obscurity / opaqueness:
    a. Security is the art of sharing secrets within entities/components of a system;
        i. Privacy implies a shadow area for freedom;
        ii. Production secret to protect authors and creators (IPR, DRM);
    b. Trust is the art of sharing -any kind of things- ,including secret and sensitive, and of cooperating, in a relationship of two entities;
    c. Traceability requires observability with rules;
        i. Data gathering, recording, auditing;
    d. Governance requires knowledge;
        i. Governing means an ability to forecast (models derived from experience);
2. A new security and trust architectural approach : clean-slate versus incremental modifications for security:
    a. Moving target, moving methodology;
        i. New and emerging generations of attackers every three years (on a continual basis);
        ii. Future requirements from diverse users and society: unexpected usage;
        iii. Evolving future fundamental technologies.

## 2.2 Segmentations of the FI components

### 2.2.1 Network infrastructure

#### *Core network*

| | |
|---|---|
| Characterised by: | Immense size but low density, one single authority, globally few actors; |
| Societal needs: | High reliability, climate meteorology, public situation awareness; |
| Technical needs: | Integrity, management, control, observability, big-big cooperation between different core networks (i.e. their authorities), internetworking; |
| Issues: | Data sharing, trustworthy situation, contract verification |

#### *Access network*

| | |
|---|---|
| Characterised by: | Huge and dense, one single authority per AN, dependence on core-network services, heterogeneity of technologies; |
| Societal needs: | Sufficient reliability, ubiquity of several ANs everywhere, transparent and fair AN selection: transparent, trustworthy criteria, discovery, service pricing; same service despite technological heterogeneity; |
| Technical needs: | Secure signalling and security signalling; |
| Issues: | Trust propagation (from home network to the Visited AN) and establishment (serving a nomad), heterogeneous security: policies, choices, cross-layer security enforcement |

#### *Edge compounds*

| | |
|---|---|
| Characterised by: | multi-authority (private-private, private-public, small-big, small-small, myriads of small, swarms, etc.), multi-technology constructs, relatively small but may include myriads of nodes; |
| Societal needs: | Easy to use, reasonably reliable and moderately secure; |
| Technical needs: | Access control to data and services, control of the whole: easy network on/off, controlled data sharing; controlled extension, additions, removals; robustness through redundancy and rerouting, adaptive, capability-aware security. |
| Issues: | Capacity of nodes, pairing, limited energy. |

### 2.2.2 Services using or relying on network infrastructures

#### *Critical Infrastructures*

| | |
|---|---|
| Characterised by: | Of public security and safety concern. Usually use telecom systems for control, observation, etc. I.e. private edge is controlled from a private platform of the same authority. In between we can have a typical telecom construct of different ANs and CNs. |
| Societal needs: | High robustness; no failures in whatever conditions; only controlled, announced turndowns |
| Technical needs: | System of system state and health establishment, trustworthy platforms for data/state exchange of stakeholders, propagation avoidance, usage/deployment of new operational models from security for security research. |
| Issues: | Availability. |

***Services***

| | |
|---|---|
| Characterised by: | Multi-party, at least two authorities (producer, consumer), implicitly running over a complex telecom infrastructure (may be a 3rd authority). Service architecture is another, different complex system. |
| Societal needs: | Fairness and integrity: announced readable clear pricing and correct billing, proof of involvement. |
| Technical needs: | Efficient secure service architectures, self-properties for lower operation cost for service providers, service composition for outsourcing/mutualisation of reliable components, provider-consumer-provider, etc. multi-party services, non repudiation, logging, accounting, traces. |
| Issues: | Reliable, secure remote execution and procedure invocation; control of exchanged data, in operation and post-operational (DRM). |

#### 2.2.3 Advanced Security Engineering

Further research on adaptive, programmable and extensible policies;

Further research on new operational models (survival, disinformation, deterrence);

Meterology and situation awareness: security data sharing, emergency centres;

Security observation, management, evaluation and validation (metrics);

Crypto research: new hash functions, multi-party operations, Tera-bps cryptography and authentication, biometric integration;

Issues: testing, comparison, validation of new proposed approaches.

### 2.3 Security of the future global digital ecosystem

#### 2.3.1 Trustworthy polymorphic Future Internet

The focus is on building robust large-scale networked digital infrastructures and systems and on their secure interconnectivity (=> resilience, identity and accountability issues), guaranteeing massive audio-video traffic at very high data rates (=> traceability, identity, signatures, IPR issues).

Europe should become one digital plate of this dynamic, competitive plate architectonics, connected through “digital hubs”. It is important to clarify the promises and constraints to the citizens, but also to clearly express our requirements on and guarantees from the external partners.

##### 2.3.1.1 Security of the core network and the critical nodes

1. **New protocols and architectures**: security at a very large scale, improvement of Internet peering systems and advanced Border Gateway Protocols between Autonomous Systems within the current Internet, reparcelling and providing robustness of the current mosaic of the Internet, probably through virtualization of Autonomous Systems.;.
    a. **Cryptography**: packet encryption at 100 Gigabit/s, flow authentication at 1 Terabit/s;
    b. New high data rate virtual routers with embedded **security by design**.
    c. Globally running applications and services (international VPN, grids, clouds, search engines) with **multi-legislation** issues: responsibility, traceability in an international environment;
2. **Security of the virtual paradigms** at all the layers and levels of the network: packets, channels, routing, bandwidths, sessions, networks, autonomous systems, operators, etc;
3. **New security architectures** to secure **high capacity storage server farms** and fast retrieval with huge data traffic in the context of the evolution of Internet with concentration

of critical nodes (Global Internet eXchange, server farms, high performance parallel computers, Web accelerators, Content Delivery Networks);

4. Regional **emergency control infrastructures** (very large scale: - country, Europe) to protect critical infrastructure and critical applications (financial networks, air traffic control), systems of systems (to avoid knock-on domino effects). This may include "infrastructural meteorology" services for infrastructures relevant to public safety and security. States should require publication of "climate" and "health" data and share it over a stock-exchange-like platform. Certain information might/should become mandatory, while other information might be optional or of a commercial nature. Control infrastructures: networked physical security balancing security and privacy, keeping individual privacy;
5. **Test beds and experimental facilities** for security of the Future Internet at the core level.

#### 2.3.1.2 Security of the edge networks

1. **Federated security**: integration of heterogeneous security policies throughout several smart ecosystems;
    a. federation and coexistence of several conflicting security frameworks, in terms of identity and levels of security assurance;
    b. security or trust models are needed for negotiating compatibility or interoperability in an open or fragmented environment;
2. **Seamless security**: Interoperability of security schemes throughout the heterogeneous landscape of access networks (3G++, Ad hoc, Sensor, etc)
3. **Transparent and user-friendly security**: security improvement of wireless technology such as:
    a. mobile phone as multi-media device;
    b. virtual desktops with enterprise data and software;
    c. mobile/wireless communications across heterogeneous infrastructures in various mode, opening and interconnection of different infrastructures and nodes;
    d. distribution control of private and/or enterprise data: data deployment, concealment and removal from various wireless devices.

#### 2.3.1.3 Multi-polar governance and security policies between a large number of participating & competitive stakeholders

1. **Mutual recognition security frameworks** for competing operators: Telecom Operators, Network providers, Service/content providers; sharing security secrets: improvement, or replacement of PKI-like security infrastructures, improvement or even replacement of DNS and ONS; collaborative and shared security mechanisms;
2. **Transparent security** for re-balancing of the unfair, unequal face-to-face relationship of the end-user in front of the network: governance of the infospheres of people => scalability, traceability, log data management, accountability management.
3. **Instruments** for **early detection of attacks**: new methods to filter adware, spam and eradicate malware and viruses (included on 3G++ smart-phones), tools and mechanisms for large-scale test-beds dedicated to security (attack simulators);
4. Real time and **large scale tests for crisis management** procedures.

### 2.3.2 Trustworthy global computing

The development of the ICT systems is characterized through change towards more openness, more complexity and, most importantly, through the reinforcement of links to the real, physical world (communicating objects, intelligent environments, networked control systems in home automation, aviation, car industry, power grids, medicine and healthcare, etc). The ICT technology is no longer in a distinct closed virtual world.

The focus is on building confident services to avoid misuse, to detect failures, and to sustain the quality of these services. The composition, orchestration of these services requires secure mechanisms for dynamic configuration of these components.

Users need, by default, to give the minimum identity attributes to access to these services and content. The security requirements need to be analysed through a business risk approach: identification of subjects, encryption of protocols, secure base software and middleware, tamper-proof applications are among the important features for securing services.

Europe should lead the technology integration for the use of available, dependable, secure services onto the networks.

#### 2.3.2.1 Security of the cloud computing

The focus is on security of future smart Web, social networks, cloud computing, grids, P2P, large distributed environments, generalized virtual networks (=> privacy and trust issues).

1. Security of the new Web services and privacy protection against observability or linkability through search engines or social networks, etc.
2. Collaborative environments, cloud computing :
    a. compartmentalization of the clouds or security of virtual entities;
    b. virtual spaces are ways to cooperate with real objects, to represent knowledge (Web2 technology, multimedia), immersive spaces are new approaches for simulation of the real world;
    c. sharing resources (computation, storage, exchanges) in a secure manner.
3. Automatic maintenance of the new digital scenes:
    a. long term and constant housecleaning of the personal infospheres;
    b. right to oblivion.

#### 2.3.2.2 Domai-specific trust, security and privacy for smart environments

The focus is on contextual security with secure smart services for sharing information and cooperative environments with societal acceptance in order to feel in control of the digital ambience, and on new infrastructures using ICT as a tool to make the real world artefacts more reliable.

1. e-Health: secure online checking, resilience in telemedicine, security at the hospital, privacy of patient medical record databases, resilient smart assisted digital living (usability and acceptability issues), medical implants (resilience);
2. e-Home: urbanization of the intelligent home, remote assistance (access control issues), privacy and personal integrity issues (ageing population, ambient assisted living);
3. e-Government: electronic voting at large scale, law enforcement database with individual data (privacy issues);
4. u-enterprise (ubiquitous enterprise, virtual desktop), e-Transport, e-education, e-Commerce, u-service (discovery, location privacy);
5. Internet of Things (RFIDs, NFC) : security infrastructures incarnated for niches (logistics, plants, medical, library);
6. immersive environment, entertainment: 3D Internet, video games, massive multiparty networked games, virtual casinos (auditability issues);
7. control and automation systems.

#### 2.3.2.3 Resilient, pervasive, self-organised computing

Self-* networks will have to move on from the obsolete concept of end to end connectivity and embrace situations in which nodes are devices which cooperate freely and spontaneously in the absence of centralized services. Ubiquitous communication systems will demand new architectures based on the independent devices, connectivity reduced to fragments, and spatial awareness of the nearby environment and local data through different nodes in the network.

The focus is on security of wireless sensor systems, pervasive networking, opportunistic networks, and mobility systems, self-organized infrastructures, dynamic heterogeneous distributed environments (=> dependability, integrity and privacy issues).

The common issue here is security in presence of scarce resources

1. Security for self organised, and other self* like ubiquitous computing systems (reconfiguration, management and repair) taking into account personal integrity, system autonomy (robustness, management), adaptive security, and machine learning of security models;
2. Security of sensor networks
    a. Adaptive security: do not try zero or full security; better provide some security than nothing (protection with scarce resources). Would need new, respective policies and adaptive and situation-aware implementations/mechanisms. Typical application: Energy-aware security. Example: only authenticate a fraction of nodes and not all nodes in the path. Switch off encryption when low on power. Other possibilities include: design with heterogeneous nodes, some nodes may not be able of certain operations, adapt service security as far as the policy allows that to be able to communicate with these nodes.
    b. Security and aggregation: in sensor networks, data aggregation is an essential paradigm. Data aggregation, when combined with the respective verifications, can be used to provide some structural security of sensor networks.

#### 2.3.2.4 Security of services and content, of software and data

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context.

The technical paradigm shift leads from protection/prevention (cryptography, access control, confidentiality through pre-established policies and respective security associations) to other operational security models.

The goal is to build components, products, services and systems with an acceptable and affordable assurance of trustworthiness.

1. **Security of services**:
    a. security policy compatible with business models;
    b. secure software lifecycle management (particularly security of software upgrades);
    c. security of increasingly dynamic aggregation or composition of services;
    d. security of middleware, distributed grids, peer-to-peer exchanges, collaborative work platforms, distributed applications involving a large number of simultaneous users.
2. **Protection of content** and **Intellectual Properties**:
    a. managing and controlling the **life cycle of personal entities** (whether data, programmes or traces) and dealing with related security issues.
    b. IPR service infrastructures, for content sharing, media distribution; protection and management of IPRs; security of audio video contents; fine-grained access to documents and usage control of distributed data;
    c. dissemination of private data to a public platform without loss of control and ownership (does not necessarily imply IRP/DRM), access control can be done through cryptography and complex key management;
3. **Usability** and security: hassle-free security, user security they can understand and privacy they can control.

## 2.4 Trust and Privacy when interacting with digital entities

Let us not forget that the future of ICT raises human and social issues. What type of digital systems should we consider for daily lives that are compatible with our values; how should we view the relationship between knowledge and the capacity of physical persons and their cultural and emotional requirements? What are, what will be and what should be the social implications of the

development, deployment and use of such systems? The evaluation of technology on a precautionary basis should guide the design of tools for the construction of ICT, ultimately not purely driven by the evolution of technology, but with a basic objective of improving the quality of life.

Pillars of privacy and trust are not just technology but education, law, governance (feedback cycle: measuring / enforcing), safety Net.

### 2.4.1 Identity management

There seems to be a broad consensus on the desire for flexible identity systems. This could take two possible forms. Citizens could have an "à la carte" choice regarding the sending and receipt of data streams:

- The ability to decide on the level of security of data streams concerning them (sent or received);
- The ability to decide the level of anonymity of these data streams.
    - The ability to choose from several possible connection types, according to the desired level of anonymity.
    - At each of these various levels, only the aspect of identity required for that particular connection is revealed.

Following the accountancy model, based on a reliable identity, to be attached to an initial territory-based registration, it would be possible to temporarily abandon this reliable identity for a particular data stream or connection, but without being able to divest oneself of the rights or facilities which the recipients or operators might require from these same streams attachable to a trusted identity.

We need to design and deploy a collection of Identity Management frameworks in order to identify through distributed infrastructures, end-users, services, contents in different situations.

There are two options which seem especially promising and coherent:

- Base the demand for traceability and accountability on global accountancy-type principles, which can encompass all networks, and such that reliable and more or less exhaustive incoming and outgoing accounts can be drawn up.
- Reintroduce, on a lower network layer, a "territorialisation" of facts and participating parties. The aim being to ensure that people and places can be guaranteed within the current communications system, whose weakness stems precisely from the difficulty in identifying and authenticating these parties, as well as actions in terms of time and place.

By partially moving system control towards establishing data either a priori or a posteriori, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows.

Other approaches have been suggested, and are worth looking at in greater detail; however, the two principal options mentioned above seem to have immediate unifying and organisational potential.

This two-pronged global accountancy and re-territorialisation approach could offer an alternative to the mutually opposing laisser-faire/network policing options. It could also buck the network trends towards ubiquitous practices, nomadism and varying identities.

1. Identity management, accountability, traceability frameworks:
    a. at the network level:
        i. to balance privacy and traceability and prevent cyber-crime and frauds
        ii. Secure management (at large) of the different network entities;
        iii. Remark: several frameworks may coexist; protocols to interact with foreign frameworks are an open issue.
    b. at the service level:
        i. with pseudonymity, while keeping large anonymity;
2. Interoperable framework throughout European Member States of Identification and Authentication

a. with multiple authentication devices, e.g. identity and authentication of ontology, virtual identities (Trusted Platform Module for hardware, smart cards for persons), biometry at large. (using multimodality: biometry, RFIDs, NFCs, physical objects, etc);
b. taking into account diversity of services (governmental, financial, medical) and richness of cultures;
c. management of profiles and identity attributes, keeping privacy, while improving searching and indexing relevance;
d. deployment of new digital signatures : cryptography of new schemes for digital signatures (to overcome the current hash function attacks - See the NIST International competition for new hash functions and new digital signatures.);
e. auditing and reporting, access and authorization control.

3. Profiling services and communities
    a. Trust and privacy issues need to be addressed for the relationship between user and services, communities of users and categories of services.

### 2.4.2 Trust infrastructures

Lack of trust is one of the main barriers to the establishment of a secure and dependable Information Society. This can be a lack of trust in the cyber-infrastructure, due to frequent attacks or fears about the design of digital systems. It is also caused by concerns about privacy, as well as by the difficulty in modelling trust relationships among digital entities and between humans and digital entities. The panel focussed on key elements necessary for securing the applications and services operating across future large-scale networked systems, including trust management models and the articulation of security and privacy to reinforce trust, with emphasis on user-centric privacy enhancing technologies, mechanisms for accountability, liability, and monitoring, and a privacy-respecting naming and identity-management framework (of individuals, organisations and digital entities).

The absence of a measurement of trust in digital systems is one of the major obstacles in the maintenance of networks and telecoms infrastructures in a controlled state, both in terms of security and reliability of operation.

The lack of trust in ICT infrastructures shows itself at every stage in their life cycle: during operation, because these systems have to confront intentional attacks or cope with accidental breakdowns and at the design stage because security or robustness are often not included in the system's specifications.

1. **Trust infrastructures** (Public and/or Private Trust Infrastructures): instrumentation of the network periphery provided by trusted new stakeholders, computing trust and security assurance, using diverse trust models (by reputation, by recommendation, by frequentation, by voting). Trustworthy providers may coexist for various services, with different levels of confidence (governmental, business-wise for-commerce, etc);
    a. Trust architectures and new protocols to delegate trust and partial trust;
    b. Trust infrastructures in a dynamic business environment with newcomers, insiders and outsiders, ingoing and outgoing stakeholders: emergence of new stakeholders: process, methodology and certification or homologation procedure to validate and check services (a priori, a posteriori);
2. **Trust instrumentation** at the end-user level: using the user as trust sensor, but also giving trust-relevant feedback to the user at the service interface;
3. **Cognitive** and learning **instrumentation** for trust:
    a. Due to sophistication of technology, integration of abstract components, co-ordination of services, autonomic tools are needed to increase confidence in the complexity management for the societal acceptance.

### 2.4.3 Privacy infrastructures and mechanisms

Logged by operators or providers who run digital systems and picked up by sophisticated sensors in monitoring systems, the digital trail left by everyone, wherever they go, can go to make up far more detailed data files than the traditional files compiled by bureaucratic administrations.

With these techniques we reach a whole new level and individuals can no longer keep in their own possession information about them which they do not wish others to see. Surveillance and GPS tracking techniques pose formidable problems when it comes to protecting personal privacy.

Objectively verifiable data was previously compiled and managed with specific and known purposes in mind. Now, however, the data-gathering system operates greedily and indiscriminately, grabbing data from each and every source. This opens up new possibilities for tracing, monitoring, shadowing and digital inquisition, with the possibility of registering and following every move of every object and processing and cross-referencing this data.

The technical paradigm shift goes from new identity management schemes and purely technical solutions to holistic societal approaches, since absolute anonymity may be neither possible nor applicable.

1. **Privacy infrastructures**: protocols, tools to check privacy assurance, and multi-identity systems keeping privacy;
    a. Sandbox security models to improve privacy issues;
    b. Right-to-oblivion security models, networked garbage collector instruments to clean personal data across infrastructures;
2. **Privacy of personal** sensitive communicating **devices**: massive deployment of intelligent devices (3G terminals, PocketPC, PC) and growth of sensitive personal data
    a. Personal trusted entities (next generation smart cards, …)
    b. Wearable and/or transportable embedded systems,
3. **Privacy & Traceability** of personal **behaviour**:
    a. Unobservability (controlling unwittingly tracings), unlinkability while supporting user's profiling and tracking to enable personalised services;
    b. Usability with diversity (diversity in Europe);
    c. Ethical issues;
        i. Illicit content, illicit computations, legal proof, content control & filtering;
        ii. Security in obscurity : we must not be hostage of one security mechanism: security Sensors manageable by end-users to "measure security assurance";
4. Digital Sovereignty
    a. Audit, proof of the past;
        i. Authentic memory of an Information system;
        ii. Auditability of personal databases;
    b. Access control & filtering;
        i. Security of content (IPR, DRM…);
        ii. Filtering of virus, unsolicited contacts & messages (spam, spit, spim), bots.

## 2.5 Measurements, metrics, models, methodologies and tools (M4T) for security, dependability, trust and privacy (SDTP)

### 2.5.1 M4T for ever-increasing complexity

1. Security for the composition of systems, security of systems of systems: more abstraction in the security paradigms (security of virtual systems, entities, etc);
2. Security of a pervasive environment with scarce resources: using statistical approaches, lightweight security models;
3. Circumvention security models, survival systems (to avoid the current routines of patching of patches);

### 2.5.2 M4T for quantitative security assessment and predictive security

1. Consistent measurements and data collection at a large scale to manage complexity, to measure availability and maximum downtime, to feed trust models, to configure in real time protection devices, etc, while achieving balance of privacy and security (statistical effective data collection, anonymisation of personal data);
2. Trust and Security models, tools and principles
    a. For adapted to local cultures : behavioural and mobility models for simulation and prediction to feed simulation models with relevant parameters;
    b. to specify the behaviour in higher abstractions and verify through formalisms (theorem proving, model checking, etc) in operations.
    c. to build large scale systems for crucial societal applications, taking into account:
        i. composition: if basic elements (primitives, elementary devices, etc) are reliable, trustworthy and secure, how can we guarantee that their composition to a more complex structure inherit these properties?
        ii. evaluation (metrics) to evaluate the correctness, quality, efficiency, reliability and, finally, security of security, especially, in a working operational setup, during execution.

### 2.5.3 Enabling technologies and standardization

1. Declarative languages in security: metadata, ontologies.
2. Multimodal biometry, secure OS for smart phones, TPM environment, new cryptography (elliptic curves);
3. Standards in security to make tools and instruments interoperable or compatible.
4. Certification and measuring level of confidence.

## 2.6 Disruptive security

The only way to make a significant leap to improve security and trust within the digital world and to make it more reliable is to introduce new security models and to implement them with new languages which include security concepts within their semantics.

These new models and languages for trustworthiness could be used in three disruptive contexts: green security, just-in-time security, polycentric security.

Finally, we must not neglect the possible arrival of Quantum technologies with new threats (cracking current asymmetrical cryptography) but new opportunities (new models to assess security and trust). We need to think about classical cryptography in the quantum era.

### 2.6.1 Green security

The focus is to save resources (energy, CO2), and to think in terms of sustainability and in terms of global energy management.

1. Security heuristics at the network level to prevent propagation of epidemics;
2. Metering security personal tools.
3. Integration security approaches to optimise and to share security resources, detecting maximum anomalous event at the source level, and inserting minimum security algorithms within the end-user terminal.

### 2.6.2 Just-in-time and real life instantaneous security

The focus is on protecting volatile digital life in vivo (*hic et nunc*), in real time (=> privacy and trust issues).

1. Tools and models for nomadism: real-life end-user security, instant or just-in-time security protocols, real time security in crisis situations; trusted secure tokens & devices (sensitive devices); secure, multiparty, massive videogames;

=> Raising automatic security tools dealing with overflow of events;

2. Delegation security to nomadic personal robots, swarms of objects, body area networks (medicine);

   => Trust infrastructures to ensure and speed up the interactions with ambient intelligence.

### 2.6.3 Polycentric security

1. Vernacular Internet: polymorphous security models, multi-polar governance: (=> scalability issues in the multi-facets management);
2. Spatial and geographic security: security with landmarks, new cryptographic protocols using trustworthy geo-reference systems (hour and location) (=> intermediation issues).
3. Multidimensional integrated security: derivation of high level security policy with fusion of multimodal securities from different sources to influence knowledge and trust and to upgrade user's awareness.

### 2.6.4 Quantum Networks

Quantum Computers should appear around 2018. We need to continue the European effort to support the development of quantum technology through the deployment of high secure services with quantum communications.

Quantum Crypto may achieve high secure distribution of secrets that classical cryptography cannot - and Quantum Crypto will be used in the context of omnipresent security technology in the future.

# 3 Future Internet and Cloud: Trust and Security Research Priorities

There are several areas of Trust and Security which need to be addressed in order to move securely into the Future Internet and Cloud computing domains. In this respect, Think-Trust recommends focusing on the development of a robust research agenda. In this section of the document, four major areas of Research Priorities are discussed. These will be updated and further developed for the final version of this report.

## 3.1 Security in (heterogeneous) networked, service and computing environments

The issues addressed include the elaboration of security challenges for the design of architectures, protocols and environments that will constitute future large-scale and globally networked ICT systems. Specifically, these include and focus on the upcoming future internet, cloud computing, the “Internet of things” with mixed mode environments consisting of diverse computing, communication & storage elements, and global e-Service infrastructures. The desired characteristics of dynamic, adaptive, scale-free, autonomic control are attractive in abstraction, though as global scale systems develop, heterogeneity (in design, resource types, operational policies, etc.) is often the pragmatic key attribute making systematic end-to-end security a challenge.

- Encompasses virtualization, cloud, private / semi-private spaces, realized by service "oriented" platforms
- Makes underlying infrastructure resilient in all environments and conditions
- Includes technologies to realize the ecosystems with key attributes of (mixed-mode) heterogeneity (of devices, device resource capabilities networks/connectivity, mobility, density and applications) and scale-less scope for growth
- Multi-domain security ad esp. across the interfaces (technological and user-level)
- Managing heterogeneous computing environments and corresponding trust domains
- Moving from physical security architectures to service level security architectures
- Need for conformal multi-domain security and especially across the interfaces (technological and user-level) where most of the problems arise

### 3.1.1 Trustworthy polymorphic future internet

#### 3.1.1.1 Security of the core network and the critical nodes

- Protocols and architectures: security at a very large scale and a high data rate (embedded security by design), globally running applications and services with multi-legislation issues in an international environment; security of high capacity storage server farms and fast retrieval with huge data traffic;
- Critical infrastructure protection for critical applications, networked physical security balancing security and privacy.

#### 3.1.1.2 Security of the edge networks

- **Federated** security: integration of heterogeneous environments throughout several smart ecosystems;
- **Seamless** security: interoperability of security schemes throughout the heterogeneous landscape of access networks (3G++, Ad hoc, Sensor, etc)
- **Transparent** and **user-friendly** wireless security.

### 3.1.2 Trustworthy global computing

#### 3.1.2.1 Domain specific trust, security and privacy for smart environments

Contextual security with secure smart services for sharing information and cooperative environments with societal acceptance in order to feel in control of the digital ambience, and on new infrastructures using ICT as a tool to make the real world artefacts more reliable in e-Health, e-Home, e-Government, u-enterprise, e-Transport, e-education, e-Commerce, u-service, Internet of Things (RFIDs, NFC), immersive environment, 3D Internet, control and automation systems.

#### 3.1.2.2 Security of the cloud computing

Security of future smart Web, social networks, cloud computing, grids, P2P, large distributed environments, collaborative environments, generalized virtual networks: automatic maintenance of the new digital scenes (long term and constant housecleaning of the personal infospheres), right to oblivion.

#### 3.1.2.3 Resilient pervasive, self-organised, opportunistic computing

Security in presence of scarce resources:

- Security for self organised, and other self* like ubiquitous computing systems
- Security of sensor networks : adaptive security and data aggregation in sensor networks

#### 3.1.2.4 Security of services and content, of software and data

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context. The goal is to build components, products, services and systems with an acceptable and affordable assurance of trustworthiness.

- Security of services: security policy compatible with business models; secure software lifecycle management; security of increasingly dynamic aggregation or composition of services; security of middleware, distributed grids, peer-to-peer exchanges, collaborative work platforms, distributed applications involving a large number of simultaneous users.
- Protection of content and Intellectual Properties:
- Usability

## 3.2 Trust, Privacy and identity management (metasystems) infrastructures

### 3.2.1 Trust and Privacy Infrastructures

#### 3.2.1.1 Trust

1. Trust infrastructures (Public and/or Private Trust Infrastructures): instrumentation of the network periphery provided by trusted new stakeholders, computing trust and security assurance, using diverse trust models (by reputation, by recommendation, by frequentation, by voting). Trustworthy providers may coexist for various services, with different levels of confidence (governmental, business-wise for-commerce, etc);
    b. Trust architectures and new protocols to delegate trust and partial trust;
    c. Trust infrastructures in a dynamic business environment with newcomers, insiders and outsiders, ingoing and outgoing stakeholders
2. Trust instrumentation at the end-user level: using the user as trust sensor, but also giving trust-relevant feedback to the user at the service interface;
3. Cognitive and learning instrumentation for trust:

    Due to sophistication of technology, integration of abstract components, co-ordination of services, autonomic tools are needed to increase confidence in the complexity management for the societal acceptance.

4. Profiling services and communities

   Trust and privacy issues need to be addressed for the relationship between user and services, communities of users and categories of services.

#### 3.2.1.2 Privacy

1. Privacy infrastructures: protocols, tools to check privacy assurance, and multi-identity systems keeping privacy;
2. Privacy of personal sensitive communicating devices: massive deployment of intelligent devices (3G terminals, PocketPC, PC) and growth of sensitive personal data
3. Privacy & Traceability of personal behaviour:
   a. Unobservability (controlling unwittingly tracings), unlinkability through search engines or social networks while supporting user's profiling and tracking to enable personalised services;
   b. Usability with diversity (diversity in Europe);
   c. Ethical issues;
4. Multi-party security & privacy protection technologies.

### 3.2.2 Identity Management metasystems

Identity provision, choice and management: real and virtual, distributed & multi-layered, partial - ID's for users, systems, devices, services. Make existing and future identity management systems interplayable.

Quantification of S&P interplay + user-in-the-loop/user-in-control(?) S&P characterization.

- Identity management, accountability, traceability frameworks:
  - at the network level to balance privacy and traceability and prevent cyber-crime and frauds (Remark: several frameworks may coexist; protocols to interact with foreign frameworks are an open issue.)
  - at the service level with pseudonymity, while keeping large anonymity;
- Interoperable framework throughout European Member States of Identification and Authentication
  - with multiple authentication devices (using multimodality: biometry, RFIDs, NFCs, physical objects, etc);
  - taking into account diversity of services (governmental, financial, medical) and richness of cultures;
  - management of profiles and identity attributes, keeping privacy, while improving searching and indexing relevance;
  - auditing and reporting, access and authorization control.
- Standardization of effective and yet federated authorization frameworks

## 3.3 Underpinning engineering principles + transparency / accountability architectures + measuring

### 3.3.1 Engineering principles to establish trust, privacy and security

This covers

- Measuring trust, security & privacy for improving capabilities for engineering
- Establishing transparency, accountability and privacy properties for the main computing entities and domains
- Transparency, accountability and privacy / pseudonymity architectures

### 3.3.2 Metrics and tools for ever-increasing complexity, quantitative security assessment and predictive security

### 3.3.3 Measurements and data collection at a large scale to manage complexity

- to measure availability and maximum downtime, to feed trust models, to configure in real time protection devices, etc, while achieving balance of privacy and security.
- to build large scale systems for crucial societal applications, taking into account composition and evaluation (metrics).
  - composition of systems, systems of systems
  - pervasive environment with scarce resources
  - circumvention security models, survival systems
  - behavioural and mobility models

### 3.3.4 Enabling technologies and standardization

- Declarative languages in security: metadata, ontologies.
- Multimodal biometry, secure OS for smart phones, TPM environment, new cryptography (elliptic curves);
- Standards in security to make tools and instruments interoperable or compatible.
- Certification and measuring level of confidence.

### 3.3.5 Cryptography

- packet encryption at 100 Gigabit/s, flow authentication at 1 Terabit/s;
- deployment of new digital signatures : cryptography of new schemes for digital signatures (to overcome the current hash function attacks);

## 3.4 Data, Policy Governance and socio-economic aspects

The FI will provide a new volatile, massive and dynamic “urbanization” of data throughout clouds, networks, smart ecosystems. The status of these data, distributed all over the world, with multi-legislation will give to the data governance an important glue role, allowing a seamless but controlled way to deal with information.

### 3.4.1 Data and Information governance

Acquisition, dissemination, access, storage issues in the ubiquitous scale-less Web x/Cloud

### 3.4.2 Data management and liability issues

Security is desired to be technology invariant (not technology-agnostic).

### 3.4.3 Multi-polar governance and security policies between a large number of participating & competitive stakeholders

1. Mutual recognition security frameworks for competing operators: Telecom Operators, Network providers, Service/content providers; sharing security secrets: improvement, or replacement of PKI-like security infrastructures, improvement or even replacement of DNS and ONS; collaborative and shared security mechanisms;
2. Transparent security for re-balancing of the unfair, unequal face-to-face relationship of the end-user in front of the network: governance of the infospheres of people => scalability, traceability, log data management, accountability management. Security, trust & privacy policy management aspects: automatic policy enforcement, policy negotiation;

3. Instruments for early detection of attacks: new methods to filter adware, spam and eradicate malware and viruses (included on 3G++ smart-phones), tools and mechanisms for large-scale test-beds dedicated to security (attack simulators);
4. Real time and large scale tests for crisis management procedures.

### 3.4.4 Economical aspects

1. Business models
2. Security markets for identity management

# Annex 1 Summary of Findings – WGs workshops #1 and #2


**Coordination Action –** ***Think Tank for Converging Technical and Non-Technical Consumer Needs in ICT Trust, Security and Dependability***

# T-T Working Groups - Workshops 1 & 2: Summary of Findings

**Issue:** **Issue 1.0**

**Date:** **09-Jul-2009**

**Editors**: Keith Howker khowker@tssg.org
Jim Clarke jclarke@tssg.org
Brian Foley bfoley@tssg.org
Kieran Sullivan ksullivan@tssg.org

## Preface

This report consolidates the main findings of the two Think-Trust Working Group workshops. Their main purpose was to look at where specific efforts are needed to deliver trust and security for the globally-interconnected digital information and communications infrastructure (sometimes referred to as cyberspace), and particularly for the Future Internet. This was mainly with respect to R&D, but the required "non-technical" dimensions of the environment, eg, the regulatory framework, awareness, personal aspects of usability, were also considered.

The workshops concentrated on a user-centred perspective: concentrating on the needs of the users themselves, their privacy and digital sovereignty and the services they use, but also remaining conscious of the defences needed for the underlying infrastructure.

The findings are in response to considerations of the range of problems from currently identifiable shortcomings to the challenges that anticipate future user requirements and the rapid developments in technology and usage:

(a) further or new research to develop technologies and potential solutions to the issues and challenges;

(b) adaptation and re-engineering, applying currently-available technologies;

(c) education & awareness
- for the user
- for industry (what needs to be done, and what possible incentives can be identified/provided)
- for policy makers (implications of new developments)

They are not presented here as detailed recommendations or worked-out statements of requirement for future R&D. Instead, in their totality, they can be used as evidence, back-up or reference for this purpose with some careful consideration.

### Common Assumptions

There is broad acceptance that the current Internet and accessed services fail to provide the means to satisfy quite basic needs for trust, security, and resilience, and that something has to be done to fix the situation – *The status quo is no longer acceptable* [1].

Other than SSL, there is little to protect the ordinary user's information and identity whilst in transit, and no guaranteed protection once in the hands of a service provider other than the requirements of the Directives [2], which are frequently not met. Specialised users such as finance and government may have developed in-house and private network protection, but all Internet users appear vulnerable to certain attacks and accidental malfunction. With increasing global dependence for much social, economic, and administrative activity, the consequences could be catastrophic [3]

Some general characteristics of future digital environments are:

- that it will be a ubiquitous and pervasive, comprising multiple heterogeneous, polymorphous infrastructures and technologies that must interoperate and that will dynamically interconnect, (re)configure and compose;
- that user-centricity is a critical consideration and goal;
- that the current problems must be fixed, and that trust and security be taken fully into account for future developments;
- that we cannot predict longer-term what entities, protocols or business scenarios will be entailed in the Future Internet [4].

## Summary

The main goal of the Think-Trust Working Group workshops has been to provide findings and recommendations for input to the RISPEPTIS [5] Advisory Board for its report, and to feed into the considerations and planning of future research in the Framework Programme. The first workshop took a general, open approach; the second focussed on four use cases, proposed by RISEPTIS, together with material from related sources including current projects, the FIA initiative, and ICT2008 sessions, etc. The use cases covered the trust and security needs for electronic identities, the challenges of joined-up eHealth services, Cloud computing, and the nomadic and mobile user. The common theme was to place the European user and citizen central to considerations, but also to look beyond, to the global context.

Taking as given the general statement of the needs for trust and security, a number of fundamental areas of concern were identified. The conclusions may be summarised in two groups: the first mainly from the user standpoint, with the second looking at means (mainly technological) of supporting the users' needs. (This outcome corresponds well with the scope of the two Working Groups.)

The headline concerns of the first group are about privacy, identity management (IDM) and accountability in the information society. These are typified by eHealth where the user/patient is right at the centre of considerations, with certain rights, duties, responsibilities, and controls, together with the generic problems of provision, use, and management of all aspects of identity – from human users to inanimate entities. These resolve mainly into matters of privacy and data protection, with a re-balancing of the transparency of users and services, and also the need for support of the user in an increasingly complex and difficult environment. The wider needs of privacy concern the protection of all aspects of identity-related information, not only the prevention of unauthorised or unintended disclosure of the primary parameters of identity, but also limitations on building quite unique identifying or identifiable personal profiles by amassing and aggregating snippets of information trails that users currently leave behind. Similarly, data protection is not only about technical prevention of disclosure of personal information, but also about the responsibilities of those responsible for handling, processing or storing it.

The second group centres on what is needed to support the nomadic, mobile user, and to enable the trusted use of Cloud-based services. A number of key characteristics and requirements are identified, together with an indication of possible regulatory support. These highlighted the need for a *standardized* architectural framework for trust and security, with the use of virtualisation to maintain separation between entities in an environment where physical boundaries have broken down. Within the architecture, a measurement infrastructure is needed, that can monitor security status and indicators, identifying and analysing attacks and intrusions, and building insight into merging threats. Continued development of underlying technologies is needed to keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Accountability, that must be respectful of privacy, is seen as vital in ensuring transparency, deterring malicious action, and providing diagnosis of failure. Possibly also typical of other platform/service-related areas, a specific need for automated security policy governance was identified, extending from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to remedial actions for non-compliance.

# 1 WG1-related – Security, Dependability and Trust in the Future Internet

## 1.1 Architecture for Trust and Security

The requirement is for a frame of reference that establishes what are the components, and how do they relate and interact, how do they compose, and how are boundaries, regions (domains) established and regulated: how does it work (correctly) and what happens when it malfunctions. The reference framework needs to support the design and specification, modelling, implementation, and operation and monitoring of the system. The emphasis is on the interoperability of all aspects of trust and security, and, therefore, there is a need for standards to describe heterogeneous entities and express the dynamic relationships between them, in order to:

(a) provide for robustness of networks, network components, end-systems and –components to protect against intrusion and damage;

(b) protect the user, user information, and services.

Many topics below call for some sort of framework, mainly to support interoperability. These potential components need to be normalised and built in to a unifying, comprehensive Architecture.

**Architectural issues**

Architectural support for dynamic, contextualised trust is needed; this entails requirements for tools and standards to express and to deploy interoperable (security) policies, together with the tools necessary for distributed trust interrogation and verification.

Architectural support must be provided for trust and privacy aspects of the Future Internet:

(a) first, with regard to transparency - security monitoring, observability and measurability and for data logging and log access;

(b) second, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties.

Architectural support for dynamic, contextualised trust is needed; this entails requirements for tools and standards to express and to deploy interoperable policies, together with the tools necessary for distributed trust interrogation and verification.

The requirements for accountability (see below) illustrate these needs: though the user can be fully accountable within the defined local context, the privacy of the user must be protected by that local domain, and inappropriate or unauthorised logging and tracking information should not be made visible outside. Where there is a need for external accountability, for use of a remote service, say, then the specifics should be set as part of the service agreement for service-access in line with (possibly dynamic) policy agreements between the domains.

## 1.2 Accountability

Accountability is fundamental to developing trust in ICT networks and services. All actions and transactions should be ultimately attributable to some user or agent (inc. as a special case Anon?). Accountability brings greater responsibility to the users and the authorities, while at the same time holding services responsible for their functionality and behaviour. It is noted that in addition to necessary technical mechanisms, there is a requirement for legal and regulatory backing to provide for appropriate sanctions and redress.

Accountability mechanisms naturally encounter problems where large amounts of data are being logged. There are also inherent privacy concerns surrounding the disclosure of such logs; there may appear to be tension or conflict between Accountability and Privacy; thus, accountability must be privacy-respecting. Engineered properly, it does in fact support privacy by, for example, providing the ability to trace accidental, incompetent, or malicious access to personal information (both owned-by and about), and working with properly protected identity in defending against incorrect allocation of responsibility.

Robust accountability is also seen as a deterrent against unauthorised intrusion – malicious or accidental; however, this must be in conjunction with, rather than instead of, access controls based on strong identification.

When establishing a means of redress by means of accountability/responsibility logs, a business-level model may be required. Lessons may be learned from the insurance sector, where any action taken must be observable by all parties involved, and where visible rules and policy awareness are a prerequisite. (note: see also policy governance, below)

Such observable action and familiarity with regulations will not be made any easier in the 'Internet of Things', where various heterogeneous devices will be present. Thus, there is a strong requirement for architectural support if accountability and observation are to be delivered in the Future Internet. Such provision is lacking in the current multi-layer, multi-domain architectures.

Interoperability between accountability domains will require new work in technical standards together with possible regulatory support – an architecture/framework defining boundaries, domains, mechanisms, protocols, and processes to deliver comprehensive interoperability.

## 1.3 Virtualisation

As physical domains and frontiers dissolve and blur, new virtual separations and boundaries must still be established, and maintained in cyberspace. Virtualisation and the mapping of physical resources into virtual constructs will need to be developed and extended. Compartmentalisation provides a means of isolating and protecting areas of trust, and controlling relationships with other areas. It also supports the simplification of complex structures into understandable, manageable components.

## 1.4 Interoperability

A specific need for automated (security) policy governance was identified. This governance extends from the formulation, agreement, and establishment between parties of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to the remedial action and redress for non-compliance. The arena for all this is again the generalised, mobile, polymorphic dynamic environment. The big challenge appears to be how to provide it without burdensome operational overhead and costs.

However, it appears that this may have common characteristics that are 'typical' of a number of basic functions, which are required to operate across a range of platforms, services and entities. (Are these common characteristics in fact aspects of policy agreement? For example, agreement between entities about their relationship? How to handle detailed aspects of, say, accountability, data protection, privacy? etc.)

## 1.5 Measurability, Metrics, Monitoring, and Reporting

Monitoring and measurement of events, actions, operations, etc. is necessary for an insight into security-related behaviour, both normal and abnormal. This allows the better provision of defences and responses for the benefit and improved protection of the network, the user, and services.

A broad understanding is required of metrics and what is to be measured, of the scope for a measurement and monitoring infrastructure, analysis of attack and failure, the economics (costs and benefits), and tools for incorporation into network systems and services that will contribute to their transparent behaviour.

Q: ultimately, is the only common unit <cost>
(rather than, say, <impact> = (*frequency* ∗ '*seriousness*')per *operation* per *user*)

Traffic and incident data relating to abnormal security events – intrusions, attacks – will support improved recognition and analysis, in turn leading to improved countermeasures (defence and response).

The gathering and sharing of data on attacks, intrusions, and system failures is understandably a sensitive issue to the victim. In addition to plain embarrassment (personal, .com and .gov contexts) such information may be of benefit to an adversary. However the sharing of such information is

vital to the improvement of defensive responses, planned recovery, and possible counterattack. The incentives to share has to overcome the reluctance; these may in extremis include regulatory reporting requirements if seen as part of a move towards a robust and resilient infrastructure that supports societal values, personal privacy and maintains a fair and open economic market-place. This will enable the establishment of trusted collaborative centres for data collection and response solutions.

Once again, some standardised framework is needed to allow controlled, trusted sharing and processing of information.

## 1.6 Protection of Network Resources

Although the findings of the Working Groups have been mainly in terms of the needs of the user, ultimately a dependable underlying infrastructure is critical to delivering the benefits from those areas.

Simplified goals include

- prevention of intrusion and penetration by accidental or malicious action;
- built-in robustness and recoverability for users, services, and the (communications) networks and their components;
- redesign, re-architect, and re-engineer as and as necessary, where this may have to include protected, privileged, channels for critical infrastructure, and even physical separation for emergency control and management of security and protection (see below).

The information and communications networks are largely owned and operated by the private sector. There are inevitably costs in providing the robust engineering needed, and public-private collaboration is likely required to ensure delivery.

The development of collaborative centres for incident reporting and collection, as 0 above, is vital to maintaining a vigilant and responsive defence against intrusion and attack – and accidental failure. International cooperation is essential in developing a coordinated response capability to major incident and threat, and again, public-private collaboration is needed to develop a comprehensive approach.

## 1.7 Technologies and Engineering to support multi-level security and assurance

The underlying security technologies and techniques need to progress so that they keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment outlined above.

- Cryptography: fast, cheap, light, (low power, ease of use and support, etc.) alternatives;
- Trusted execution (environment) – how else do we know that what is supposed to happen really does happen;
- Trustworthy functionality – SW and HW; how to design, produce, and assure trustworthy components, and how to build them into larger trusted entities and assemblages? This calls for tools (themselves trustworthy) and ‘criteria’ that will support the policy governance outlined above. The technology needs a platform-independent dimension to allow for interoperability of trusted entities – in addition to the security aspects of trustworthiness, we need to address the wider issues of quality and dependability;
- Measurement and metrics – related to the previous item – we need to be able to measure aspects of trustworthiness, and to articulate and quantify the dimensions and units; this is required in the wider field of assessment of trust/risk and security/vulnerability;
- Basic engineering (1): we need to weigh up the considerations of cost and economics, power and energy versus strength, performance and functionality;

- Basic engineering (2): control and management infrastructures separated from the normal user/service 'layers', cf <out-of-band-signalling>, possibly physically separate, higher-cost, hardened mil-spec connection and functional components, so not subject to common failure and attack (the converse of current sub-letting of some Critical Infrastructure to the public networks, however this is not to suggest that management control should share cyberspace with all CI)
- Education, Training, and Awareness: in addition to the general user help and support, above, there need to be standards for professional training and proficiency, and the tools and methodologies for the designers and engineers to build and maintain the future networks;
- technological vigilance – what is coming over the horizon, and what are the implications (eg, quantum technologies, nano-technologies, bio-(geno-)technologies, photonics, … )

# 2 WG2-related – Privacy and Trust in the Information Society

Typified by e-Health, as a high-demand instance, – putting the user at the centre of considerations, with rights, duties, responsibilities, and controls, and the problems of provision and management of user identity:

- Privacy: protection of all aspects of 'me'
  - Identity-related, location and time, my data, and what I do, in conformance with agreed policy
    (Note: There may be non-negotiable elements – I cannot by law forfeit or deny certain rights and duties, say)
  - Measures to control profile aggregation, to avoid and also to clean-up the detritus in the wake of our activities, plus regulatory controls to outlaw intrusive practices.
- Data-protection: clear responsibilities for data-controllers
  - Responsibilities and liabilities;
  - How and where data is stored and handled, and what is permissible (authorised?) use of user-data – what actions and by whom (includes delegation), together with effective controls

## 2.1 Support for Personal Information Control and Access

User-centric identity management, providing strong mutual authentication between data subjects and data controllers is a pre-requisite, however more research is needed into how personal data should be stored and structured by data controllers to maximise the transparency available to individuals, and to minimize the costs and burdens of fulfilling access requests. Increasing the depth and scope of the personal data available to data subjects online may increase privacy risks unless accompanied by a holistic approach to system security design. Tools are required to enable consent management to comply fully with EU D-P rules – eg user access to personal data and to help data-controllers to comply

As in may other topics here, a balance between privacy and justifiable accountability has to be struck.

## 2.2 Identities and Identity Management

Identity lies at the heart of trust and security requirements and issues. It also lies at heart of the solutions to satisfy these issues. In addition to identities of, or attached to, humans and their organisations, all entities, real and virtual, in the digital environment must be covered – naming and addressing, but in new dimensions. Identity and identification need to be globally usable, and to interwork at several levels.

The requirement is for a framework for identity provision/creation, handling, and usage that supports interoperability between different regional or cultural domains:

- Identity provision and global mutual recognition between administrations: official identities, organisation-related identities and roles, personal (cf nick-names) and ad-hoc/temporary/one-time IDs or aliases;
- Management and use of complex/fragmentary/partial identities, including roles, anonymity and pseudonymity within certain limits, that respect privacy and freedom of expression but restrict damage to innocent individuals and groups, and subversion of society and nation.

Kim Cameron's Laws of Identity [6] provide guiding principles to how identity is to be protected and respected.

**Methodology for multi-party security and privacy IDM design, including metasystem standardisation**

The multi-party aspect concerns the fact that any transaction typically involves multiple parties (eg, clients, servers, peers, notaries, etc.) based in different security domains under different privacy regimes, each involving different identity providers and policy rules. The topic area includes the meta-system issues raised by the need to interpret, translate, and optimally reconcile policy rules, statements, and terms expressed in different languages to represent different semantics across the different domains of the parties involved. Resolving such issues will clearly require common cross-domain standards.

**"Minimum disclosure" credential management**

Although theoretical approaches and some prototyping do exist, we are still far from deployment in practice through lack of common UI design and policy standards.

Basic cryptographic designs exist to build credentials that can be used to support user-centric, limited disclosure of identity information. These need to be complemented by suitable open standards and semantics that can be leveraged to create an ecosystem and a market that will justify the investment for developing necessary products.

A consequence is also that if minimum disclosure is 'per situation', then authentication requirements are also specific (and minimised) to the needs (and context) of what is being accessed.

## 2.3 Privacy and Data Protection

A fundamental right, recognised in European law and tradition, is the respect and protection of privacy in terms of information about or relating to the individual, together with the data that belongs to the individual. Many high-profile instances of disclosure have been incompetence – human error – but there are many instances of active malfeasance (even if some may ultimately be in the public interest). Legislation is all already in place and is being further developed such that it establishes responsibilities for those in charge of information; but tools and facilities are required that will enable data controllers to discharge their duties properly. Further policy and technical measures are needed to combat the covert amassing of information relating to individuals and groups – profiling, aggregation, data-mining and crawling, etc. – both before and after the act: possibly to outlaw and prevent the extraction of information but also sweeping up personal detritus that may be disclosed or discarded in ignorance.

## 2.4 User support and orientation

The complexities of how security facilities and mechanisms are to operate are beyond the comprehension and capabilities of all but a handful of experts. Some form of automation, provided by helpful interfaces, tools and off-the-peg profiles, is needed that will allow the user to make sensible decisions to suit personal circumstances and preferences. But to make sensible decisions, even if only to select some typical, standard profile, there is still the need for awareness by the user of what is going on, what are the risks protected against, etc. Therefore, some awareness programme or Help facility should be available, providing a wide range of support and advice from the ICT naïve to the reckless know-all. This will require close cooperation between the technology designers and ergonomic and usability experts.

The general usability of the security facilities is critical to success; again this has to provide for the complete spectrum of user-expertise: from the above help for the complete novice to interfaces and toolkits for network administrators.

**UI design according to privacy requirements**

There is currently a lack of research in user-interface design based on users' privacy requirements. Meaningful and understandable controls are required. Strong authentication, without the need for strong identification is one goal (i.e. non-declarative, strong authorisation). There also exists a need for tools to assess risk. For example, how do we know what is happening in a data controller? Could a PKI be implemented for a data controller?

It was noted that current policy statements from service providers are not designed to be understandable by the users, but to get access to their desired service or information; users accept, with a tick-in-the-box, privacy policies that may well not be in line with their needs.

Interoperability and consistency of privacy policies calls for tools and standards as in (0), above.

## 2.5 Trust Management & Governance

Firstly, some workable definition for trust is required; which may be linked to accountability and governance but also to the dependability of systems and their operational transparency. Common languages / translators and protocols for trust policy, specification and negotiation would be a good starting point. This could then allow the construction of trust as an entity itself.

Localised (contextualised) individual points of trust can be used as collective indicators and, for example, be leveraged to measure the consistency of multiple (potentially trustworthy) actors. Multiple channels could also be used, to increase confidence via independent routes.

A number of temporal aspects of trust must also be managed, given that any degree of trust accepted may only be on a short term basis, especially in real-time scenarios, as well as the fact that it may be only determined using incomplete/delayed contextual information. The trust lifecycle, incorporating the formation, breakdown, and recovery of this trust must therefore be fully supported, with contextualised, distributable, interoperable, and understandable policies in place to implement and manage dynamic trust relationships.

Formal semantics and syntax for trust management and operation are required, capable of differentiation between

- objective assurability against recognised criteria and standards
- subjective trust based on reputation, recommendation, experience, … .

## 2.6 User-Service Relationships

The user needs service access that provides a proper mutual balance of transparency and accountability with respect to rights and duties. At present, this balance appears to be in favour of the service provider – little more than, for example, **<I accept> – click!** – take it or leave it. In practice access is going to be much more complex and dynamic than is currently the case, and hence a framework is needed that will provide for the performance, in real time, of the agreed terms of the relationship between service and user (client). The user wants to be able to trust what is happening with (their) information, and how agreed duties of care are discharged, even though there will be discontinuities, change of device, change of location, etc.

Service providers should be able to present their security policy in terms of claims of the responsibilities and protection that they offer – with respect to, say, the SP's policy for ensuring privacy of personal information, or what protection is offered for corporate data, or the accountability relationship between parties . These claims should be verifiable by the user. The resulting agreements should then be manageable in line with the proposals in 0 above concerning automated policy governance.

## 2.7 Non-declarative strong authentication

There is a clear need to replace username/password login by stronger schemes while not exploding the costs for authentication supported by services providers. Today, users can select any

credentials they like in a "declarative" way. This brings an advantage to allow anonymous usage of services, but it also comes with major issues and crime risks for large services like Web mail or web-based applications. "Non declarative" authentication mechanisms can be biometrics, two-factor authentication (what I know + what I have) or new schemes to simplify login. The goal is to ensure that traceability, when required by policies, will be possible. The internet is not a special case in our society. Protecting privacy does not mean zero-accountability. Policies will define where traceability is required and a strong authentication mechanism, responsible and non-repudiable, is highly needed.

## 2.8 Privacy friendly biometrics – "One way" enrolment & usage protocols

While a biometric process may not completely eliminate duplicate enrolments, they are, nonetheless, a continuous means for identification. 'Supervised' enrolment protocols may well be incorporated into identification and authentication systems, based on biometric processes. Carrying out cryptography separately from biometrics has the virtue that one is decomposing the solution into two simpler, well-established problem domains. However, owing to the inherently noisy nature of biometric templates, doing crypto and biometrics separately would appear to require using a central database of biometric templates if the design goal is unique enrolment of individuals, in order that matching can be done against previous enrolments. In summary, this refers to a system where you could capture a live biometric on someone, together with a hardware token, and without a central template database. It would be a breakthrough to have a practical design where it was not logically necessary to have database of templates in order to implement unique (i.e. non-duplicated) enrolment of individuals (in some application domain). When discussing privacy-friendly biometrics as a possible solution area, it was agreed that a clear distinction must be made between supervised biometrics (e.g. border-control) and unsupervised biometrics/registration (e.g. building-access using retina identification). The trust relationship between the stakeholder./.user and the registration source (e.g., government, bank, organisation) is a key consideration factor here.

## 2.9 Virtual social control, e.g., virtual neighbourhoods, including reputation systems

If the Future Internet were to become a multi-tier system consisting of a highly controlled and mostly automated part and a creative, open, but inherently insecure part, research must be done to understand how social disapproval and negotiation mechanisms can be implemented in the future creative Internet. The practical aspects of research include virtual social interaction environments, reputation generation and maintenance, negotiation, forgiveness, and restitution. The main aim is to facilitate trust and understanding.

## References


[1] US Cyberspace Policy Review (at 'Executive Summary')

[2] European Directives: *Data Protection* [Directive 95/46/EC] and *Privacy* [Directive 2002/58/EC],

[3] EU Ministerial Conference on Critical Information Infrastructure Protection Tallinn, 27-28 April 2009

[4] The Butterfly Effect: that massive changes may be the result of (sequences of) small, quite random events or actions in the past: James Glieck, *Chaos: Making a New Science* (1987)
*however*, the converse is that it is generally possible to discover with 20/20 hindsight the route whereby we arrived here (cf weather, financial crisis, …)

[5] RISEPTIS: Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society; see http://www.think-trust.eu/riseptis.html

[6] Kim Cameron's Laws of Identity

*Grant agreement number:* 216890


*Project title*

Think Tank for Converging Technical and Non-Technical Consumer Needs in ICT Trust, Security and Dependability

*Instrument*

Coordination & Support Action

*Deliverable reference number and title*

D3.1B Recommendations Report (Interim)

| | |
|---|---|
| *Start date of project:* | 1st January 2008 |
| *Duration:* | 30 months |

# Contents

# 1 Introduction

The RISEPTIS Advisory Board report '**Trust in the Information Society**'[1] sets out the high-level risks and challenges associated with trust in our digital environment (Cyberspace, Information Society, Future Internet, etc.). Trust is required to support our growing dependence on this digital environment for many aspects of our private and working lives. The report makes six recommendations for action in this respect.

The Think-Trust deliverable D3.1 is complementary to the RISEPTIS report, and should be read in the light of the RISEPTIS recommendations. The deliverable focuses on the research challenges which need to be addressed to realise the RISEPTIS recommendations. These challenges and research priorities are consolidated from the perspective of the Think-Trust Working Groups (WGs), which have met twice in plenary session since the start of the Think-Trust project. Deliverable D3.1 is an iterative document, refined in three versions;-

- D3.1A, produced in Summer 2009, outlined a broad vision of a digital future, its benefits and possibilities, and consequent risks and dangers.
- **D3.1B, highlights a set of interim research challenges, arising from the RISEPTIS Report. Further detailed background on aspects of these challenges can be found in D3.1A[2]. D3.1B is being submitted to the Commission as input to their deliberations on the 2010 Work Programme.**
- D3.1C, due for completion in Summer, 2010, will take account of input from various stakeholders and interest groups. A public, online consultation process[3], launched at an FIA workshop on October 7th, 2009, has been initiated to secure this input. The inputs will be used to refine and further develop the challenges identified D3.1B. The third and final version of D3.1 (i.e. D3.1C) will present the results of this public consultation process.

Figure 1 shows the development of D3.1, throughout the Think-Trust timeline:

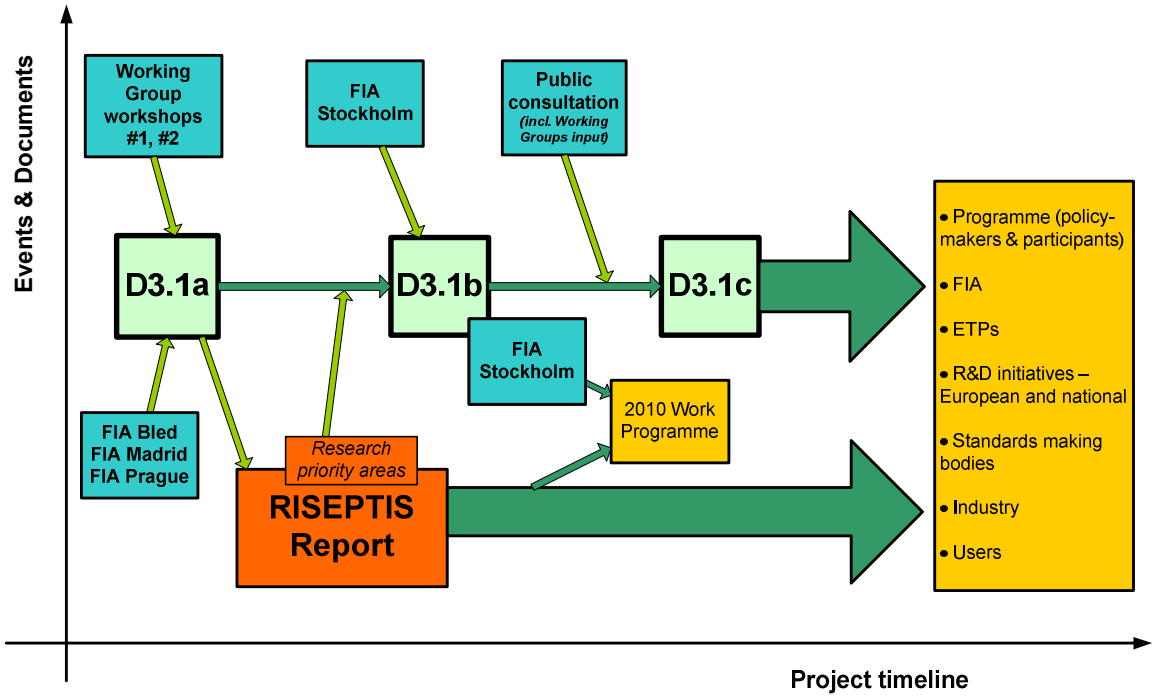



**Figure 1** *Development of D3.1*

[1] http://www.think-trust.eu/riseptis.html

[2] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[3] http://www.think-trust.eu/general/news-events/public-consultation-launched.html

# 2 RISEPTIS

The RISEPTIS Report[4] identifies six high-level recommendations. The focus of deliverable D3.1B is to detail the research challenges arising, in particular, from recommendation 1 in the RISEPTIS Report, which recommends the stimulation of inter-disciplinary research in the area of trust and security.

Deliverable D3.1B also gives a high-level examination of the research and technology implications of the other five RISEPTIS recommendations. However, these require substantial social, legal, and regulatory developments, in addition to the development of appropriate technical infrastructures.

The six RISEPTIS recommendations are outlined below:

## 2.1 Research, technology development and deployment

**Recommendation 1:** ***The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the*** **Information Society*.***

This recommendation is specifically about advancing European Research and Technology development. Four priority areas are proposed by RISEPTIS. These priority areas reflect the inputs that have been provided to the RISEPTIS Advisory Board by the Think-Trust Working Groups. The four priority areas are:

(a) Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet;

(b) Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability;

(c) Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography);

(d) Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management.

These four areas are not independent and have many common underlying concepts and mutual dependencies, (which is reflected in our approach to the identification of the research challenges in section 4).

## 2.2 The interplay of technology, policy, law and socio-economics

**Recommendation 2:** ***The EC should support concrete initiatives that bring together technology, policy, legal and social-economic actors for the development of a trustworthy Information Society.***

There is a need for a supportive, non-technological framework that should be developed alongside the technical elements. For example, there is a need to provide:

- Regulatory backing for accountability between Member State jurisdictions (or beyond), as is already the case for data-protection.
- A framework for common (or mutual/reciprocal) legal recognition of e-identities and the support aspects of interoperability, (noting past histories of, say, digital signature).

Research should not be confined to a one-way flow of regulation to support technical advances. However, it has proved difficult in the past to develop the contra-flow of ideas and the demands of those with a socio-economic perspective, where, apart from privacy and data-protection, we have often had to rely on technologists putting on their citizens' hats to articulate the needs of individuals and organisations.

In addition to the engineering aspects of trust, the non-technical social and psychological components must also be understood and put into context.

[4] http://www.think-trust.eu/riseptis.html

## 2.3 A common European framework for identity management

**Recommendation 3:** ***The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity.***

This recommendation crystallises the two previous recommendations around a specific use case. The requirements of this spectrum must be explored. These include simultaneous demands for the rigorous protection of privacy, with equally robust attention given to identification and authentication of interacting entities, as well as the control, monitoring and accounting for subsequent operations.

In bringing forward the achievement of specific societal goals as part of an economic recovery programme, a large scale project has been proposed (RISEPTIS recommendation number 5) that would seek to unify and integrate various disjointed approaches to e-identity that currently operate in different European e-commerce and e-government service sectors. This initiative needs to take into account the requirements of a broader range of users (consumers) and providers of services. This will allow the appropriate engineering of solutions or the identification of further research areas.

## 2.4 Further development of EU legal Framework for data protection and privacy

**Recommendation 4:** ***The EC should work towards the further development of the EU data protection and privacy legal frameworks as part of an overall consistent ecosystem of law and technology that includes all other relevant frameworks, instruments and policies. It should do so in conjunction with research and technology developments.***

The main technological direction underpinning this recommendation is the support of legal and regulatory initiatives already under way to extend the vision of privacy and data-protection. Further research into technologies for protecting and minimising the propagation and disclosure of personal information is required to combat increasing risk of accidental or coincidental exposure.

The lapses in duty of care by data controllers will be more easily identified and attributed with the tracing and accountability capabilities recommended for inclusion in the underlying architecture.

## 2.5 Large scale innovation projects

**Recommendation 5:** ***The EC together with industrial and public stakeholders should develop large-scale actions towards building a trustworthy Information Society which make use of Europe's strengths in communication, research, legal structures and societal values - for example, a Cloud which complies with European law.***

Much of the basic technology to support further work towards trust in the information society is well known. However, certain incentives and stimuli should be applied to develop these technologies to overcome inertia and to mainstream their use. There has been a lack of long-term vision in the industry, both suppliers and consumers – 'where's the business case?' – allied with a head-in-the-sand attitude to the exposure and damage being sustained, not so much by e-business itself, but more by a commercial world that is under increasingly organised attack. Large-scale projects will provide a stimulus, putting some urgency into the supply-side and demonstrating benefits to the consumer/demand-side of business.

## 2.6 International cooperation

**Recommendation 6:** ***The EC should recognise that, in order to be effective, it should address the global dimension and foster engagement in international discussions, as a matter of urgency, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.***[5]

[5] Work in this direction is already underway via the Coordination Action project INCO-TRUST (www.inco-trust.eu)

Europe cannot act in isolation. There are indeed many benefits that will accrue from establishing a solid European platform for trust, but given the inherent global nature of the Internet and the Web, Europe must collaborate with international partners to **establish standards that will enable trusted interoperability**. As well as the necessary technical standards, there must be corresponding standards on privacy and data-protection norms. These should not only regulate what happens to information within signed-up domains, but also regulate the behaviour and accountability of the data-controllers.

The development of new approaches, such as Cloud computing, increases the urgency for regulatory and technical standards. The essence is that services are ubiquitous and pervasive, which in turn contributes to their dependability and cost-effectiveness. To this must be added the other dimension of trustworthiness. The mirror image of this is of the globally mobile or nomadic user whose requirement is for a consistent, trusted service wherever and whenever.

# 3 Context

This section provides a background context (trends, threats, vulnerabilities and risks) for the trust and security research challenges identified in section 4 of this Deliverable. It also lists the landmark topics identified by the Think-Trust Working Groups, as well as briefly describing how the Future Internet Assembly events[6] have informed the deliberations regarding the identification of future research challenges.

The overall challenge context continues to be the development of a *pervasive and trustworthy network and services infrastructure,* with the *Future Internet* as the bed-rock of the Information Society.

## 3.1 Trends

Some key features are noted here as drivers of future research action:

**Increased, heterogeneous accessibility to converged information and services. (For example, ubiquitous, mobile access, very high bandwidth fixed networks and access);**

Networks and future communication systems will have to move on from the concept of end-to-end connectivity (as in the current Internet) and embrace situations in which nodes are devices which cooperate freely and spontaneously in the absence of centralised services. Ubiquitous communication systems will demand new architectures based on the independent devices, connectivity reduced to fragments and spatial awareness of the nearby environment and local data through different nodes in the network.

**Increasing volume of transactions, and even higher volume of traffic;**

The advancement of digital technology in all areas is accelerating the rate of expansion in the volume of computer data and of the massive integration of software into our daily lives. Seamless digital technologies will gradually surround individuals, creating a tight mesh and a digital environment, which will profoundly increase usage. That is, the establishment and interoperation of the three complementary, ubiquitous environments:

- computing (information stored, processed and presented here and now),
- communication (access anytime, anywhere, using the best available channel) and,
- storage (collected, stored, described and displayed information and knowledge, available anywhere, anytime)

**Large growth of sensors and slave-labour devices (*Internet of Things*), taking over the management of routine operations in commerce, utilities, the environment, and law enforcement and security provision;**

We are seeing an emergence of contactless smart cards and radio-frequency recognition labels (parcel logistics, pet tagging, etc), networks of sensors in towns (multiple-window cameras), in the countryside (forest fire and earthquake detectors), in businesses (real-time warehouse inventory, mobile vehicle fleet sensors), networks in our homes and cars, personal assistance robots, tele-diagnostics etc. Whilst the current internet has connected 1.5 billion computers and mobile phones have connected 4 billion people, the Internet of Things may connect hundreds of billions of objects.

**Increasing mobility of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access to information and services;**

Nomadism[7] and/or mobility[8] destabilise the secure, personal cyberspace that is available when the user/device is static. The security of mobility requires an anchor of geography and time. Nomadism and mobility emphasise the need for a spatiotemporal security framework based on the *hic et nunc* (Latin for "here and now).

[6] http://www.future-internet.eu/events.html

[7] *Intermittent connection and session from various locations*

[8] *Continuous connection to a digital infrastructure and activity on the move*

**Convergence of types: voice, visual, entertainment, social and business services. (For example, twitter.gov, and 'official' blogs)**

The widespread interconnection of networks and digital convergence further accentuates the computerisation process, which is making computing, telephone and audiovisual information increasingly compatible and interoperable. Progress in wireless technology has made possible the popularisation of mobile communication and has very substantially changed the way that businesses operate.

***Nano* to *mega* computing and communication – from (i) cheap, incoherent, tiny, low-resource entities in massive numbers handling the routine, to (ii) the gigantic cooperative high-resource super-grids addressing the difficult and complex**

Computing will involve minuscule, sometimes invisible objects, with scarce resources, which are possibly non-identifiable but only traceable. These will be the end-points of a network which no longer has a few billion capillaries, but rather several Tera-nodes. Research on nano-architectures, nano-applications, and nanoprotocols, will transform the new network suburbs.

At the other end of the scale, computing will involve gigantic, complex poly-infrastructures (Internet, GRID, GSM, 3G, Galileo/GPS, the Internet of objects, Earth observation satellites). Computing of the gigantic means new services (Internet Telephony, Skype, etc.), which are also tools for surveillance, anticipation, crisis management, etc.

All of these have implications for the way society operates, and will make new and increasingly demanding requirements for trust from the users/consumers.

## 3.2 Existing threats, vulnerabilities, risks

The defects and failure/damage opportunities of the current Internet include:

- Fragility – networks and end-systems are vulnerable to simple attack, with information easily accessed, destroyed, copied and stolen, or falsified;
- Software is subject to design, implementation and usage errors, (hardware is not faultless, but more easily verified during design);
- Domino effect across inter-dependent systems in the case of accidental malfunction and/or failure, and attack propagation;
- Unprotected networked data exchange, but also via external media;
- Lack of user-awareness regarding their data, together with difficulties in understanding and availing of privacy-providing tools. The burden to the user in using these often complex tools hinders their acceptance and uptake;
- Basic usable security and trust facilities that enable the user to make informed choices or decisions.

Some malicious specifics:

- Fraud – breach of enterprise records/systems, stolen/captured credit card and bank details;
- Intrusion – Trojans: key-logging; colonisation, 'hacking';
- Impersonation through identification theft or failure;
- Phishing etc. relying on deception (spoofing) of user;
- Identity profiling from digital trails;
- Unauthorised disclosure: 'inside jobs' (police, government agencies, etc. for press and private investigators);
- Malware – viruses, worms, etc., for vandalism or blackmail/ransom threats
- IPR abuse – unauthorised file sharing, plagiarism;
- Denial-of-Service attacks

Unjustified trust – use of the 'open' net for sensitive operations (own goals):

- Defence-related – internet gateways to 'secure' systems;
- Emergency services;
- Utility management;
- Health systems;
- Financial/economic systems;

## 3.3 New threats, vulnerabilities, risks

New architectures will include structures and protocols that handle the blurring of boundaries between:

- what previously would be identifiable as domains (of, say, responsibility or control);
- real, logical, and virtual domains;
- where functionality actually lies – in hardware, in software, in the network, in information itself;
- what is an application and what is a service?

These all raise new, and extended security problems, not least from their volatility and fluidity. Attention is required to ensure that the new architecture (as a whole) pays attention to its *own* security needs and implications, as well as those of its *clients*.

Specific potential for vulnerabilities comes from the increasing integration of services. These include large and critical societal infrastructure, such as power and water distribution systems, transport communication means, and information and communication systems which support these infrastructures. This gives rise to the possibility of avalanching failure.

A consequence of this total penetration of our lives is the danger of the diminution and dilution of personal privacy and sovereignty (and that of enterprises or even administrations) – the possibility of multiple *big-brothers* watching, recording, and analysing our actions.

As new more comprehensive and complex trust and security measures are introduced, they bring with them new requirements for the non-expert user to be informed and to make appropriate decisions – in many cases, < I ACCEPT> the informed default advice from the "security" interface.

## 3.4 Working Group findings (landmark topics)

Two related themes have led the thinking of the Working Groups:

- **user-centricity: placing the individual user at the centre of considerations and requirements**
    - rebalance relationship of user/consumer with service providers
    - control over *MY* identity/data
    - usability/accessibility of security facilities
    - protect users, (from others and themselves)
- **the need for the users to be able to trust their own digital environment as part of a larger ecosystem – the *network*, *Information Society* or even *cyber-space***

In this context, the following areas for further research were identified by the two Working Groups. For further details on these areas, please refer to the consolidated findings of the two Working Group workshops in Annex A.

**Architecture**

- Architectural issues, e.g. dynamicity, accountability, transparency, etc.
- Architecture for Trust and Security
- Interoperability

**Instrumentation**

- Measurability, Metrics, Transparency

**Accountability**

- Accountability and Responsibility
- Accountability

**Trust engineering**

- Trust Management & Governance
- Virtual social control, e.g., virtual neighbourhoods, including reputation systems

**Identity**

- Methodology for multi-party security and privacy IDM design, including metasystem standardisation
- Identities and Identity Management
- Non-declarative strong authentication

**Privacy and data-protection**

- Privacy transparency tool support
- "Minimum disclosure" credential management
- Privacy friendly biometrics– "One way" enrolment & usage protocols

**Usability**

- User support and orientation
- Use of Services
- UI design according to privacy requirements

**Engineering & technology**

- Technologies and Engineering to support multi-level security and assurance
- Virtualisation

## 3.5 Future Internet Assembly Events

The Future Internet Assembly (FIA) has held four events thus far, in Bled, Madrid, Prague and Stockholm. Breakout sessions and discussion on trust, identity and privacy have taken place at each meeting. These discussions have also informed the research and development challenges outlined in this interim Deliverable.

One of the chief FIA goals is to identify cross-domain research themes, among the different cluster areas[9], namely:

- Management and Service-aware Networking Architectures (MANA);
- Services and Software (platforms and infrastructures);
- Content Creation and Media Delivery
- Trust and Identity;
- Internet of Things;
- Real world Internet;
- Future Internet Research and Experimentation;

[9] http://www.future-internet.eu/home/clusters.html

- Future Internet Socio-Economics.

More information on related cross-domain issues (including presentations, position papers and event reports) arising from the FIA sessions is available at the 'Trust and Identity' wiki[10] (facilitated by Think-Trust) and the FIA page of the European Future Internet Portal[11].

[10] http://security.future-internet.eu/index.php/Main_Page

[11] http://www.future-internet.eu/home/future-internet-assembly.html

# 4 Research & Development Challenges

This section outlines the key research challenges that require attention in order to provide trustworthy hardware and software for the Information Society, based on the four priority areas identified by recommendation 1 of the RISEPTIS Report. The research challenges also take account of the context set out in section 3 of this document (Working Group findings, FIA outputs, etc.), as well as recognising the topics already covered in previous calls (up to Call 5).

## 4.1 Trust 'engineering'

The lack of trust in ICT infrastructures (including entities, actors, service providers) shows itself during *operation* (because systems must confront intentional attacks or cope with accidental breakdowns), and at the *design* stage (because security or resilience are often not included in the system's specifications). Trust is not absolute and will be quantified by the preferences and intuitive policies of users. This gives rise to the need for an overall *trust framework* (rather than a *security framework* per se), where trust-relationships between entities are established and managed to encompass trust 'preferences', trust 'policy' and trust 'weighting'. This would include:

- development, expression and use of trust indicators;
- automatic computation of trust assertions based on policy frameworks that take into account user preferences;
- life-cycle management, including maintenance, repair and recovery;
- models, methodologies, measurement of trust;
    - tools to assist users calculate it (a combination of assisting the user and quantifying personal trust);
    - to assess availability/downtime/integrity/confidentiality to feed into trust models
- delegation and acceptance.

Alternative approaches should also be explored, including more complex social controls in the virtual world, including *reputation*, *recommendation*, *frequentation*, *voting*, *gaming*, etc. approaches.

### 4.1.1 Quantification of trust, security and privacy

Advances in the insurance analogy (see 4.10) can only happen if we change how we look at the security level of systems. We need a better quantification model. Investment in experimental setups and test-frameworks that can be thoroughly measured in terms of security would advance this process. This would also allow the following question sets to be examined:

- Do results on trust experiments scale from the laboratory environment to the real worlds of the Future Internet?
- Can security predictions be generalised across different software components, programming languages, systems, environments?
- How do we collect and share security-related data for experimental research in the line of the work presented?

## 4.2 Architecture

In general, architectural support must be provided first with regard to transparency – security monitoring, observability and measurability for data logging and log access – and secondly, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties. There are a number of aspects to these architectural challenges:

- *meta* architecture – would higher-level abstractions help to structure a global information security architecture?

- *network* and *service* architectures – examine the scalability and interoperability of the current architecture and consider domains, partitioning, compartmentalisation in a Cloud environment (including dynamic service composition/aggregation)
- architectural *standards*
    - pre-conditions for interoperability;
    - verification of conformance requirements;
    - built-in emergency measures;
    - establish workable definitions concept (metadata, ontologies, etc.);
    - support for security policy management, including the ability to attach policy information to data.

A core question in this section is the "functionalisation" of security properties: wherever we are able to functionalise, we can improve the acceptance of security. Therefore, we need to ask, how can this be done in a systematic way? *Security patterns* provide a first approach, but this needs more systematic management.

## 4.3 Cyber-security: Engineering and Technology

Techniques and mechanisms to provide protection, assurance and integrity are required. These must keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Such tools should be robust and resistant to failure and attack (survivability). As well as these tools, criteria and standards to support policy governance is also required. Technologies need a platform-independent dimension to allow for interoperability of trusted entities.

- Virtualisation should be examined in this regard, since it allows complex concepts such as high-demand, critical services, to be built on top of limited technologies.
- Security in the presence of scarce resources must also be considered:
    - self-organised and other self-* ubiquitous computing systems
    - sensor networks – adaptive and able to aggregate data
- Legal domains with different priorities: how to address in a virtualised scenario? Technology is needed to support this "dynamic switch of security controls" based on legal policies.
- Education, Training, and Awareness: in addition to the general user help and support there is a requirement for standards for professional training and proficiency, and the tools and methodologies for the designers and engineers to build and maintain the future networks. (Close relationships with established CERT[12] teams and ENISA[13] would be of added benefit to this goal.)

## 4.4 Accountability

There will always be faults, failures, mistakes and attacks. Accountability is a research priority, as it creates the means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress.

There are two options which seem especially promising and coherent:

- Base the demand for traceability and accountability on global accountancy-type principles, which can encompass the whole network, and such that reliable and finely granulated incoming and outgoing accounts can be drawn up.
- Reintroduce, on an intermediary network layer, a "territorialisation" of facts and participating parties. The aim is to ensure that people and places can be guaranteed within the current

[12] http://www.cert.org

[13] http://www.enisa.europa.eu

communications system, whose weakness stems precisely from the difficulty in identifying and authenticating these parties, as well as actions in terms of time and place.

By partially moving system control towards establishing data either *a priori* or *a posteriori*, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows.

In this light, the following should be examined, with particular attention to the issues created in highly distributed service-oriented architectures (e.g. cloud computing):

- An interoperable, accountability framework, including consistent interpretation of security policy agreements; implying the need for appropriate standards for protocols and interfaces, and for tools to enable compliant usage;
- Accountability balanced with privacy: investigation of protocols that can actually address both;
- Delegation, proxy, anonymity management;
- Non-repudiable processes/records;
- Context-dependent attributability;
- Channels for investigation, analysis, liability and redress;
- Real-time, large-scale test-beds for crisis management procedures;
- Domains of accountability to protect the interests of users;
- Close attention to the engineering and economics of accountability: raw audit-trail information generated has the potential to drown the system.

Closely related, are the business requirements for accounting, billing and charging for services or facilities. Accountability processes have traditionally been based on audit trails and attribution of actions. In addition we now require:

- Anonymous/pseudonymous charging and payment systems;
- Anonymisation or impersonation heuristics to produce untraceable, but trustworthy, valid sources/channels for information; for example, for economic, social or health-related statistics.

## 4.5 E-Identity

RISEPTIS recommendation 3 calls for the development of a common EU framework for identity and authentication. It is recognised that there will not be a single, unified format or scheme for eIDs, and that there will be multiple national or regional and commercial eID domains There is also broad consensus on the need for flexible identity systems where users might have an *à la carte* choice (as an aspect of user-centricity) regarding identity-data options:

- The ability to decide on the level of security of their data streams (sent or received);
- The ability to decide the level of anonymity of these data streams:
    - The ability to choose from several possible connection types, according to the desired level of anonymity.
    - At each of these various levels, only the aspect of identity required for that particular connection is revealed.

These options give rise to a number of challenges, which would expand the development of underlying mechanisms and techniques, and use what is already available. The following should be explored from a user-centric perspective:

- framework to support interoperability between different schemes and environments (between, say, *mobile* and the *cloud*) with support for and use of partial IDs[14]
- functional requirements; e.g. as an enabler for access control and accountability;

[14] See D3.1a – *a la carte* identity

- lifecycle management of eID, including protections to restrict loss, theft, error:
    - network level – accountability to balance privacy and traceability
    - service level – pseudo-anonymity
- framework to support interoperability between different schemes and partial IDs[15]
- linking IDs with dependent concepts, such as accountability
- claim-based approaches using novel and existing cryptographic protocols to eventually avoid architectures with a central component that everyone needs to trust
- (technology supporting new) business models for central, decentralised, and claim-based approaches;
- communication setup and routing that are identity-data-aware only as necessary for the functions of the network, without making the related users identifiable.

## 4.6 Privacy

Objectively verifiable data was previously compiled and managed for specific and acknowledged purposes. Now, however, data-gathering systems operate greedily and indiscriminately, grabbing data from each and every source. This opens up new possibilities for tracing, monitoring, shadowing and digital inquisition, with the possibility of registering and following every move of every object and processing and cross-referencing this data[16]. The technical paradigm shift goes from new identity management schemes and purely technical solutions to holistic societal approaches, since absolute anonymity may be neither possible nor applicable.

To protect the identity-related data of the user, the following should be examined:

- fine granularity access control to identity-related information;
- further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data;
- use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users;
- methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction;
- possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates;
- personal/communal collector of personal garbage/litter;
- use and control of identity-related information for network (e.g. routing) purposes without compromising privacy;
- standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments;
- tools and concepts for deleting data in the internet (“forgetting“).

## 4.7 Protection

Related to **Privacy** (including business confidentiality), the protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications) require the following:

[15] See D3.1a – *a la carte* identity

[16] O'Hara, K., Tuffield, M. and Shadbolt, N. (2008) Lifelogging: Issues of Identity and Privacy with Memories for Life. In: Identity and the Information Society, 28-30 May, 2008, Arona, Italy.

- domains, partitioning, compartmentalisation – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage;
- fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc;
- mutual authentication, with multiple devices (ideally, technology invariant);
- new cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age;
- uses of eID and its components in protecting the interests of its subject (data protection, etc.)

## 4.8 Usability

The Future Internet, and more generally, tomorrow's communication networks, look to have one overriding feature: they will be focussed squarely on the individual (the citizen, the end user, the consumer). The aim of all future R&D programmes will be to influence the nature and scope of this central position. There are two viewpoints to consider:

- Does "being central" mean being observed (even monitored, spied upon) by the surrounding system? This would allow the automatic configuration of the surrounding system/services to suit the user's tastes/requirements.
- Does "being central" mean that one's choices will interact with and influence one's environment? That is, do surrounding systems support voluntary disclosure of user information and can services subsequently be re-configured to reflect such disclosures?

There are trust issues in both these instances: Do users trust the first system enough to allow it to effectively spy on them? Do users trust the second system enough to disclose their data to it? The challenge here is not to offer users a stark choice between one or other of these two options, but rather to address the downside of both.

Making usability a permanent requirement of engineering would be a step in the right direction when addressing this challenge. Specific engineered-based research is therefore required to address the following issues:

- What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered?
- What are the impacts and implications for the underlying mechanisms and functionality?
- Attention to user/system interaction: sympathetic user interfaces, but with advanced options
- Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile).

## 4.9 Management and Governance

The proper management and operation of security policies must be considered in the context of the environment in which they operate. These settings could be ambient, heterogeneous, volatile, etc. Continuity of security relationships within these dynamic environments must also be appropriately managed (if unfeasible, what alternatives can be implemented under this guiding principle?). Control could be possible at all levels: self-controlled, user-controlled, centrally controlled or community controlled.

- A framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs.
- Technical support must be provided for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions. At a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to *common law* and the support of small claims.

- The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.

## 4.10 Socio-economic

RISEPTIS Recommendation 2 calls for convergence of technology with other areas and disciplines; Recommendations 3 to 6 contain specific requirements for parallel advances in non-technological areas.

- The role of other business/industry should be examined to learn how they handle security/risk-analysis. For example, can the insurance industry balance risk and cost for different categories of users? This could lead to the formal certification of trustworthy products/services and the classification of users. Using the insurance analogy: no-claims discount, additional premiums for risky use, exclusions, etc.
- Economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons;
- The EU legal framework should be incorporated, including all jurisdictions currently covered, together with new laws and regulatory measures if necessary.
- There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?
- The market place and related drivers for eID management (and other security and protection) should be explored:
    - To place Identifying credentials on different platforms;
    - Users can switch from one to another if not happy;
    - Economic value of secondary usages?

# Annex A – Working Group Workshops: Consolidated Findings

## Architecture

### Architectural issues

Architectural support must be provided for trust and privacy aspects of the Future Internet: first, with regard to transparency - security monitoring, observability and measurability and for data logging and log access; second, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties.

Architectural support for dynamic, contextualised trust is needed; this entails requirements for tools and standards to express and to deploy interoperable policies, together with the tools necessary for distributed trust interrogation and verification.

The requirements for accountability illustrate these needs: though the user can be fully accountable within the defined local context, the privacy of the user must be protected by that local domain, and inappropriate or unauthorised logging and tracking information should not be made visible outside. Where there is a need for external accountability, for use of a remote service, say, then the specifics should be set as part of the service agreement for service access in line with (possibly dynamic) policy agreements between the domains.

### Architecture for Trust and Security

The requirement is for a frame of reference that establishes what are the components, and how do they relate and interact, how do they compose, and how are boundaries, regions (domains) established and regulated: how does it work (correctly) and what happens when it malfunctions. The reference framework needs to support the design and specification, modelling, implementation, and operation and monitoring of the system. The emphasis is on the interoperability of all aspects of trust and security, and therefore there is a need for standards to describe heterogeneous entities and express the dynamic relationships between them.

### Interoperability

A specific need for automated (security) policy governance was identified. This governance extends from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to the remedial action for failure or non-compliance. The arena for all this is again the generalised, mobile, polymorphic dynamic environment. The big challenge is to achieve this goal without incurring burdensome operational overhead.

It appears that this particular interoperability requirement may have characteristics that are common to, or 'typical' of a number of basic functions that are required to operate across a range of services and entities. (Are these common characteristics in fact aspects of policy agreement? For example, agreement between entities about their relationship? How to handle detailed aspects of, say, accountability, data protection, privacy, etc.?)

## Instrumentation

### Measurability, Metrics, Transparency

While up-to-date statistics would be useful as a starting point for the measurement of any secure/insecure entity, this information is in fact scarce, and available test data are often out of date and misleading, not being based on recent real-life measurements. Reasons for this lack of information include: rapidly changing attack modes; victims of attack typically not disclosing information, as well as inherent privacy issues contained therein; for example, proprietary data whose sharing and exposure may affect company competitiveness; and, the sheer complexity of distributed attacks.

Work on measurement of TSD-related factors is needed in order to get a better understanding of priorities for technology R&D plus actual deployment. Work already under way in this area needs to be reviewed, and possible approaches examined that could address metrics and what is to be measured, scope for a measurement and monitoring infrastructure, analysis of attack and failure, the economics (costs and benefits), and tools and instrumentation for incorporation into network systems and services that will contribute to their transparent behaviour.

A corollary of monitoring the Future Internet is that privacy concerns are inevitability raised, with a balance between accountability and opacity being required. Any measurement of security, therefore, must be implemented by a well designed mechanism to find this equilibrium. A further constraint is the need for comparative security metrics, which implies that quantitative, as well as qualitative measurements are needed.

A generally applicable approach to increased transparency (and hence trust) should be developed, concerning the provision of facilities for the accessor to verify certain 'claims' made by the accessed entity, with respect to, say, its handling of personal information.

# Accountability

**Accountability and Responsibility**

Accountability is fundamental to developing trust in ICT networks and services. All actions and transactions should be ultimately attributable to some user or agent. Accountability brings greater responsibility to the users and the authorities, while at the same time holding services responsible for their functionality and behaviour. It is noted that in addition to necessary technical mechanisms, there is a requirement for legal and regulatory backing to provide for appropriate sanctions and redress.

Accountability mechanisms naturally encounter problems if large amounts of data are being logged. There are also inherent privacy concerns surrounding the disclosure of such logs. When establishing a means of redress via these accountability/responsibility logs, a business-level model might therefore be adopted. Lessons could be learned from the insurance sector, where any action taken must be observable by all parties involved, and where visible rules and policy awareness are a prerequisite.

Such observable action and familiarity with regulations will not be made any easier in the 'Internet of Things', where various heterogeneous devices will be present. Thus, there is a strong requirement for architectural support if accountability and observation are to be delivered in the Future Internet. Such provision is lacking in the current multi-layer, multi-domain architectures.

Interoperability between accountability domains will possibly require new work in technical standards together with possible regulatory support.

**Accountability**

There may appear to be tension or conflict between Accountability and Privacy; thus, accountability must be privacy-respecting. Engineered properly, it does in fact support privacy by, for example, providing the ability to trace accidental, incompetent, or malicious access to personal information (both owned-by and about), and working with properly protected identity in defending against wrong allocation of responsibility. Robust accountability is also seen as a deterrent against unauthorised intrusion – malicious or accidental; however, this must be in conjunction with, rather than instead of, access controls based on strong identification.

# Trust engineering

**Trust Management & Governance**

Primarily, a workable definition for trust is required; which may be linked to accountability and governance but also to the dependability of systems and their operational transparency. Common languages / translators and protocols for trust policy, specification and negotiation would be a good starting point. This would then allow the construction of trust as an entity itself.

Localised (contextualised) individual points of trust can be used as collective indicators and, for example, be leveraged to measure the consistency of multiple (potentially trustworthy) actors. Multiple channels could also be used, in line with the concept of 'out of band' signalling.

A number of temporal aspects of trust must also be managed, given that any degree of trust accepted may only be on a short term basis, especially in real-time scenarios, as well as the fact that it may be only determined using incomplete/delayed contextual information. The trust lifecycle, incorporating the formation and breakdown of this trust, must therefore be fully supported, with dynamic contextualised, distributable and understandable policies in place to implement dynamic contextualised trust.

**Virtual social control, e.g., virtual neighbourhoods, including reputation systems**

If the future internet were to become a multi-tier system consisting of a highly controlled and mostly automated part and a creative but inherently insecure part, research must be done to understand how social disapproval and negotiation mechanisms can be implemented in the future creative internet. The practical aspects of research include virtual social interaction environments, reputation generation and maintenance, negotiation, forgiveness, and restitution. The main aim is to facilitate trust and understanding.

# Identity

**Methodology for multi-party security and privacy IDM design, including metasystem standardisation**

This topic area is concerned with how to design comprehensive and coherent privacy-protecting identity management systems correctly, from scratch, assuming one does not have to cope with legacy systems.

The multi-party aspect concerns the fact that any transaction typically involves multiple parties (eg, clients, servers, peers, notaries, etc.) based in different security domains under different privacy regimes, each involving different identity providers and policy rules. The topic area includes the meta-system issues raised by the need to interpret, translate, and optimally reconcile policy rules, statements, and terms expressed in different languages to represent different semantics across the different domains of the parties involved. Resolving such issues will clearly require common cross-domain standards.

**Identities and Identity Management**

Identity lies at the heart of trust and security requirements and issues. It also lies at heart of the solutions to satisfy these issues. In addition to identities associated with humans and their organisations, all entities, real and virtual, in the digital environment must be covered – naming and addressing, but in new dimensions. Identity and identification need to be globally usable, and to interwork at several levels.

The requirement is for a framework for identity provision/creation, handling and usage that supports interoperability between different regional or cultural domains:

- Identity provision and global mutual recognition between administrations: official identities, organisation-related identities and roles, personal (cf nick-names) and ad-hoc/temporary/one-time IDs or aliases;
- Management and use of complex/fragmentary/partial identities, including roles, and anonymity and pseudonymity within certain limits that respect privacy and freedom of expression but restrict damage to innocent individuals and groups, and subversion of society and nation.

Kim Cameron's Laws of Identity provide guiding principles to how identity is to be protected and respected.

**Non-declarative strong authentication**

There is a clear need to replace username/password login by stronger schemes while not exploding the costs for authentication supported by services providers. Today, users can select any credentials they like in a "declarative" way. This brings an advantage to allow anonymous usage of services, but it also comes with major issues and crime risks for large services like Web mail or web-based applications. "Non declarative" authentication mechanisms can be biometrics, two-factor authentication (what I know + what I have) or new schemes to simplify login. The goal is to ensure that traceability, when required by policies, will be possible. The internet is not a special case in our society. Protecting privacy does not mean zero-accountability. Policies will define where traceability is required and a strong authentication mechanism, responsible and non-repudiable, is highly needed.

# Privacy and data-protection

**Privacy transparency tool support**

Tools for supporting privacy transparency are required for individuals and Data Protection Officers; these include tools for enforcement and dynamic consent management. The right for individuals to

access their personal data from data controllers is a cornerstone of the EU Data Protection legal framework, but in reality there has been little consideration at the system design phase about how these rights can be effectively, safely, and conveniently exercised by data subjects.

The reality is that many people today do not know who has access to their personal information. Even if users can see their data, they may have no control over it; i.e. to remove / delete / amend what they deem inappropriate or false. A privacy transparency tool must incorporate dynamic consent management and be built into the architecture of any identity management system.

User-centric identity management, providing strong mutual authentication between data subjects and data controllers is a pre-requisite, however more research is needed into how personal data should be stored and structured by data controllers to maximise the transparency available to individuals, and to minimize the costs and burdens of fulfilling access requests. Increasing the depth and scope of the personal data available to data subjects online may increase privacy risks unless accompanied by a holistic approach to system security design. However there is virtually no literature directly addressing these topics.

**"Minimum disclosure" credential management**

Although theoretical approaches and some prototyping do exist, we are still far from deployment in practice through lack of common UI design and policy standards (See points 3.1.6and 3.1.7, above).

Basic cryptographic designs exist to build credentials that can be used to support user-centric, limited disclosure of identity information. These need to be complemented by suitable open standards and semantics that can be leveraged to create an ecosystem and a market that will justify the investment for developing necessary products.

A consequence is also that if minimum disclosure is 'per situation', then authentication requirements are also specific (and minimised) to the needs (and context) of what is being accessed.

**Privacy friendly biometrics– "One way" enrolment & usage protocols**

While a biometric process may not completely eliminate duplicate enrolments, they are, nonetheless, a continuous means for identification. 'Supervised' enrolment protocols may well be incorporated into identification and authentication systems, based on biometric processes. Carrying out cryptography separately from biometrics has the virtue that one is decomposing the solution into two simpler, well-established problem domains. However, owing to the inherently noisy nature of biometric templates, doing crypto and biometrics separately would appear to require using a central database of biometric templates if the design goal is unique enrolment of individuals, in order that matching can be done against previous enrolments. In summary, this refers to a system where you could capture a live biometric on someone, together with a hardware token, and without a central template database. It would be a breakthrough to have a practical design where it was not logically necessary to have database of templates in order to implement unique (i.e. non-duplicated) enrolment of individuals (in some application domain). When discussing privacy-friendly biometrics as a possible solution area, a clear distinction must be made between supervised biometrics (e.g. border-control) and unsupervised biometrics/registration (e.g. building-access using retina identification). The trust relationship between the stakeholder./.user and the registration source (e.g., government, bank, organisation) is a key consideration factor here.

# Usability

**User support and orientation**

The complexities of how security facilities and mechanisms are to operate are beyond the comprehension and capabilities of all but a handful of experts. Some form of automation, provided by helpful interfaces, tools and off-the-peg profiles, is needed that will allow the user to make sensible decisions to suit personal circumstances and preferences. But to make sensible decisions, even if only to select some typical, standard profile, there is still the need for awareness by the user of what is going on, what are the risks protected against, etc. Therefore, some awareness programme or Help facility should be available, providing a wide range of support and advice from the ICT naïve to the reckless know-all. This will require close cooperation between the technology designers and ergonomic and usability experts.

**Use of Services**

The user needs access to services that provide a proper mutual balance of transparency and accountability with respect to rights and duties: at present, a balance that appears in favour of the service provider. For example, <I accept> – click! In practice access is going to be much more complex and dynamic than is currently the case, and hence a framework is needed that will provide for the performance, in real time, of the agreed terms of the relationship between service and user (client). The user wants to be able to trust what is happening with (their) information, and how agreed duties of care are discharged, even though there will be discontinuities, change of device, change of location, etc.

**UI design according to privacy requirements**

There is currently a lack of research in user-interface design based on users' privacy requirements. Meaningful and understandable controls are required. Strong authentication, without the need for strong identification is one goal (i.e. non-declarative, strong authorisation). There also exists a need for tools to assess risk. For example, how do we know what is happening in a data controller? Could a PKI be implemented for a data controller?

It was noted that current policy statements from service providers are not designed to be understandable by the users, but to get access to their desired service or information, users accept, with a tick-in-the-box, privacy policies that may well not be in line with their needs.

Interoperability and consistency of privacy policies calls for tools and standards.

# Engineering and technology

**Technologies and Engineering to support multi-level security and assurance**

The underlying security technologies and techniques need to progress so that they keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment outlined above.

- Cryptography: fast, cheap, light, (low power, ease of use and support, etc.);
- Trusted execution (environment) – how else do we know that what is supposed to happen really does happen;
- Trustworthy functionality – SW and HW; how to design, produce, and assure trustworthy components, and how to build them into larger trusted entities and assemblages? This calls for tools (themselves trustworthy) and 'criteria' that will support the policy governance outlined above. The technology needs a platform-independent dimension to allow for interoperability of trusted entities – in addition to the security aspects of trustworthiness, we need to address the wider issues of quality and dependability;
- Measurement and metrics – related to the previous item – we need to be able to measure aspects of trustworthiness, and to articulate and quantify the dimensions and units; this is required in the wider field of assessment of trust/risk and security/vulnerability;
- Basic engineering: we need to weigh up the considerations of cost and economics, power and energy versus strength, performance and functionality;
- Education, Training, and Awareness: in addition to the general user help and support, above, there need to be standards for professional training and proficiency, and the tools and methodologies for the designers and engineers to build and maintain the future networks.

**Virtualisation**

As the physical boundaries dissolve and blur, new virtual separations and boundaries must still be established and maintained; virtualisation and the mapping of constructs to physical resources must be developed and extended. Compartmentalisation provides a means of isolating and protecting areas of trust, and controlling relationships with other areas. It also supports the simplification of complex structures into foreseeable, manageable components.

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 27 January 2010

# PART 4 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

**The need for the EC to fund the development of an electronic requirements management process and deliverables to support existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified model that also supports national and regional variations.**

**Such a process could also include new standards requirements and best practice recommendations as they become available.**

**The process and deliverables would reduce costs and duplication of effort across European organisations and remove the existing discriminatory barrier that all micro and SME face when attempting to create innovative solutions that satisfy legislative, standards and best practice for the European and global markets.**

# 1. The importance of codifying standards, laws and policy requirements electronically

The US National Institute of Standards and Technologies Computer security Division has 17 active Federal Information Processing Standards[1] (FIPS), and over a 100 active Special Publications[2] that all Federal Information Processing systems must comply with. These standards and special publications relate to information assurance risk management processes, identity management, cryptographic security standards, configuration of security hardware, business survivability, achieving high availability, auditing, physical access controls and other important subjects relating to information processing.

The NIST FIPS and SP documents are freely available to the public and can be used as a basis for creating IT processing systems by non US Federal organisations. This body of work represents many "best-practices" that could be adapted for use internationally and if adopted, would result in a more secure global IT infrastructure. Corresponding documents are known to exist for the UK and Europe.

The Payment Card Industry Data Security Standard[3] is an example of an industry standard that must be met by organizations that process card payments.

In addition to these information processing standards, there are a large number of national and international laws that a company is required to comply with. For example some international companies might have to simultaneously consider, the European Data Privacy Directive[4], the American Health Insurance Portability and Accountability Act (HIPAA) of 1996, US Communications Assistance for Law Enforcement Act, US Electronic Communications Privacy Act, the German Informational self-determination law, the Canadian Personal Information Protection and Electronic Documents Act and so on.

**It is exceedingly difficult for a new software project (such as an e-commerce web-site) to know that it has met these requirements.** This difficulty is compounded because the requirements are not readily defined in an exploitable format. There is currently no mechanism available for a new project to import all the legislative requirements and best practice recommendations on data privacy into a requirements management tool. Each project must individually identify, and read the relevant laws, manually extract the requirements (imperfectly), so that they can then begin to show traceability of requirements satisfaction down to the executable, test suite and business processes. These requirements will need to represented in open standards based formats so they can be imported by most of the project management and requirement management tools. For example the process should generate deliverables that can be imported by tools like Borland CalibreRM and IBM Rational DOORS and their open source equivalents.

**We note that many of the Think-Trust ideas implicitly require this type of deliverable but D3.1B does not explicitly propose it.**

For example section 4.4 of Deliverable 3.1B states: "Accountability is a research priority, as it creates the means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress." Section 4.2 of Deliverable 3.1B recommends "verification of conformance requirements". Section 4.3 of Deliverable 3.1B raises the question of supporting different legal domains that have different priorities stating that "Technology is needed to support this 'dynamic switch of security controls' based on legal and best practice policies".

**Clearly this can only be cost effectively achieved if the laws and legal policies requirements are electronically specified and can be traced through to the source code.**

If every large organisation must build a requirements document for themselves already, so they can be sure they satisfy their obligations under law, then it makes sense that this be done in an authoritative and comprehensive manner so that the singular effort can facilitate the creation of law abiding, secure IT systems by even the smallest micro innovative design company. This lack of co-ordination and unification within at least one set of design tools **discriminates heavily against smaller corporations and constitutes a serious barrier to the creation and dissemination of new solutions.**

---

[1] http://csrc.nist.gov/publications/PubsFIPS.html

[2] http://csrc.nist.gov/publications/PubsSPs.html

[3] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[4] http://en.wikipedia.org/wiki/Data_Protection_Directive

# 2. An example of how capturing the security requirements of other countries could help Think-Trust meet one of its identified objectives

We quote the following requirement stated in section 4.10 of T-T D3.1b:

> *"There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

In National Security Systems and US Federal IT Systems this subject is comprehensively addressed under what the US call an "Information Assurance Risk Management Framework". The principal goal of the US National Security Community Information Assurance (IA) risk management approach is to enhance the mission assurance posture of the US National Security Community by protecting its information assets. An IA Risk Management Program enables a US Federal Department, Agency, Bureau or Office to successfully assess IA risks arising from information systems, prioritize those risks, implement security controls to mitigate the risks and meet their information assurance priorities, assess the operational performance and effectiveness of those controls, and maintain the appropriate level of trust that enables the sharing of national security information with other enterprises. *For more information on the comprehensive American risk frameworks, see CNSS Policy No. 22, FIPS 199, FIPS 200, FIPS SP 800-53, CNSSI-1253 and FIPS SP 800-60 as starting points.*

This comprehensive framework attempts to ensure that the security controls applied to a particular information system are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

It would seem desirable to electronically encode the national requirements for the US, identify and electronically encode all equivalent efforts in the EU, and then create a unified model security model that draws out the common international requirements and create regional appendixes for localization efforts. This common framework would provide an excellent platform for enabling the global community to increase assurance of our common service and software infrastructures, while also reducing the cost of regional certification efforts when desired/required. **This could be a joint undertaking by the US and the EU.**

If we side step out of information assurance and consider the European Data Privacy Directive, this is an example of where Europe could "export" its enhanced social norms to be facilitate their adoption by US organisations seeking to improve their data privacy operations internally within the US and to ensure they are providing appropriate protection of the data they manage on European citizens and organisations.

# 3. Synaptic's recommendations to Think-Trust

**We argue that D3.1B should strongly point to the need for the codification of EU standards, policies, and laws in an electronic format that can be exploited by requirements management and reporting tools including:**

- Parallel deployment of laws, policies and security standards as electronically importable requirements that permit their ready adoption, integration and verifiable traceable compliance in existing and future systems. In this context, Systems includes business, software and hardware processes,

- Establishing a large scale project to identify the common themes and requirements of international laws, various national laws, policies and standards, and unifying those requirements in a single suite of electronic requirement documents, and then building annexes that outline the variations and additional requirements that must be met to satisfy any given jurisdiction or law. Priorities of requirements should be advised by Governments as part of a safe-harbour arrangement to protect organisations so long as they can show strong evidence of their progress towards obtaining full compliance of their systems in independent audits,

- Ensuring that the system of requirements is maintained real time, and safe-harbour provided to organisations who have shown compliance with electronic requirements if there is a gap between the occurrence of law on paper and the subsequent rendering of that law in electronic form,

**to enable organisations/corporations of all sizes (Micro, SME, large enterprise) to adopt and show compliance to regional and international norms and thereby provide appropriate confidentiality, integrity and availability of software systems for all stake holders. END**

## About Think Trust

Think-Trust (T-T) ( www.think-trust.eu/ ) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [5]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [6] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

## About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit. At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[7].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

---

[5] http://www.think-trust.eu/riseptis.html

[6] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[7] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Thursday, 28 January 2010

# PART 5 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

## The need to evaluate the effectiveness of data depersonalization techniques and it's impact on the community; and

## Measuring the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness so as to guide resource management and improve EU marketplace international competitiveness.

# 1. The need to evaluate the effectiveness of data depersonalization techniques and it's impact on the community

Pseudo-anonymity and true anonymity are core themes that run through the text of T-T D3.1b.

Of critical importance is establishing a comprehensive framework for measuring data depersonalization (also called data anonymisation in section 4.4 of T-T D3.1b), in all its forms, and then reviewing the effectiveness of existing and proposed techniques.

**Without an objective benchmark, how can the EU community be sure that privacy enhancing technologies are effective?**

For this reason, it is important to survey data depersonalization techniques currently used by the civilian industry and establish to what extent they are effective.

We need to assess the positive and negative impacts of the resale of this depersonalized data in the community.

**Most critically we need to study the way consumers of depersonalized data use the information and specifically evaluate if they are able to re-personalise the data** in meaningful ways that undermine the objectives of de-personalization. If the depersonalization techniques are not adequate to protect identity (before or after sale), we need to identify what techniques and what parameters are appropriate for commercial data depersonalization and what limitations must be placed on those who consume/use depersonalized data.

Synaptic argues that after adequate open international peer review, there is a need to enforce effective techniques and parameters across the entire life cycle of depersonalized data as Government policies. Furthermore, this review process should be continuous and accumulative so that new and improved data mining techniques, and adaptive behaviors of the data-consumers, can be monitored and compensated for.

Synaptic advanced these issues at the US National Cybersecurity Summit and consequently they were advanced to be included in the Summit's deliverable, the Summit Participants Idea Report. That Report has been used as input the US Administrations cybersecurity planning. See Appendix A1 for a short action plan as written up in the US Summit Participants Idea Report on these issues.

# 2. Measuring the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness

We quote the following requirement stated in section 4.10 of T-T D3.1b:

> *"There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

This raises the question: what is the impact of data breach to the individual?

The US have defined an extensive "Information Assurance Risk Management Framework" to assess IA risks arising from information systems, prioritize those risks, implement security controls to mitigate the risks and meet their information assurance priorities, assess the operational performance and effectiveness of those controls, and maintain the appropriate level of trust that enables the sharing of national security information with other enterprises. *For more information on the comprehensive American risk frameworks, see CNSS Policy No. 22, FIPS 199, FIPS 200, FIPS SP 800-53, CNSSI-1253 and FIPS SP 800-60 as starting points.*

This comprehensive framework attempts to ensure that the security controls applied to a particular information system are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

There are three potential impact levels: low, moderate, and high.

A fair amount of human judgement is required to correctly classify the potential impact levels to each risk.

For example, in US national security systems, the definition of low potential impact is: if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. (Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.) The potential impact is defined as High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

These frameworks are excellent and should be applauded, promoted and adapted so they are most suitable for wider adoption outside of US Federal Systems. This appears to Synaptic to be an area where EU and US can collaborate with mutual benefits.

**This said, and without detracting from the value of the existing work, we argue that insufficient data exists to enable an organisation to accurately establish the value of information loss to stake-holders, including customers and clients.** Without such information it is not possible to make an informed decision about the necessary level of security mechanisms required. Without this information, decisions are made on personal and subjective opinions which may not accurately reflect the perspective of the full stake-holder community. This is an area that can be improved with potentially great rewards for the global community.

Large scale field studies are required to establish the value of information loss with respect to different classes of data including financial, medical, intellectual property, relationship information and geolocation of time for different groups including Enterprises, SME, and individuals.

These studies must be considered in a global context. Simple services provided in one country (Such as web email services hosted by Google) may be used for sensitive purposes (such as communications between human rights activists) and have serious ramifications if security mechanisms fail.

These studies can be extended to assess the financial and emotional impact of down-time or availability of access to services[1]. For example how does a call center establish the financial impact on the wider community for a given average wait time of *x* minutes before reaching a human on the other end of the line? Is it appropriate to achieve 100% loading on call centers staff to maximize profits for share holders at the expense of people on the end of the line? **Can EU norms be set to ensure a level playing field inside EU and in a way that optimizes the overall efficiency and international competitiveness of the European marketplace?**

A greater understanding of the value of different types of information, as held by the different portions of the community, can inform those responsible for managing that information on behalf of others so that appropriate risk management strategies can be put in place. (See section A.7 of the Appendix in this document for more information on our proposal submitted to the US NITRD).

Synaptic advanced these issues at the US National Cybersecurity Summit and consequently they were advanced to be included in the Summit's deliverable, the Summit Participants Idea Report. That Report has been used as input the US Administrations cybersecurity planning. See Appendix A2 for a short action plan as written up in the US Summit Participants Idea Report on these issues.

---

[1] Modern risk assessment techniques such as those proposed in the paper by Aissa, Anis Ben, Abercrombie, R.K., Y., Sheldon, F.T. and Mili, Ali called "*Quantifying Security Threats and Their Impact: Theory and Practice*" published in Innovations in Systems and Software Engineering, Springer London, ISSN 1614-5046 (Print), ISSN 1614-5054 (Online) that takes into account all stake holders might be adapted to the task.

# 3. Synaptic's recommendations to Think-Trust

**We argue that D3.1B should strongly point to the need for the studying the effectiveness of existing data depersonalization techniques, to identity ways in which depersonalization may be being re-personalized by corporations, and to propose a framework for a) appropriate methods for data depersonalization by providers, b) guidelines and limitations on how depersonalized data can be used by its consumers to prevent re-personalization, c) continual monitoring and improvement.**

**We argue that D3.1B should strongly point to the need for the studying the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness as a deliverable that will feed into the assessment of appropriate risk management technologies and resource management for information processing systems.**

**See the two appendixes for further recommendations.**

**END**

# APPENDIX

## A1. Evaluating the effectiveness of data depersonalization techniques and it's impact on the community

**Author:** Benjamin GITTINS (Synaptic Laboratories Limited)

*Found in the "National Cyber Leap Year Summit 2009: Exploring Paths to New Cyber Security Paradigms Draft Report" ( http://www.co-ment.net/text/1451/ ) and published in official the "National Cyber Leap Year Summit 2009 Participants Idea's report" ( http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf)*

**Description -** Establish if data depersonalization techniques used by the civilian industry are effective and assess the impacts of re-sale of depersonalized data in the community. Study the way consumers of depersonalised data use the information. If the depersonalization techniques are not adequate to protect identity (before or after sale), identify what techniques and parameters are appropriate for commercial data depersonalization. After adequate peer review, enforce these techniques and parameters as Government policies.

**Inertia -** Commercial interests for selling data / Poor community-wide awareness of the risks associated with sale of personal data collected by organisations.

**Progress -** Several papers have identified that it is possible to identify the persons present in some depersonalized data released by large organisations.

**Jumpstart Activities -** Collect a large representative sample of commercial exchanged depersonalised data (find data sold by a large online commercial store, and a mobile phone provider selling location data), bring together experts in the field to evaluate how easy it is to re-personalise the data, bring together legal team to evaluate the implications of data that is not effectively disassociated from the user. Compile any changes required to law.

Action Plan - Identify the security and legal experts / acquire large representative data sets of the type of information sold / start a conference and advance it with funding.

**Who can help -** NITRD, US State Department, Electronic Freedom Foundation, Jeff Jonas of IBM, weak signal analysis, other published researchers in this field.

# A2. Measuring the wider impacts of unauthorised information disclosure

**Author:** Benjamin GITTINS (Synaptic Laboratories Limited)

*Found in the "National Cyber Leap Year Summit 2009: Exploring Paths to New Cyber Security Paradigms Draft Report" ( http://www.co-ment.net/text/1451/ ) and published in official the "National Cyber Leap Year Summit 2009 Participants Idea's report" ( http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf)*

**Description -** Methodologies for Evaluating appropriate security controls based on the confidentiality, integrity and availability of IT systems now exist. However insufficient information exists to allow an organisation to establish the value of information loss to stake-holders, including customers and clients. Without such information it is not possible to make an informed decision about the necessary level of security mechanisms required.

Large scale field studies are required to establish the value of information loss with respect to different classes of data including financial, medical, intellectual property, relationship information and geolocation of time for different groups including Enterprises, SME, and individuals. Such studies could be extended to assess the financial and emotional impact of down-time or availability of access to services.

A greater understanding of the value of information managed by others, and its management, by the stake holders can better inform organisations on how to manage their IT infrastructure and risks.

**Inertia -** Commercial interests for selling data / Commercial interests to maintain 'just-enough' security to protect against legal liability. There is little incentive for organisations to identify the true cost of security breaches against individuals.

**Progress -** Technologies exist which can be used to collect this information.

**Jumpstart Activities -** Identify the financial, social sciences, security and legal experts. Develop a set of questions to measure metrics on. Engage many universities and some organisations to perform surveys and collect the data. Process the data publish reports and set metrics for depersonalisation standards.

**Action Plan -** Identify interested financial, social sciences, security and legal experts. Develop action plan and secure funding. Perform studies in hospitals and other medical practices.

**Who can help -** NITRD, CyberSpace Sciences and Information Intelligence Research - ORNL - DoE, RTI International, Universities, EU Think Trust.

## About Think Trust

Think-Trust (T-T) ( www.think-trust.eu/ ) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [2]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [3] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

## About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit. At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[4].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

---

[2] http://www.think-trust.eu/riseptis.html

[3] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[4] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Friday, 29 January 2010

# PART 6 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

## Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimizing facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments;

## We recommend that a Global PET solution should be explicitly designed to pro-actively prevent abuse by Governments or Regions;

## and

## We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems.

# 1. Escrow and Data Retention

In section 4.4 on Accountability, the Think-Trust deliverable D3.1B discusses:

> **"Delegation, proxy, anonymity management"** and
> **"Anonymous/pseudonymous charging and payment systems".**

Section 4.4 also states:

> **"By partially moving system control towards establishing data either *a priori* or *a posteriori*, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows."**

Synaptic is concerned that Think-Trust may be proposing the design of Privacy Enhancing Technologies that:

- embeds global identity information with each "data flow" in a way that permits escrow functionality such that "data either *a priori* or *a posteriori*" can be recovered; and/or
- creation of systems that "mass archive" potentially interesting information in a way that permits the identity of the parties and the cleartext to be recovered either *a priori* or *a posteriori*.

**Synaptic strongly recommends that Privacy Enhancing Technologies should be explicitly rejected by Think-Trust when and if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments.**

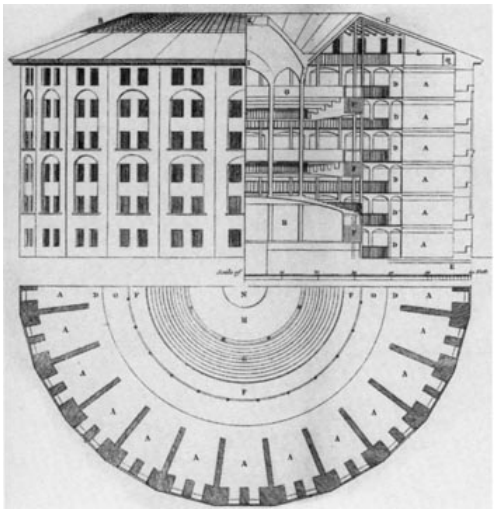
> "At a crypto conference when Clipper was hot, I was approached by Birgit Pfitzmann, a German cryptographer with a very compelling statement that moved me greatly. *'Brian, America is very fortunate, you have never had a truly evil Government. Perhaps corrupt, perhaps inept, but never truly evil. We in Europe have not been so fortunate. I trust the Government I have today, but I will not give it power over me that I would not trust in the hands of a future Government I would not trust.' And I agree with her.*"
> – Brian Snow, former Technical Director of the information assurance directorate of the NSA, 2006

*The Clipper Chip is a cryptographic device intended to protect private communications while at the same time permitting government agents to obtain the "keys" upon presentation of "legal authorization."*

If a Government is permitted the CAPABILITY to employ centralized escrow measures on all security systems in the name of "accountability" within its jurisdiction, this would fundamentally undermine trust and create the perception – if not the reality of – a panopticon, and open potential for real abuse of the captured and permanently archived data.

The concept of the original panopticon design (illustrated to the right for use as a prison) is to allow an observer to observe (-opticon) all (pan-) prisoners without the prisoners being able to tell whether they are being watched, thereby conveying what one architect has called the "sentiment of an invisible omniscience."

There is a real concern that all sensitive data might be *a priori* or *a posteriori* exposed in a way that the sending and receiving parties cannot ascertain, audit or control.



> *"Whoever is **uncertain if divergent kinds of behavior will be recorded at any time and this information will be stored permanently, used or passed on**, will try not to attract attention by these kinds of behavior. Whoever expects that e.g. the attendance of an assembly or the participation in a civic action group will be registered by the authorities and that this will probably cause risks, may probably abandon their corresponding fundamental rights (Art. 8, 9 GG). This would not only impact the individuals' chances for development but also the public interest because **self-determination** is a necessary condition for the functionality of a liberal democratic polity which is based on its citizens' ability to act and to participate."*
>
> *– from the German Federal Constitutional Court census judgment of 1983 as quoted in the article "Current Legal Issues on Video Surveillance" contributed to the SECURITY Congress 2000, Oct. 9-12, 2000 in Essen by Dr Thilo Weichert.*

**Synaptic asks how can Government controlled pseudo-anonymity protect the civilian from potential abuses within the current, or future Government?**

The paranoid members of our community would probably be correct in fearing that citizens using pseudo-anonymity would be flagging themselves for special attention by their secret Government security organisations.

It would be reasonable to assume that in many cases Government Security Organisations (under the flag of national security) would be able to monitor all Government 'certified secure' channels in exactly the same way, and with the same impunity and lack of external oversight, they are doing already over unsecured communication paths.

Of course if a Government chose to maintain escrow access to sensitive personal and corporate data then the question becomes one of security of the data thus obtained. Governments have a questionable record of holding secure their own records and systems, much less confidential data they accumulate on the general public.

**Furthermore, the complexities of international stability are increased as a result of potential international espionage, even between EU member states.**

See Part 3 of our input to the Think-Trust D3.1b consultation process for more information on the importance of end-to-end redundancy, no single points of potential failure and separation of powers.

# 2. The need for legalized interception systems to be cryptographically secure

According to a review by the well known American cryptographer Matt Blaze and 4 co-authors, a real problem that exists in the USA today is that the American wiretap protocols -- used in the most serious criminal investigations -- were apparently designed and deployed (and mandated in virtually every communications switch in the US) without first subjecting them to a meaningful security analysis.

According to Matt Blaze current US Legalised Interception systems were engineered to work well in the average case, but ignored the worst case of an adversary trying to create conditions unfavorable to the eavesdropper. And as the services for which these protocols are used have expanded, they've created a wider range of edge conditions, with more opportunities for manipulation and mischief.

See their paper, Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps[1] which examines the standard "lawful access" protocols used to deliver intercepted telephone (and some Internet) traffic to US law enforcement agencies.

**— It is conceivable that a similar situation exists in European States.**

**If wiretaping and escrow systems are going to be built, then we propose that they must be engineered at the same levels of auditability, robustness and security as National Security Systems and with the same accountability and privacy controls required in Enterprise systems by European Data Privacy Directives.**

[1] http://www.crypto.com/papers/calea-ccs2009.pdf

# 3. Current interception systems put the community at risk

We extensively quote an article by highly respected cryptographer Bruce Schneier published on CNN[2]:

> **U.S. enables Chinese hacking of Google**
> **January 23, 2010**
>
> Google made headlines when it went public with the fact that Chinese hackers had penetrated some of its services, such as Gmail, in a politically motivated attempt at intelligence gathering. The news here isn't that Chinese hackers engage in these activities or that their attempts are technically sophisticated -- we knew that already -- **it's that the U.S. government inadvertently aided the hackers**.
>
> In order to comply with government search warrants on user data, Google[3] created a backdoor access system into Gmail accounts. This feature is what the Chinese hackers exploited to gain access.
>
> Google's system isn't unique. Democratic governments around the world -- in Sweden[4], Canada[5] and the UK[6], for example -- are rushing to pass laws giving their police new powers of Internet surveillance, in many cases requiring communications system providers to redesign products and services they sell.
>
> Many are also passing data retention laws, forcing companies to retain information on their customers. In the U.S., the 1994 Communications Assistance for Law Enforcement Act required phone companies to facilitate FBI eavesdropping, and since 2001, the National Security Agency has built substantial eavesdropping systems with the help of those phone companies.
>
> Systems like these invite misuse: criminal appropriation, government abuse and stretching by everyone possible to apply to situations that are applicable only by the most tortuous logic. The FBI illegally wiretapped[7] the phones of Americans, often falsely invoking terrorism emergencies, 3,500 times between 2002 and 2006 without a warrant. Internet surveillance and control will be no different.
> …
> China's hackers subverted the access system Google put in place to comply with U.S. intercept orders. **Why does anyone think criminals won't be able to use the same system** to steal bank account and credit card information, use it to launch other attacks or turn it into a massive spam-sending network? Why does anyone think that only authorized law enforcement can mine collected Internet data or eavesdrop on phone and IM conversations?
> ...
> These risks are not merely theoretical. After September 11, the NSA built a surveillance infrastructure to eavesdrop on telephone calls and e-mails within the U.S. **Although procedural rules stated that only non-Americans and international phone calls were to be listened to, actual practice didn't match those rules.** NSA analysts collected[8] more data than they were authorized to and used the system to spy on wives, girlfriends and notables such as President Clinton[9].
>
> But that's not the most serious misuse of a telecommunications surveillance infrastructure. In Greece, between June 2004 and March 2005, someone wiretapped more than 100 cell phones belonging to members of the Greek government: the prime minister and the ministers of defense, foreign affairs and justice.
>
> Ericsson built this wiretapping capability into Vodafone's products and enabled it only for governments that requested it. Greece wasn't one of those governments, but someone still unknown -- A rival political party? Organized crime? Foreign intelligence? -- figured out how to surreptitiously turn the feature on.

---

[2] http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html

[3] http://topics.edition.cnn.com/topics/Google_Inc

[4] http://www.thelocal.se/12334/20080610/

[5] http://www.canada.com/Technology/Feds+give+cops+Internet+snooping+powers/1706191/story.html

[6] http://www.theregister.co.uk/2008/05/20/central_government_database_proposed/

[7] http://www.nytimes.com/2010/01/21/us/21fbi.html

[8] http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=1

[9] http://www.wired.com/threatlevel/2009/06/pinwale

> **And surveillance infrastructure can be exported, which also aids totalitarianism around the world.** Western companies[10] like Siemens and Nokia built Iran's surveillance. U.S. companies helped[11] build China's electronic police state. Just last year, Twitter's anonymity saved the lives of Iranian dissidents, anonymity that many governments want to eliminate.
>
> In the aftermath of Google's announcement, some members of Congress are reviving a bill[12] banning U.S. tech companies from working with governments that digitally spy on their citizens. Presumably, those legislators don't understand that their own government is on the list.
>
> The problem is that such control makes us all less safe. Whether the eavesdroppers are the good guys or the bad guys, these systems put us all at greater risk. Communications systems that have no inherent eavesdropping capabilities are more secure than systems with those capabilities built in. And it's bad civic hygiene to build technologies that could someday be used to facilitate a police state.

With regard to the question posed by Think-Trust in section 4.10 of T-T D3.1b:

> *"Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

Synaptic rhetorically asks: How can we measure the damage of data breaches to human rights activists in China?

# 4. Equal Accountability Inside Security Systems

It is not sufficient to say, "Enterprises must behave in this proper way by law", and then not impose functionally equivalent requirements on ALL branches of Government.

Historically Accountability, Transparency, Systems of Checks and Balances, and Separation of Powers have been the founding principles of democratic institutions. The Spirit of Laws (French: L'esprit des lois) is a treatise on political theory **first published anonymously** by Charles de Secondat, Baron de Montesquieu[13] in 1748 that covers a wide range of topics in politics, the law, sociology, and anthropology. In this political treatise Montesquieu advocates constitutionalism and the separation of powers, the preservation of civil liberties and the rule of law, and the idea that political and legal institutions ought to reflect the social and geographical character of each particular community. All these fundamental principles remain as valid today as they did in 1748.

It is these principles that has led to the design of Governments that permit individual citizens of limited means to have some level of trust in the integrity of their Governing system.

The **separation of powers**, **checks-and-balances and the rule of law** should not be an option but a legal requirement in cyber-security systems or electronic law-enforcement activities particularly as it is clearly acknowledged that cyberspace touches every citizen.

Furthermore, it is not sufficient to say that security mechanisms must be in place by law for one group, if some of the mechanisms that are put in place effectively shift liability away from the largest stake holder, or make that large stake holder less accountable than others. This practice is already far to common:

> "The conventional wisdom is that security priorities should be set by risk analysis. However, reality is subtly different: many computer security systems are at least as much about shedding liability as about minimising risk. Banks use computer security mechanisms to transfer liability to their customers; companies use them to transfer liability to their insurers, or (via the public prosecutor) to the taxpayer; and they are also used to shift the blame to other departments ('we did everything that GCHQ told us to')."
> -- Ross J Anderson[14], UK Cryptographer,

---

[10] http://news.bbc.co.uk/2/hi/technology/8112550.stm

[11] http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print

[12] http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/16/BU151BIO84.DTL

[13] http://en.wikipedia.org/wiki/Charles_de_Secondat,_Baron_de_Montesquieu

[14] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.27.4524

**Synaptic recommends that a research subject would be to consider in what way legal policies can guide the design and implementation of all information processing and all monitoring systems so that all stake holders can be held externally accountable without exception.**

For example laws that:

- stipulate that information processing and monitoring systems must hold ALL stake-holders equally accountable to each other;
- require information processing and monitoring systems to protect the legitimate interest of all stake-holders (and not just the interest of the share-holders);
- require that a stake holder must be readily informed of all actions (including security actions/investigations) taken against their personal sensitive data (even if this might be delayed by some small fixed amount of time, such as maximum 6 to 12 months) - including how this information will be used, and how long it will be retained, and how they can seek redress; and
- require that accountability of internationally deployed information processing and monitoring systems must not be shifted completely away from the users jurisdiction and also must not be constrained to any singular national body.

To provide further support to this argument, let us first consider the Elysée Scandal—named after the palace where the late President Francois Mitterrand set up an undercover listening room. Mitterrand's operatives tapped the calls of his political enemies: lawyers, businessmen, journalists, and even the actress and Chanel model Carole Bouquet. This took place in the mid-1980s but only surfaced recently, and 12 conspirators were brought to trial[15]. **What's interesting—and disturbing—about the Elysée Scandal is that at the time, French authorities had justified the surveillance as a necessary tool to fight terrorism.** This type of action should be detectable near real-time, not several years later after the event, after the damage has been done.

To quote the Wired magazine article that goes into more detail on the illegal wiretapping by the FBI:

> An internal audit found that the (US) FBI broke the law thousands of times when requesting American' pone records using fake emergency letters that were never followed up on with true subpoenas – even though top officials knew the practice was illegal, according to The Washington Post.
> …
> "What is new in the Post's reporting today is that it was FBI supervisors and senior officials who were abusing the system," said Greg Nojeim, a lawyer at the Center for Democracy and Technology.
>
> "The FBI has been assuring us for years that the abuses of the Patriot Act could be cured by more layers of internal review, but now we learn that the supervisors themselves were abusing the process," Nojeim said. **"When people are under pressure, internal review is not enough, there needs to be external oversight, and the best way to do that is to have a judge look at the situation."**
>
> - Ryan Singel, Wired Magazine, Jan 19, 2010

**Synaptic argues that Europe's exceptional rules for enforcing data privacy and accountability at the commercial level should also be applied in all information processing systems, including monitoring systems, created for Governments.**

**Again we argue that accountability of such systems MUST transcend a singular national body, because national Judges are likely to feel the same National pressures that the national security organisations feel.**

[15] http://www.time.com/time/magazine/article/0,9171,1027463,00.html

# 5. The research agendas and systems designed by the EU should be considered for how they influence other nations

The United States and the European Union both proclaim themselves as pillars of democracy to the international community.

As standards of democracy, how they behave has some influence on the behavior of all other Nations.

The research agendas, and the Identity and IT systems proposed by the European Union will also set the next "high water mark" for the behavior of other Governments internationally, particularly as we now live in a globally interdependent and interconnected world village.

**The expectations of the common person in the global community will be influenced by the research and development agendas, and security systems built by Europe.**

We quote Brian Gladman, a respected cryptographer who has extensive experience working in the UK MoD[16]:

> "Although many democratic countries have institutions and approaches that can significantly limit and control government abuse of key escrow capabilities, **this is not more generally true and in many countries these would undoubtedly be used as a means of oppression.** If democratic countries implement such measures they then have no moral or ethical basis on which to deny these facilities to governments that will use them against their own citizens.
>
> **The ability of encryption to allow people to interact with each other on a global scale without fear of oppression by their governments is just about the most potent capability mankind has had for advancing democracy and human freedom on a global scale.** I consider it a tragedy that the United States in particular, with its strong tradition of promoting democracy and human freedom, should be seeking to deny this technology to those who most need it."

**END**

[16] http://gladman.plushost.co.uk/oldsite/career/index.php

# 6. Synaptic's recommendations to Think-Trust

Synaptic is concerned that Think-Trust may be proposing or be thought to be proposing the design of Privacy Enhancing Technologies that could be adapted to operate as centralized monitoring systems.

Synaptic strongly recommends D3.1B explicitly rejected Privacy Enhancing Technologies when they could act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments.

Synaptic argues that if D3.1B supports the design of wiretaping and escrow systems then Think-Trust should assert that they must be engineered at the same levels of auditability, robustness and security as National Security Systems and with the same accountability and privacy controls required in Enterprise systems by European Data Privacy Directives to protect the citizen and to free the international community from the existing risks of uncontrolled politically motivated abuse and to prevent the growth of totalitarian states.

Furthermore, synaptic strongly recommends D3.1B explicitly recommend that existing "legalized interception" systems to be studied for their cryptographic security and if they must continue recommend that they:

- have inbuilt end-to-end redundancy;
- are free of single points of potential catastrophic failure;
- distribute trust and separate powers management across multiple autonomous security authorities and nation states;
- permit international external oversight to identify and a legal framework that ensures abuses are corrected and agents held accountable.

**Synaptic recommends that a research subject would be to consider in what way legal policies can guide the design and implementation of ALL information technology security systems that hold all stake holders externally accountable without exception.**

For example laws that:

- stipulate that information processing and monitoring systems must hold ALL stake-holders equally accountable to each other;
- require information processing and monitoring systems to protect the legitimate interest of all stake-holders (and not just the interest of the share-holders);
- require that a stake holder must be readily informed of all actions (including security actions/investigations) taken against their personal sensitive data (even if this might be delayed by some small fixed amount of time, such as maximum 6 to 12 months) - including how this information will be used, and how long it will be retained, and how they can seek redress; and
- require that accountability of internationally deployed information processing and monitoring systems must not be shifted completely away from the users jurisdiction and also must not be constrained to any singular national body.

## About Think-Trust

Think-Trust (T-T) ( www.think-trust.eu/ ) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [17]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [18] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

## About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit. At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[19].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

---

[17] http://www.think-trust.eu/riseptis.html

[18] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[19] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

SYNAPTIC LABORATORIES LTD.

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

# Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

## PART 1 - Covernote

In 2009-2010 the European Network and Information Security Agency (ENISA) http://www.enisa.europa.eu/ made a call for Scenario Proposals on Emerging and Future Risks.

One proposal was then selected for study in 2010 in the area of Trust and Privacy. In this area ENISA was looking for proposals to identify major risks in the area of trust, security and privacy posed by new and emerging technologies and applications. ENISA restricted scenario proposals from including proprietary technologies. Synaptic participated in this Call with a scenario focused on the risks associated with the global dependency upon Public Key Cryptography (PKC) and Public Key Infrastructure (PKI). Synaptic proposal, as included in this document, satisfied all ENISA's submission requirements and was shortlisted by ENISA.

We are placing a copy of the submission online for the benefit of those who may have an interest in PKC dependent systems (SSL/TLS, SSH, SSL-VPN etc) and PKI. The writing style selected for the submission was chosen to hopefully make the issues more accessible to a wider, non-technical audience.

According to Article 3(a) of Regulation 2004/460, ENISA fulfils the task of collecting appropriate information in order to analyse current and emerging risks. It concentrates on risks at the European level, which could produce an impact on the resilience and the availability of electronic communications networks as well as on the availability, integrity and confidentiality of the information accessed and transmitted through them. ENISA provides the results of the analysis to Member States, the Commission and other stakeholders.

Synaptic originally submitted to ENISA a long version of our scenario, totalling some 56 pages with citations. This had to be reduced to a 3 page submission, to satisfy the ENISA guidelines. An anonymous version of the 3 page submission entitled: "*The risks of continued EU dependency on PKI and PKC*" was eventually reviewed by members of the ENISA Permanent Stakeholders Group.

In this web article the 3 page version (which appears below before the main document) can be considered as an executive summary of the longer document, which is entitled: "*The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers*."

The 56 page submission provides a scenario on three distinct stages in the life of "John Smith", a hypothetical UK identity management security expert working in the international Aerospace and Defence sector. John's eyes and thoughts provide us an opportunity to explore a series of events in a way that sheds insight into the underlying technical issues facing the European (and at times global) community.

The first stage is set in the present, the second stage in 5 years, and we show how decisions made in stages one and two can extrapolate out in a third stage set in 9 years. The submission then goes on to outline the rationale and significance of our proposed scenario including information on current and emerging US and EU research and development agendas.

The submission ends with a section outlining the empowering benefits to the EU (global) community of a comprehensive risk management report on PKI and an easy-reference table of the 90 different threats and issues under 8 headings identified within the submission. Extensive citations are embedded as footnotes throughout the long version document.

Synaptic has been actively researching and designing cybersecurity solutions to address many of the risks and issues identified in this ENISA submission. Six Synaptic proposals have been accepted and advanced by the US National NITRD Cybersecurity Summit (August 2009). Papers on the Synaptic proposals will be presented at the Cyber Security and Information Intelligence Research Workshop http://www.csiir.ornl.gov/csiirw/ in April 2010 and at the IEEE Key Management Summit http://2010.keymanagementsummit.org/ in May 2010.

We trust that you find our submission to ENISA to be of value in your own risk management processes.

We welcome any comments on this ENISA submission and any enquiries about our proposals to protect PKC/PKI from the identified threats.

Benjamin Gittins and Ronald Kelson

SYNAPTIC LABORATORIES LTD.

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

# Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

## PART 2 -

## 3 Page (Executive Summary) Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

The risks of continued EU dependency on PKI and PKC.

# Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

1. **Working Title:**

The risks of continued EU dependency on PKI and PKC.

***(Original title:***

*The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.)*

**2. Stakeholder Group:**

Industry

**3. Impact Area:**

Trust and Privacy

**4. Target audience:**

All stake holders in public key cryptography (PKC) and public key infrastructure (PKI) including User Groups, System Administrators, Certificate Authorities, Critical Infrastructure Projects (CIP), Legislators, European Commission, Research Community, Co-ordination Action programs, National Security Agencies.

**5. Brief outline of proposed scenario:**

Efficiencies demand greater interconnectivity in all (inter)national (PKI dependent) ICT systems. By 2015 single point of trust weaknesses in PKI are exploited. Cyberfraud now >1,000 BEuro annually. An arms race ignites around quantum cryptanalysis. With mounting PKI failures and no PKI succession planning, the EU Internal market is destabilised as public confidence in eCommerce and eGov plummets. More laws demand the use of PKI dependent biometrics. Countries trade biometrics and increase citizen surveillance.

*Note: Citations and further technical references are available in our 56 page supporting document (found in part 3)*

**6. Rationale / Significance of proposed scenario**

The problems with PKC and PKI are « *understood as issues already visible as possible future risks to network and information security* » and present a « *significant risk of undermining the smooth functioning of the Internal Markets* ». Below we outline how our scenario has « *security problems already identified as global issues* » and that « *there is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues* ». Critically, international co-operation is required for **PKI Succession Planning** to prevent destabilisation of the Internal Market, prevent market fragmentation, and generally to protect EU interests. **Today's PKI architecture has already been found wanting** and, according to unchallenged expert opinions published in documents generated by U.S. Cyber Security Initiatives, today's PKI is also considered a significant barrier to the universal adoption of cryptography which is now believed necessary to increase cybersecurity and mitigate fraud and identity theft. **There is an increased threat** as a consequence of emerging global tensions and the escalation in the development of cyber war capabilities resulting in an increased sophistication of the perpetrators, whether they are nation states or individuals. There are no super powers in cyber space, with modern technology and readily available hacking tools every citizen is powerful. **There is increased criticality** because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cybersecurity.

**Global single point of trust failures** exist in the architecture of the civilian PKI which enables any of the 20+ PKI Root Certificate Authorities to generate malicious certificates against any website address (based on the results of the MD5 Rogue Certificate Authority Attack). Today approximately 86% of fraud happens by management at a level against their own organisations. This is significant given that current PKI architecture is vulnerable to insider attackers. **The Internet is becoming increasingly Militarised by Governments.** The U.S. Air Force is advocating Cyber War. The U.S. has already conducted cyberwar in IRAQ with attacks that exploited the mobile phone network. **Weakness in PKI and PKC are likely to be exploited during cyberwar.**

The United States captures the biometrics of everyone entering their country. **Biometrics are already being traded internationally by the United States and other countries.** Biometrics will be increasingly combined with CCTV systems by law-enforcement agencies, effectively resulting in a **civilian panopticon**. Biometric data does not change significantly over the life time of an individual, however ECRYPT has small confidence in existing algorithms and key lengths beyond ten years, particularly for asymmetric algorithms (ECC, RSA, D&H) that protects biometrics. Archived biometric data could be widely exploited in the medium term. Increased risks typically lead to increased monitoring. **Comprehensive Internet surveillance would complete the civilian panopticon vision.**

**The RSA algorithm currently protects a billion applications.** PKI currently protects transactions worth trillions and investments worth tens of billions. With the massive momentum built up around the deployment of the 20th century security solutions using PKI, at-risk PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU (30 year operational life). Projects using PKI (or likely to use PKI) include (international, national and cross Government) ID initiatives including (eGovernment, UK NIS, e-Passports, FP6 STORK), Aerospace (SESARJU, Galileo) and other Government projects (CIPHER Project, UK ICT Strategy). In fact most Government and Civilian ICT systems critically rely on at risk PKI for security. **ECRYPT advise that they have little confidence in PKC (RSA, ECC) 10 years into the future.** The EU, US, and China Governments are funding research into code breaking quantum computers. To quote Prof. Seth Lloyd: "*The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.*" If just one (open or closed) quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. **There will be significant instability and liability shifting if this happens.**

US NIST has stated "*that in the light of quantum computing Cryptographic Key Management system designers MUST look at means other than using public key-based key management systems*", so that these systems can achieve "*resilience against quantum computing attacks*" (2009). There is new legislation being rapidly advanced in the USA today that would require the US NIST to lead the USA's international cybersecurity standards. New Identity Management, Key Management and cyberspace security standards may become weapons of coercion and not tools of global social empowerment for the 98% of the world's population that is not .gov, or .mil. Without international participation at the highest level, without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community.

SECOQC advises that current QKD networks are not suitable for use as large scale public networks such as the Internet. An attack recently eavesdropped 100% of a quantum cryptographic key due to weakness due to a photon detector vulnerability in modern QKD deployments. **This leaves only symmetric key technologies such as AES-256.**

**7. Benefits**

**THE EU COMMUNITY IS MARGINALLY SECURE TODAY – THE EU COMMUNITY IS TOTALLY UNPREPARED FOR THE FUTURE COMPUTING TECHNOLOGIES THAT IT IS DEVELOPING**

**Current and immediate future benefits (Public Key Infrastructure & Single point of trust failure)**

1. The report would provide an **authoritative, independent establishment and confirmation of the known weaknesses of PKI**. It would **highlight the unacceptable risks and ramifications of relying on security systems with system wide single-point-of-trust failures** that can negatively effect, and potentially destabilise, the entire EU community.
2. The report would **mitigate continued non-action by calculating and articulating the risks and potential negative impacts** from the loss of security and privacy, and the roll-on negative economic impact to EU Nations and stake-holders as a result of not immediately addressing the known weaknesses posed by PKI.
3. Once we are able to consider **the mean failure cost for each stakeholder** (which is the cost we expect to incur as a result of the lack of security), this loss **can be balanced against the cost of improving system security**. In this way a well-formed risk assessment report can provide an estimate of an appropriate amount to spend to address the known threats.
4. A risk management study **would support the existing EU calls (FP6 SecureIST) for the development of a universally acceptable hardened information technology infrastructure** that can provide MEDIUM to LONG-TERM assurances (50-to-100 years).
5. The outcome of such a study by ENISA on PKI **would feed into the Unified Identity Framework proposed by the RISEPTIS, and influence the design of security mechanisms in the €2.1 Billion SESARJU development efforts** and could potentially influence every segment of the European and the electronically connected Global community.
6. The ensuing benefits from a report that **instigates change in the EU Community includes a vastly improved ICT security infrastructure for future** sensitive and valuable computer applications, systems with higher availability, greater survivability from targeted attacks, improved stability during periods of aggressive behaviour by any nation providing a certificate authority. That is, ICT systems implemented with adequate levels of information assurance reduce their vulnerability to cyber attack and do not promote cyber war escalation. Consequently, **there will be less dependence on invasive surveillance and development of cyber-attack capabilities as deterrents.**

**Short-Medium Future benefits (Public Key encryption & Quantum Computers)**

7. The additional benefits from a report which instigates change in the EU community with respect to quantum computer attacks is:
   a. **a significant reduction in the amount of intellectual property/sensitive personal data that will be at risk of exposure,**
   b. **a reduction in the severity of ICT exposure to real-time attacks against access control systems,**
   c. **the avoidance of reworking expensive EU funded critical infrastructure projects from known anticipated attacks, and**
   d. **improved design and reduced operational costs** by avoiding rip-and-rapidly-replace scenarios that would otherwise occur by non-action today.

With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively effect the data security of every European citizen, or to be used as an ICT weapon to attack other countries.

We are not suggesting that the fundamental research into quantum computing should be reduced, or slowed, particularly as this is an internationally competitive research agenda which may offer other non-military benefits. What we are arguing is that there needs to be a focussed PKI risks/threats/costs/benefits study to inform decision makers and lead to adequate guidelines within EU funded research and development programs to address the known risks. By way of example, the previous EU call for 50-to-100 year security (by FP6 SecurIST) was ignored and utterly ineffective in inducing change of behaviour within any segment of the EU community. To our mind it is incomprehensible that the EU has not funded, at least to an equivalent level, the RESEARCH, DESIGN, DEVELOPMENT and DEPLOYMENT of appropriate low-risk countermeasures at the READY to ensure the global community can protect against the negative side-effects of the EU research initiatives in quantum computing. It will take major systems such as EMVCo more than ten years to migrate to a new security paradigm, when one becomes available! The lack of redundancy, distributed trust and resilience in PKI infrastructures are major risks that are compounded by the code breaking quantum threat.

SYNAPTIC LABORATORIES LTD.

**Ronald Kelson**
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

**Benjamin Gittins**
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

**Synaptic Laboratories Ltd.**
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Wednesday, 31 March 2010

# Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks

## PART 3 -

## Full 56 Page Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.

# Submission to ENISA's Call for Scenario Proposals on Emerging and Future Risks

## 1. Working Title

The risks to current, emerging and, future technologies which rely on Government approved standards-based public key technologies with their known risks of catastrophic failure and potential to create cyber war, caused by the presence of multiple existing single points of potential trust failure, whereby one player can compromise the entire global system and the known future risks from code breaking quantum computers.

## 2. Stakeholder Group

Industry

## 3. Impact Area

Trust and Privacy

## 4. Target audience

Legislators, European Commission, Research Community, Coordination Action programs.

## 5. Brief outline of proposed scenario: The next 9 years in the life of a security expert

### 5.0 Executive Summary

Our message is simple:

1. Today, PKI protects transactions worth trillions and investments worth tens of billions. Almost the entire globe is betting the whole shop on PKI; [PKI-001]
2. PKI is a brittle single layer of defence with many known complex problems and limitations; [PKI-002]
3. The global cryptographic community knows that Government standards based PKI could catastrophically fail within ten years, but in spite of this risk and the many single points of potential critical failure, the EU continues massive PKI rollouts even in long term (10-30+ year) critical infrastructure projects; [PKI-003]
4. The community has not yet fully comprehended the extent of PKI dependency, the range of risks and threats, and the complexity of the international issues. This failure results in the continued dependency on PKI and the lack of corrective action which in turn threatens core EU principles, EU Market future, and EU stability; [PKI-004]
5. Preventing cyberwar and cyberfraud (valued at 1,000 billion USD per annum by the FBI) are now at the top of the agenda, and the USA has already started a major project to look for improvements and alternatives to PKI as part of its massive cybersecurity initiatives. [PKI-005] The issue of finding a replacement to PKI affects all of Europe. [PKI-006] A PKI replacement must be balanced so that it takes into account the legitimate interests of all stake holders and does not favour the (political, commercial, military) interests of any one nation or group. [PKI-007] A PKI replacement must be internationally acceptable to enable inter-operability of future global ICT systems. [PKI-008] For these reasons the study of the problem/s in PKI, and the negotiation of the requirements for an international PKI replacement, is beyond the scope of any one nation or organisation or major project such as SESARJU. It demands and deserves the full attention of the EU.
6. A risk assessment study is required to survey the known PKI issues and evaluate their potential impact on stakeholders in the EU community. Short term, mid term and long-term technical, research and policy risk treatments need to be proposed to ensure that current security deployments are bolstered and future security deployments enhance the European agenda rather than further jeopardise it.

In this section we present a scenario that addresses the requirements identified as relevant to ENISA[1]. Our multi-stage scenario is set over 9 years which «*analyses Current and emerging risks*» from the use of public key cryptography (PKC) and public key infrastructure (PKI) that:

1. Are « *understood as issues already visible as possible future risks to network and information security* »; and
2. Present a «*significant risk of undermining the smooth functioning of the Internal Markets*»

This scenario highlights how the PKI « *security problems identified are a global issue* » and that « t*here is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues* » to prevent market fragmentation.

We have set the future scenario over a period of 9 years to demonstrate how decisions taken, or indeed not taken, in the present, could have an exponential impact at a later date. The entire scenario is supported with extensive citations. We identify 90 different issues in 8 subjects. We cross reference these 90 different issues as they occur in the text using [square brackets]. These issues are listed in tabular form at the back of the document for ease of reference.

Our scenario highlights the growing massive global reliance upon public key cryptography in an array of critical applications. In fact the RSA algorithm is now claimed by RSA Security to be deployed in MORE than one billion applications world wide. The rate and range of deployments in both Government and commercial applications continues to build momentum. This continues in spite of the known, complex and potentially catastrophic risks and limitations. [PKI-009] When this momentum and complexity is considered in the context of the constraints caused by the current harsh economic times, it is obvious that it is not economically viable for a security company to research, develop and trial new solutions, even to protect against potentially catastrophic known risks, unless there is already an identified buyer. [PKI-010] For the same compelling reasons, the buyers similarly do not want to fund this type of project, particularly in the absence of clear leadership from Government and industry concerning the critical issues of interoperability and standards compliance [PKI-011]. Therefore there are multiple reasons why an EC level approach must be taken to the study of the PKI issues.

**Today's PKI architecture has been found wanting**[2] and, according to unchallenged expert opinions published in documents generated by U.S. Cyber Security Initiatives, today's PKI is also considered a significant barrier to the universal adoption of cryptography which is now believed necessary to increase cybersecurity and prevent fraud and identity theft.

**There is an increased threat** as a consequence of emerging global tensions and the escalation in the development of cyber war capabilities resulting in an increased sophistication of the perpetrators, whether they are nation states or individuals. There are no super powers in cyber space, with modern technology and more readily available hacking tools every citizen can be a super power.

**There is increased criticality** because the emergence of the Internet has shifted more economic and social activity online, making security virtually synonymous with cyber security.

**There is increased vulnerability** because emerging computing paradigms such as networking, distributed computing, and mobile/pervasive computing open wide security gaps that are hard to control.

Our scenario highlights how the lack of adequate research and analysis on these known risks can trigger a chain of side-stepping and liability shifting [PKI-012]. Ultimately, the known risks we describe apply to (practically) all ICT security systems, and some were already being described as a "*nightmare*" as early as 2004[3]. There exists the potential for countless amounts of past and present secure data being exposed and a vast array of critical systems put at operational risk [PKE-001].

---

[1] Regulation (EC) no 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (text with EEA relevance). In Official Journal L 077 (13 March 2004), pp. 0001 – 0011. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[2] P. Gutmann. *Everything you Never Wanted to Know about PKI but were Forced to Find Out*. Available at http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf

[3] Buchmann, J., Coronado, C., Doring, M., Engelbert, D., Ludwig, C., Overbeck, R., Schmidt, A., Vollmer, U., and Weinmann, R.-P. *Post-quantum signatures*. Report 2004/297, Cryptology ePrint Archive, October 2004. Available at http://eprint.iacr.org/2004/297

In the United States the National Institute of Standards and Technology (NIST) has already placed cryptographic key management firmly on the US and future international cybersecurity agenda (see section 6.4.3 below) [PKI-005]. NIST has already instigated a project to begin to address the problems, with a call for designers to look at new and different solutions that do not use public key cryptography [PKE-002]. Europe must co-ordinate with the US efforts or, as we will show, massive fractures in the international markets can occur [PKI-013].

We will highlight in our scenario the known security problems/risks/threats that exist as a result of this dependency on public key cryptography, and discuss the impact on current, emerging and future technologies and how their reliance on PKI can negatively effect the global community. We will touch on the complex issues of international identity management, biometrics and the use of PKI as a core enabling technology in these applications.

**We also show how the study of PKI can be applied constructively to address and resolve the risks whereby many countries seek to be a single point of control over all data exchanged** [SPOTF-001], [SPOTF-002]**, including data of citizens from other countries, that falls into its possession, without any international distribution of trust or resilience.** A new model of international distributed and shared trust with redundancy can be evolved that helps to remove the multiple single points of control and potential catastrophic failure that exist in many of our IT systems today and that in many cases can be exploited today against a citizen or to wage cyber war.

Our scenario focuses on three distinct stages in the life of "John Smith", a hypothetical UK identity management security expert working in the international Aerospace and Defence sector. John's eyes and thoughts provide us an opportunity to explore a series of events in a way that sheds insight into the underlying technical issues facing the European (and at times Global) community. The first stage is set in the present, the second stage in 5 years, and we show how decisions made in stages one and two can extrapolate out in a third stage set in 9 years.

This is a possible scenario of the future that can be avoided if action is taken now.

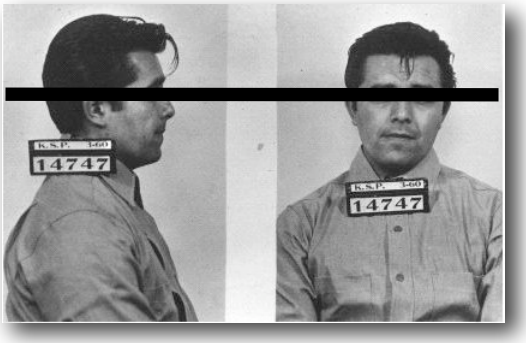
The EC should, in the near term, perform a comprehensive cost/benefit analysis, including the immediate, mid term and long term risks arising from the use of standards based public key cryptography in cybersecurity. This would be invaluable data to inform current and future large EU projects. It should clarify and quantify the risks, it should outline a preferred development path forward, and it should make recommendations on the preferred mechanisms, process and European representative body to lead the necessary international co-operation effort. This effort would be timely, as the USA has already rapidly advanced new draft Federal Legislation that will require the US NIST to lead the USA's international efforts and activities towards creating new international cybersecurity standards.

## 5.1 Scenario: 2010 (Current Risks)

John, a cryptographic and identity management expert of 30 years of age, is waiting in a chair at the National Identity Service (NIS) customer centre located at London City Airport. Today John will be applying for a UK National Identity Card (NIC) and updating his ICAO MRTD e-Passport. John, like most people, is feeling a little apprehensive, about what he is about to permit to take place.

John's passport will expire in about two years however, he has been told that it would be *highly desirable* if he took the opportunity to have a biometric passport ready for his new aerospace security job at Thales. John has recently applied for the position at Thales and was advised he will be given the job on the condition of his identity credentials and background security check passing. John has applied to work on the Single European Sky ATM Research (SESARJU) project during its €2.1 billion development phase. John has been short-listed for the position due to his experience which includes working on the aerospace and defence Transglobal Secure Collaboration Program (TSCP) identity management project[4].

Today the NIS will capture and permanently archive John's biometric data including 10 fingerprints, a photo of his face from the front and the side, and his signature. John knows this is exactly the set of biometrics that they capture when enrolling convicted criminals into prison [BIO-001], which makes him wonder if he has just enrolled himself into some similar controlled environment for non-law breaking citizens? [BIO-002] *(Image to right is public domain)*




[4] http://www.tscp.org/

Like many people, it is not just the initial discomfort in the *process* of capturing of his biometrics and its similarities with the criminal justice process that concern John – it's also the many risks associated with what can happen with his biometrics *after* his details are captured.

In particular, John understands that access to his biometrics will be controlled using public key cryptography. John has closely followed the most recent US cryptographic key management initiatives, so he is aware of many of the known risks that threaten all PKI dependent applications.

John knows that the US NIST has already called for designers to search for key management solutions that do not rely on public key encryption (PKE) and which are resilient against quantum computers [PKI-014]. He knows it is a fact that quantum computers may grow to a size that will catastrophically break all existing deployed public key cryptography (PKC), encryption and digital signatures, possibly within ten years according to some quantum computer experts [PKE-003]. He also knows that in 2009 Google announced[5] that they were already achieving some better results using the hardware provided by quantum computing company D-Wave Systems Inc. Since biometric (and other) data will be archived and cannot be changed obviously during his lifetime [BIO-003], John wonders at the sense in protecting biometric data (and trillions in transactions and tens of billions in investments) with PKI, since it offers no redundancy and relies on brittle cryptographic algorithms (such as RSA and D&H) that are known to be at risk of complete failure [BIO-004]. However, putting that to one side for now in 2010, John has other concerns.


John recalls sitting at a presentation during the 2008 Annual Smartcard & Electronic Identification Congress and Exhibition (CARTES) in France[6] when Kathleen Kraninger (illustrated to the right[7]) spoke.

Kathleen, the then Deputy Assistant Secretary for Policy at the Department of Homeland Security, openly disclosed how the United States *actively encourages sharing of biometrics with other countries* [BIO-005].

John, a little taken back by the one sided short discussion on international trading of biometrics, which did not identify any of the risks of international trading in biometrics, followed up later to confirm that he had heard correctly.

To quote a testimony[8] made before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification":

> "*To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems,* ***we will be able to securely share terrorist information internationally*** *to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to* ***identify and weed out terrorists and other dangerous people****, we have the same* ***obligation to work with our partners abroad to prevent terrorists from making any move undetected****." … "So what is next? We need to aggressively pursue innovation. Those who want to do us harm continue to contemplate ways to exploit our weaknesses, so we cannot afford to slow down." … "We recognize that with the power of biometrics* ***and a foundation of international cooperation****, we can transform and enhance the way the people travel the world and the way we protect our nations from those who would do us harm*."

---

[5] Neven, H., Denchev, V. S., Drew-Brook, M., Zhang, J., Macready, W. G., and Rose, G. *Nips 2009 demonstration: Binary classification using hardware implementation of quantum annealing.* Tech. rep., GoogleBlogs, December 2009. Available at http://www.google.com/googleblogs/pdfs/nips_demoreport_120709_research.pdf

[6] http://www.cartes.com

[7] kathleen.kraninger@dhs.gov – Image Courtesy of http://2002-2009-fpc.state.gov/fpc/113944.htm

[8] Kraninger, K., and Mocny, R. A. *Testimony of deputy assistant secretary for policy kathleen kraninger, screening coordination, and director robert a. mocny, us-visit, national protection and programs directorate, before the house appropriations committee, subcommittee on homeland security, "biometric identification"*. Testimony, Rayburn House Office Building, March 2009. Available at http://www.dhs.gov/ynews/testimony/testimony_1237563811984.shtm

Again, the emphasis was clearly on the claimed benefits, but there was no reference to the risks. As of mid-2008, the FBI's biometrics database alone held 56 million prints[9]. Apparently the recent increase in prints is not due to an explosion in crime or terrorism, but more fingerprinting in the private sector. The FBI now processes prints from teachers, bank employees and other non-criminals. "*That is our growth business,*" says Debbie Chapman, who works in the FBI data centre. US State and Federal legislation, such as the Patriot Act and Border Safety Transportation Act, are also driving expansion, remarks Thomas E. Bush 3rd, who served as Assistant Director of CJIS until earlier this year. "*We're seeing literally daily different legislation that requires fingerprint-based background checks.*" Biometrics is also moving to military detainees. "*Right after 9/11, we began fingerprinting people in Guantanamo and started exchanging those fingerprints with other countries*," Bush says. "*In one example, we found out of the first 100 fingerprints we sent to one country, we had three identifications in that country's criminal history database.*" And that is precisely the future of biometrics: linking different systems, particularly international databases. "*It will be the international connection,*" Bush says. "*These systems will be connected by biometrics in the not-too-distant future.*" John knows all these connected systems will be PKI dependent.

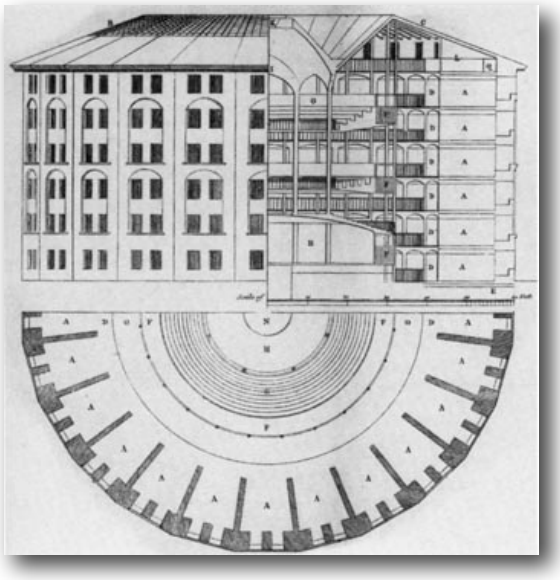
Wondering how extensive the international sharing was today, John found the following article [10]:

> "*Miller, (a consultant to the Office of Homeland Defense and America's security affairs) said the United States has bi-lateral agreements to share biometric data with about 25 countries.* ***Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement.***"

With India alone planning to capture the biometrics of 1.2 billion citizens[11] [BIO-006], John can't help but think there are going to be a lot of biometric linked "trading cards" for Government agencies to play with.

John travels internationally regularly on business, so he knows that if it's not his home country quietly trading his biometrics without his knowledge, it might be another country. America systematically captures the biometrics of everyone entering the United States. [BIO-007] John knows that it is only a matter of time before his biometrics may soon be traded internationally. John wonders if they will tell him at the U.S. airport or at any other foreign location where his biometrics data is accessed or captured, how they will use and share his biometrics? [BIO-008]

John knows ultimately he has no control over where his biometrics might go, or how they might be used. They might be used in identity fraud against him [BIO-009], or his employer, or others, for illicit systems access, funds transfers, Government and corporate espionage or for IP theft purposes. John is also aware that the definition of "*a dangerous person*", or "*terrorist*", is very flexible and open to different political interpretation [PAN-001], not just from country to country, but also between different parties in his own country. John also knows that the data could be exploited by others as a tool in cyber warfare. These are all important issues to John, particularly as he appreciates the importance of his employment in the security industry, and also because he has ambition to rise to very senior posts during his working career.



Even in his own country John has concerns about how the data might be abused at some future time. By correlating John's mobile phone cell data in combination with extensive CCTV networks and facial recognition systems supplied with his biometric data, it may not be possible, in the near term future, for John to move outdoors in city areas with any privacy from Governments [PAN-002]. *(Image of original panopticon prison to right is public domain)*

---

[9] http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?storyID=news/SCAN110509.xml&headLine=U.S.%20Builds%20Largest%20Biometric%20Database

[10] Magnuson, S. Defense department under pressure to share biometric data. In NationalDefenseMagazine.org (January 2009), NDIA. Available at http://www.nationaldefensemagazine.org/ARCHIVE/2009/JANUARY/Pages/DefenseDepartmentUnderPressuretoShareBiometricData.aspx

[11] http://uidai.gov.in/

The concept of the original panopticon design (illustrated to the right for use as a prison) is to allow an observer to observe (-opticon) all (pan-) prisoners without the prisoners being able to tell whether they are being watched, thereby conveying what one architect has called the "*sentiment of an invisible omniscience*."

John wonders if he has just enrolled himself into a global citizens '*prison*' with eventually any number of possible invisible controllers, where the multitude of Governments potentially accessing his personal data may now or in the future have very different motivations about its storage and use.

With a shudder, John recalls the Report of the Defense Science Board Task Force on Defense Biometrics[12]:

> "*Often, it is wise to protect, **sometimes even to disguise**, **the true and total extent** of national capabilities in areas related directly to the conduct of security-related activities. This is a classic feature of intelligence and military operations; it also potentially applies to biometrics.*" …
>
> "*We may expect that biometrics-based tools and techniques will be increasingly deployed in sensitive applications, and used to achieve important successes in support of national objectives. In so doing, we must seek to preserve the security of what the intelligence community calls 'sources and methods,' even while being able to headline the outcomes of such use when otherwise deemed appropriate.*"

John can think of a lot of reasons that this doctrine may also apply to military advances in quantum computing and attacks against PKI.

Similarly to the brittle nature of ICT systems protected primarily by encryption, where if the encryption algorithm fails there is no resilience or possibility of recovery from the theft and exploitation of past recorded secure data, John also understands that any one of those Governments could become a single point of critical failure in the safe storage and 'correct' use of his own personal biometric data [BIO-010].

> "*Department of Defense policy should tilt toward saving the 'original' biometric (in high resolution) rather than relying only on the processed metric/template.*"
> – On Defense Biometrics (2006)

John also knows that his biometric data will be used as part of access controls in both his employment and personal life to secured programs, services, data and restricted areas. If his raw biometric data is in the hands of other nations and their agencies, as a result of trade or simple international travel, might this biometric data be used[13] to attack critical systems? [BIO-009] And as the community becomes trained to provided biometrics on a routine basis, it is easier for attackers to acquire it.

John is concerned that he may be implicated in illicit actions through the use of his biometrics, and depending on the scenario, conceivably he may not be able to convince others that he was not the perpetrator. Similarly to brittle encryption defences, there can be no recovery from the theft and misuse of biometrics. Biometrics are not like a compromised password, they cannot be changed. John wonders how his entire life might be affected if his biometric data was misused. It is becoming an increasingly biometric dependent world, and he can imagine the difficulties he could face in the future with respect to his freedom of access and movement if his biometrics become compromised. Clearly if they were misused, then the authorities concerned for security reasons would probably need to notify an unknown list of other national agencies and potentially foreign Governments, and as far as John was aware there was no recovery process other than for him to be placed on a biometric 'black list'.

John tries to put this line of thought into another perspective in his own life. John wonders if his attendance at a noisy but lawful political demonstration in Ireland calling for greater transparency and accountability in the UK Government when he was 20 years old might be brought up some time in the future and cause him employment problems. After all, according to a Guardian newspaper article[14], the UK Police in 2009 were funded £9m to log 'domestic extremists'.

---

[12] Defense Science Board (DSB). *On defense biometrics*. Unclassified report of the defense science board task force, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Washington, D.C. 20301-3140, September 2006. Available at http://www.acq.osd.mil/dsb/reports/ADA465930.pdf

[13] Slashdot. *Hacker Club Publishes German Official's Fingerprint*, Available at: http://hardware.slashdot.org/article.pl?sid=08/03/29/1941206

[14] Lewis, P., Evans, R., and Taylor, M. Police in £9m scheme to log 'domestic extremists'. In www.guardian.co.uk (October 2009). Available at http://www.guardian.co.uk/uk/2009/oct/25/police-domestic-extremists-database .

Allegedly, detailed information about the political activities of campaigners is being stored on a number of overlapping IT systems, even if they have not committed a crime. It is not hard to imagine that a future Government might consider *anyone* in physical attendance at a political demonstration as a potential radical (terrorist). John recalls the well documented COINTELPRO (an acronym for Counter Intelligence Program) series of covert, and often illegal, projects conducted by the United States Federal Bureau of Investigation (FBI) aimed at investigating and disrupting dissident political organizations within the United States between 1956 and 1971[15]. Not surprisingly the FBI's stated motivation at the time was "*protecting national security, preventing violence, and maintaining the existing social and political order*."

John values a reasonable balance between individual freedom and social responsibility. John was acting on his own principles when he chose to participate in the political demonstration in Ireland. Now, with hindsight, he feels the weight more fully of a civil liberty issue he considered while a student at university:

> *"Whoever is **uncertain if divergent kinds of behavior will be recorded at any time and this information will be stored permanently, used or passed on**, will try not to attract attention by these kinds of behavior. Whoever expects that e.g. the attendance of an assembly or the participation in a civic action group will be registered by the authorities and that this will probably cause risks, may probably abandon their corresponding fundamental rights (Art. 8, 9 GG). This would not only impact the individuals' chances for development but also the public interest because **self-determination** is a necessary condition for the functionality of a liberal democratic polity which is based on its citizens' ability to act and to participate."*
>
> – from the German Federal Constitutional Court census Judgement of 1983 as quoted in the article "Current Legal Issues on Video Surveillance" contributed to the SECURITY Congress 2000, Oct. 9-12, 2000 in Essen by Dr Thilo Weichert.

If the authorities or media have archived footage of the demonstration John attended then John knows it will be possible to systematically identify all participants at a later date.

John notes that extraordinary conditions can sometimes lead good people in an organization to rationalize inappropriate behavior. Systems need to be designed to mitigate inappropriate behaviour from occurring, for example through models that offer redundancy and distributed trust, and that enable the detection of inappropriate behaviour when it does occur [SPOTF-003]. Entrenched systems may also invite potential for abuse and may need to be replaced. John is aware that ~65% of fraud in Europe is perpetrated by senior management[16] [SPOTF-004]. Sometimes an entirely new system is required to provide the desired properties, such as has occurred with country wide taxation systems in the past.

So, given everything that he knows about the risks and limitations of PKI itself, and how easily PKI reliant systems such as biometrics could be miss-used, John wonders if he is making the right decision to allow his biometrics to be captured now. From a personal perspective, he knows it will help him win his new job, but just as clearly his compliance can be read as agreement with and support for a security regime that clearly has serious flaws. [BIO-011]

A relaxed, attractive and socially outgoing male customer service representative approaches John and shakes his hand. "*Aaron's my name, how are you? Got all your documents?*" John is noticeably put at ease by Aaron's sociable personality. With a nod of John's head, Aaron offers to arrange John a coffee and walks him to a private booth. They sit down and a coffee arrives shortly.

Aaron shuffles through some papers and, after noting that all the paperwork is present, begins to speak: "*As a British Citizen working in aerospace I confirm that you are eligible to be an early adopter of the new NIS card. Did you know the card acts as a passport when you're travelling within the European Economic Area (EEA) and Switzerland, and that you can buy age-restricted items, such as alcohol, DVDs or video games as the card proves your age without revealing private information like your address?*"

John smiled politely.

---

[15] Hoover, J. E. Counter Intelligence Program (COINTELPRO). Comprehensive information available at http://en.wikipedia.org/wiki/COINTELPRO, 1956-1971.

[16] Aguilar, M. K. Profile of a fraudster: Subtle, senior, and stealthy. In www.complianceweek.com (May 2007), Available at http://www.complianceweek.com/article/3327/profile-of-a-fraudster-subtle-senior-and-stealthy

Aaron continues: "*And John, you will be glad to know that these card lock you as an individual to one identity through use of details like your name, address and fingerprints,* ***so they're also highly secure***." [17]

John thinks, "*Secure for who, and secure from what?*" but knows he really doesn't have much choice about this process, and it is common popular thinking that people who do not want to provide personal data must have something to hide, and so he keeps his thoughts to himself.

Of course John knew the issues surrounding the security of the system itself were much more complicated than Aaron was probably told, or cared to know, and this was not the place or time to argue. John, like many people, was well aware of the controversy around the security of e-Passports and the UK National Identity Card. However, John as a cryptographic expert had a deeper appreciation of what the complications were, for example **the problems surrounding the use of public key cryptography (PKC) in these systems**.

As previously indicated, John understood that PKC was a brittle single line of defence that offered no resilience or recovery [PKE-004], and that civilian PKI systems could be exploited by several parties to create cyber war or to conduct fraud [PKI-015]. John also understands that the UK NIC, as with all ICAO MRTD passports, employs the use of an RFID chip and is designed so that passport control points can query the chip offline. This is promoted as a feature that allows the checking system to validate the credentials just by talking with the Radio Frequency ID (RFID) chip. However, there is a catch. The complication is one of key and certificate management. John is aware of the 2009 US NIST Cryptographic Key Management Workshop that identified various limitations with current cryptographic key management, but this is a special example [PKI-016]. With over 183 countries issuing ICAO passports, and in theory, each country acting as their own Root Certificate Authority (RCA), and each RCA having several dependent Certificate Authorities, there are a lot of public keys and certificates to manage. To simplify the checking process, the RFID chip *helpfully* supplies a copy of the public key that signed the document details to the document reader device. If the reader/terminal does not go online, or has not previously gone online, and VALIDATED that this public key certificate it received from the RFID chip was indeed issued by the specific country that the passport claims to be from, then it becomes possible for any party to forge the electronic identity and electronic biometrics held within an e-passport.

The forging of identity credentials with attacker-supplied digital signatures has been convincingly demonstrated. [PKI-017] [18]

For now John has no choice but to assume, rightly or wrongly, that there is no existing code breaking size quantum computer in existence. John knows that by 2004 there were already more than 150 public quantum computing research projects and that one of the primary reasons for QC research is because of their proven capability to break codes, particularly PKC. John has his reasonable doubts about whether or not the arrival of the first such computers will ever be announced to the public due to its significance to national security. No doubt the person or group or nation state with control of or access to such a computer will wish to maximise its advantage. From a different perspective, a public announcement would be highly unlikely to happen because John can imagine the impact on public confidence and markets if such a computer was announced. For example, all confidence in eCommerce and eGovernment and digital certificates would evaporate, since they are totally dependent upon PKC.

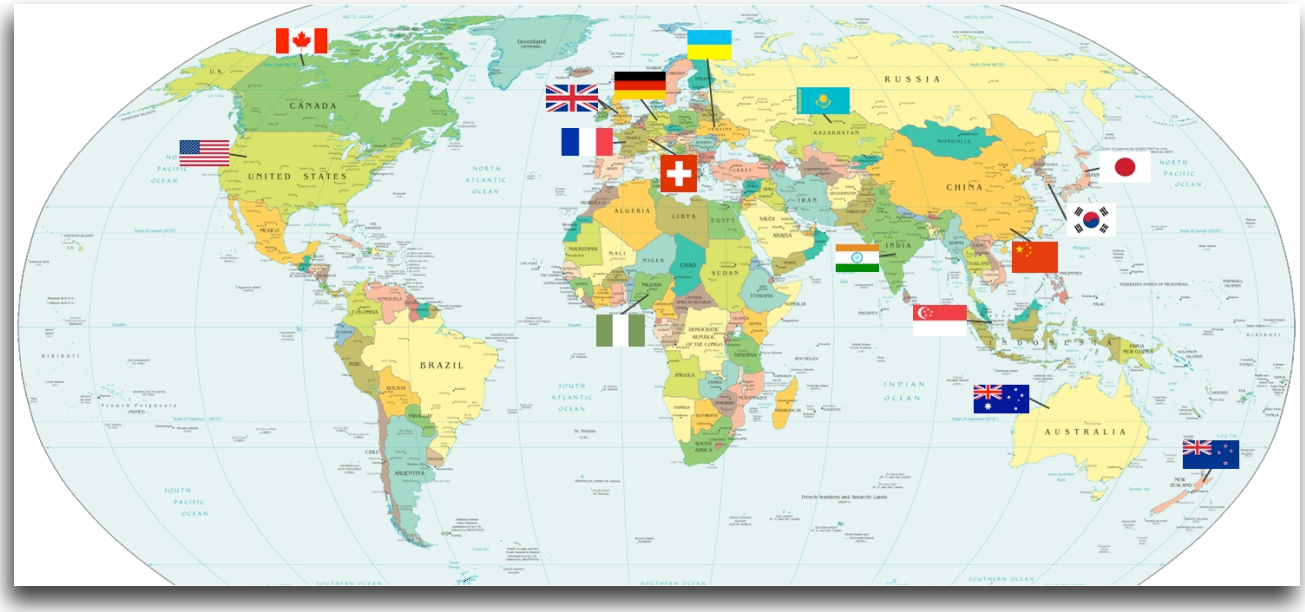
To return to the issue of the critical role of PKI dependent digital certificates in the ICAO Machine Readable Passport scheme, John knows that each of the 183 ICAO members are responsible for managing their own public key certificate authority, and each ICAO member must also have all the public keys for the certificate authorities of the 182 other members. When John last checked (2010), only a very few countries (less than 17 as illustrated below [19]) were maintaining and making their keys available on a centrally administered database of public keys.

---

[17] http://idsmart.direct.gov.uk/index.html

[18] Boggan, S. *'fakeproof' e-passport is cloned in minutes*. In www.timesonline.co.uk (August 2008), Times Newspapers Ltd. Available at http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece

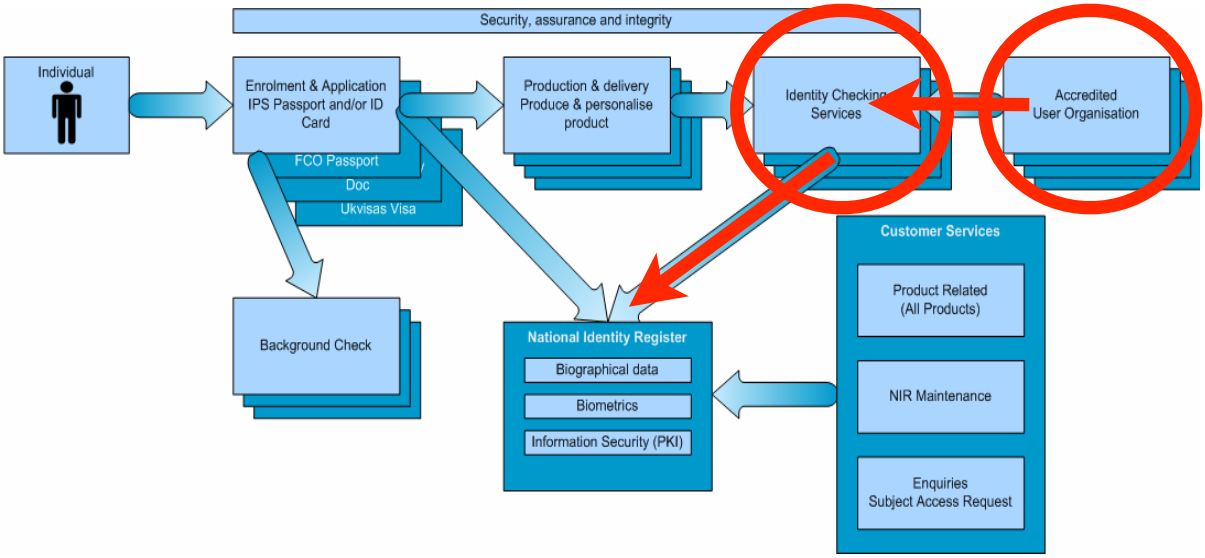
[19] Courtesy of ICAO - http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD%20World%20Map.jpg




Therefore, in a global scenario, most electronic international passport checks cannot be electronically validated with the issuing country, and therefore electronic forgery is possible as has already been conclusively proven [PKI-017].

One of the important ways the UK NIC scheme increases security is by offering a "Passport/Card Validation Service [20]" that allows any UK company to check "online" the identity details on the passport/card against the data stored on the UK National Identity Register, for a fee.

John was unable to determine from the Home Office Identity & Passport Service website if this service is accessible to foreign organisations such as border control.




To gain this increase in protection, an organisation seeking to validate that John's ID has not been forged has to have business processes and accounts in place to check back with the National Identity Registry (as illustrated above with the two red arrow[21]). This step to detect fraudulent cards in the UK NIC scheme is an improved security solution over the ICAO system. It is interesting that added feature completely side-steps the Public Key component of the ICAO scheme. This clearly demonstrates that the NIC architects determined that the public key cryptography used in the ICAO passport/card itself in this application is not adequately secure. [PKI-018]

---

[20] http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/34.htm

[21] NIS Strategic Supplier Framework Prospectus, 2007. Image and document available at: http://www.securitydocumentworld.com/client_files/070809_nis_strategic_supplier_framework_prospectus_v2_2.pdf

However, this added measure only shifts and partially addresses one of the known PKI risks, because presumably the link between the "Accredited User Organisation" and the "Identity Checking Services" is protected using Public Key Cryptography. It is also likely that the link between the "Identity Checking Services" and the "National Identity Register" is protected using Public Key Cryptography. We note that the diagram above clearly shows that the National Identity Register uses PKI for "Information Security".

Even if the Aerospace and Defence public key infrastructure (CERTIPATH/TSCP) is used (as opposed to the Civilian PKI structure such as Verisign), the system will continue to have single-point of trust failures within the certificate infrastructure, and the system will still be vulnerable to code-breaking quantum computer attacks.

Furthermore, if the diagram accurately portrays the system, there is no "separation of powers" within the "National Identity Register", nor the presence of a powerful independent audit body monitoring the activities of the NIR. This raises data privacy and data integrity concerns from insider attacks (administrators or even senior management).

John notes to himself that this type of centralised biometric data storage system cannot be deployed across Europe because some EU member States, such as Germany, do not permit the collection and storage in one location of all a citizens personal data due to risks of potential abuse. For John this is just another example of the international complexity that must be addressed when the risk/cost/benefit analysis of the European and indeed global dependency upon PKI is eventually studied, making it clearly as it were a 'whole of EU' project.

To return to the UK NIC Customer Service Centre, John acquiesces and "*voluntarily"* permits his biometrics to be captured so that, in exchange, he can travel more easily internationally and in order for them to be used for employment and other identification purposes. Next, his biometrics are then transmitted back to the National Identity Register. John's biometrics will be used to create his National Id Card, and to create his ICAO Machine Readable Travel Document. Both documents use biometrics, and their security mechanisms, will be considered valid for a period of 10 years. [BIO-012]

John knows that some people think that ten years is a solid margin of time for a document to remain secure. However ECRYPT has repeatedly advised that they have little confidence in public key cryptography 10 years into the future.

So, John is not alone when he already anticipates that perhaps in the future there may be stronger e-passport schemes. However, applying stronger security in the future will be too late to protect against some catastrophic attacks. John knows that data today is easily recorded as it travels over private or public networks. Since this archived traffic will include his unchanging biometric data, therefore today's security must offer resilience against attack for John's entire lifetime, not just for ten years.

John thought, at any time in the future, an attacker only needs to break the security protecting his **current** passport and related archived traffic to be able to steal and exploit secure data, including his unchanging biometric information. [BIO-013] John knows that this fact actually encourages hackers to record currently secure data, in what are called 'wait-and-see' attacks, whereby the hacker could auction this data to the highest bidder, particularly later when the security becomes obsolete and easily breakable [PKE-005]. This worries John because he expects that his biometrics will be used for the rest of his life. He has ambitions to rise to a very senior position during his career, which he expects will involve gainful employment for another 40 years. Then, when he retires, John expects that access identity controls, for example to his pension fund and Government social security services, will make use of his biometrics. In the context of his hoped for and potential lifespan of 100 years, a ten year security margin with low assurance thereafter makes little sense to John [BIO-003], particularly when stronger security options are already available.

John now leaves the UK National Identity Service Customer Centre and travels by train back to his home. John uses the train as it reduces his carbon footprint and it gives him time to either think about identity management issues or share more time with his 4 year old daughter and his partner when they travel together. In his new employment, John will be working on the SESARJU identity management and cryptographic key management technologies. This will be a very difficult project if they really try to address the known risks and threats. He knows the aerospace community (through the TSCP organisation) has spent approximately 5 years working just to reach agreement on how to apply the standards for an international identity management project and creating a secure email standard[22]. This new standard specifies how to implement the ***existing*** US Federal Processing security standards. [PKI-019] The TSCP/Certipath public key infrastructure, which uses public key certificate authorities, extends the US Federal PKI system[23]. Will the

---

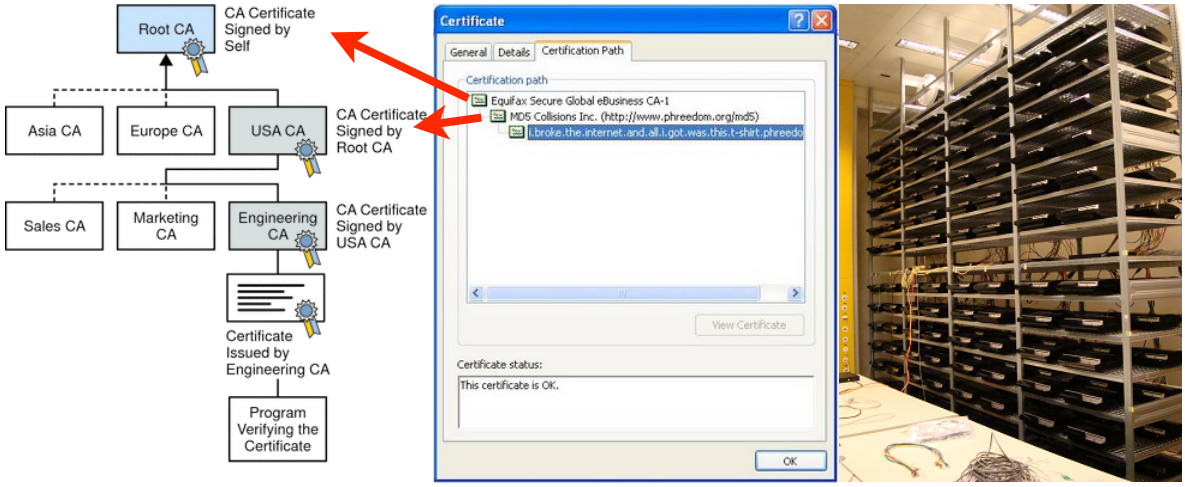
[22] Certipath. TSCP, international aerospace and defense industry secure e-mail capability. Version 2.1, CertiPath LLC, August 2008. Available at http://www.tscp.org/pdfs/SecEmlTechSpecv2-1GR.pdf

[23] http://www.idmanagement.gov/fpkipa/

SESARJU managers determine that it falls within the projects mandate to take cognisance of the latest findings of the US cybersecurity initiatives and address the known risks and threats, or will they take the cheaper and faster option of just adopting the best security solutions currently available, which will mean continued PKI dependency? Given the complexity and international scope of the issues and risks, it is unreasonable to expect one project, even a large one such as SESARJU or Galileo, to tackle a 'whole of Europe' problem. Thinking more about SESARJU, John knows that the new air traffic control systems will be extensively exploiting cyberspace. For example GPS services will supplement and in some cases may replace radar, and so cyber security will be even more critical for the safe operation of this 30+ year critical infrastructure project.

With these complex issues and concerns in mind, John now recalls the United Nations Telecommunication Union Chief's warning in 2009 of the risk of the next world war being in cyber space, a space with no super powers, as every citizen can be a super power[24]. [CYBER-001] He is aware of the growing, important US cybersecurity initiatives that are beginning to address these issues, and in particular he is thinking about the ease with which the civilian identity name space (such as the Internet Top Level Domains[25], [26]) management could be exploited to create cyberwar. [PKI-015]

John is recalling the MD5 Rogue Certificate Authority attack[27], where a group of civilians were able to exploit a cryptographic weakness in the certificate authorities of several Root Certificate Authorities, including a RCA managed by VeriSign. What grabbed his attention more than the cryptographic weakness was **how they were able to then exploit this fault to make and provide a fake certificate on ANY website on the planet to any civilian Internet user** (Firefox, Internet Explorer, Safari, …) [PKI-020]




*The middle panel above shows a forged Certificate, which is accepted by the Windows Operating System which states: "This certificate is OK." See MD5 Collisions Inc. (http://www.phreedom.org/md5) The right panel shows the cluster of Sony Playstation 3' devices that were used to find the MD5 collision which led to the rogue Certificate Authority, which in turn could generate fake certificates for any website on the Internet.*

Putting aside the technical weakness in MD5, John is wondering how and why the global Internet public key infrastructure architecture was designed with a global/system-wide single point of potential trust failure that permitted one mistake/vulnerability to expose every participant on the Internet? [PKI-021]

---

[24] Walker, G. ITU chief stresses need for cooperation to protect cyberspace. In United Nations Radio (October 2009). Article available at http://www.unmultimedia.org/radio/english/detail/83203.html, audio: http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-itucyberspace.mp3?save and http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-toure2.mp3?save.

[25] http://en.wikipedia.org/wiki/Top-level_domain

[26] http://www.iana.org/domains/root/db/

[27] Stevens, M., Sotirov, A., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A., and de Weger, B. M. M. *Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate.* In CRYPTO '09, vol. 5677 of LNCS, pp. 55–69. Available at http://eprint.iacr.org/2009/111 see also http://www.win.tue.nl/hashclash/rogue-ca/

> *"Anyone who selects a public CA on a factor other than price fails to understand the trust models that underlie today's use of CAs."*
> —Lucky Green [28]

John then asks himself, given that VeriSign comprehensively understand the civilian CA model, why would they run apoorly maintained CA with weaker security properties under a different brand name (RapidSSL), when they fully understood that this practice weakens the security of the global village? [PKI-022]

Clearly, if the wider public understood the significance of the serious weakness of the civilian CA model, or if there was an attack that was broadly felt by the public, then this would negatively impact on eCommerce and markets, and also the acceptance of eGovernment initiatives, because the guarantee of authenticity of certificates is critical in all these systems. [PKI-023]

**John has read that the USA has used cyber attack against insurgents in Iraq (2003) and was also contemplating cyber attack against Iraq banks but stopped short of that due to the Iraq banks interconnectivity with banks in France[29].**

**John wonders what would happen if a Government forced a Root Certificate Authority (or Domain Name Authority [30]) to fake identities of a foreign country during a time of war?** [PKI-024] **What would happen if this escalated internationally?**

**John knows that issues like this have prompted President Obama to put cyber security to the top of his agenda, but these are international issues and John wonders what the EC is doing about them. Even though air transport is critical to tourism in the EU and therefore a high profile potential target for cyber attack, John doubts that there will be any mechanism or capacity to get these issues seriously addressed in the SESARJU project.**

John knows that he does not need to look at the worst case 'cyber war' scenario. Cyber crime is already a very serious and growing problem which now has an annual global "turnover" in the criminal world of more than 1000 Billion USD [recent numbers from an FBI white paper] with the hardest hit industries being the banks and the insurance companies [31].

Approximately 86% of fraud happens by management at a level that can be ***sustained by the system without reaching a level that causes sufficient attention*** to expose the crime.

According to KPMG, U.S. companies loose an estimated **5 percent of their annual revenues to fraud** – about $638 billion in 2006 alone, according to research by the Association of Certified Fraud Examiners [32]. In a study of 360 fraud investigations conducted by KPMG in 2007, **89 percent** of the perpetrators committed fraud against their own organizations. **Based on actual cases** in Europe, the Middle East, and Africa, KPMG found that 86 percent of perpetrators in the cases studied held management positions; **60 percent of those were members of senior management or board members**; **11 percent were chief executive officers (CEO)**. [PKI-024]

What if identity fraud attacks were perpetrated by an organised a combination of senior management in banking and senior technical management in a certificate authority to misappropriate money in an international scheme? [PKI-025]

As John has thought repeatedly, PKI is a brittle system with many system-wide single points of potential trust failure. The most obvious line of approach to addressing the single-point-of-trust failure problem is to introduce redundancy

---

[28] http://www.mail-archive.com/cryptography@wasabisystems.com/msg02344.html

[29] Harris, S. ***The cyberwar plan***. In National Journal Magazine (November 2009), NationalJournal.com. Available at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php .

[30] O'Connor, T. *Week 3: International cyber crime and security, cybercrime and cybercriminals*. In Network security syllabus (December 2009). Available at http://www.apsu.edu/oconnort/3100/3100lect02b.htm

[31] Oak Ridge National Laboratory, Cyber Security and Information Intelligence Research Workshop, http://www.csiir.ornl.gov/csiirw

[32] KPMG. *Profile of a fraudster survey 2007*. Forensic advisory, KPMG International, April 2007. Available at http://www.kpmg.co.uk/pubs/ProfileofaFraudsterSurvey(web).pdf

into the system, such that trust around an identity is distributed amongst competing service providers – ensuring each identity was validated by two independent Root Certificate Authorities in some well-defined standardised way.

As a hardened pragmatist John knows that this could be an unpopular proposal in the established public key infrastructure industry that makes a lot of money out of the current model. John expects that even the industry generally would not agree to consider undertaking a new risk/cost/benefit analysis without clear support from Government. John expects that, without such an analysis, even an evolutionary upgrade would meet with industry resistance: [PKI-026]

- Root Certificate service providers could feign offence at the suggestion that their security systems were insecure or required the support of other root (sovereign) certificate authorities, as this might weaken their customers perception of the value of their existing service;
- Root Certificate service providers could argue that the (some consider exorbitant) costs they charge already for a 12 month certificate would have to increase further to support the extra effort needed to distribute trust and create resilience through redundancy creation across, and co-operation between, providers;
- Developers who are having trouble supporting the already complex public key infrastructure would have to retroactively upgrade every application to support dual standards;
- Customers ordering certificates might have to co-ordinate the activities of two recalcitrant certificate authorities;
- Not to mention internal objections from some senior management who currently had the opportunity to exploit their position as a single point of potential system failure or fraud; introducing a new system that distributed trust and created redundancy might expose existing fraud as much as remove the opportunities for fraud.

In the face of potentially entrenched self interest and arguments about added cost, and in the complete absence of a proper risk/cost/benefit analysis, John knows that an EC level, 'whole of Europe' comprehensive study needs to be done, coherently taking all the factors into account, aligned to the welfare of the global community and not just the interests of any one commercial/national organisation, industry or pressure group. [PKI-027]

John knows he is not alone in worrying about "*the identity management issue*", however much of the conversation is discussed behind closed doors due to vested interests and different perspectives and agendas on the issue. Depending on who John talks to, the problem varies from one of protecting against technical weakness, to ensure smooth operation of the Internal Market, empowering citizens to control their own identity, enabling citizens to interact more effectively with Government, all the way to the extreme objectives of "*locking down*" the civilian population so they can track all their activities for law-enforcement purposes, and the militarisation of the Internet.

John has no idea how he might even begin to approach these issues in the SESARJU project, and rally the support of his management, much less how his managers might win the interest and support of the project 'investors'.

John's mind moves to consider the rapidly advancing US Cybersecurity Initiatives.

John is aware that the last near-term action point on the US 60-day Cyberspace Policy Review report is to "*Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation*". [PKI-028]

US 60-day Cyberspace Policy Review report also states "*The United States must work actively with countries around the world* ***to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations***".

John is aware that subsequent to the publication of that Report, the US NIST held an official Cryptographic Key Management (CKM) workshop to[33]: "*improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support* ***a global cryptographic key management infrastructure***".

However John had wished these publications went further, to explicitly state that these designs must take into account the legitimate interest of ***all*** stake holders, and explicitly require that the design must mitigate against Militarisation, against designs that favour the "*National Interests*" of one Nation over all others, against the potential for "*fraud*" by certificate authority insiders, managing the system, and against the risk of targeted action against specific citizens or even cyber war that could be performed by instructions of (current or future) Governments.

---

[33] http://csrc.nist.gov/groups/ST/key_mgmt/

John is aware that there are calls emanating from inside NIST for "*resilience against quantum computing attacks*", "*cost-effective, fault-tolerant, and highly available*", and "*that in the light of quantum computing CKM system designers MUST look at means other than using public key-based key management systems*." [PKE-002]

But as far as John knew, such a widely accepted identity/key management system does not exist yet. [PKE-006] He knows that the research into quantum cryptography is still in its infancy with a new attack brought in 2009 [34] [35]. [QKD-001] Even so, its advocates state publicly that existing quantum key distribution systems are not suitable to protect the Internet. [QKD-002] This only leaves symmetric key technologies (the opposite of public key technologies) as the most trustworthy approach.

Like most security experts John knows that the US Navy is setting up a new Cyber Command at Fort Meade[36] (Headquarters of the US NSA) and that President Obama has sought a Budget approval of **3.6 billion USD** for the US Comprehensive National Cybersecurity Initiative (CNCI) for 2011 alone[37]. [CYBER-002]

Apparently the US Army wanted "*to be in charge of security for the 11 million Internet users, seven million PCs and 15,000 networks belonging to the Department of Defense (which is the largest Internet user on the planet). All the services are scrambling to get their Cyber War defenses strengthened, but the air force wanted to be in charge*." … "*The U.S. Air Force is still advocating more Cyber War attacks by American Cyber War organizations*."[38] See also [39]

But as Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence stated in his Keynote Speech at the NIST CKM Workshop, "*the Cybersecurity Initiative is primarily to protect .mil and .gov information. Somebody should worry about .com. Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet*."[40] [CYBER-004]

John wonders what the cost will be to support the necessary research and development, and globally coordinated efforts for that remaining 98%, and what role Governments, United Nations, and the Organisation for Economic Co-operation and Development will play [CYBER-005] and how the entrenched security organisations will move forward particularly if they is no clearly identified buyer in these harsh economic times.

In the civilian and EU sectors, John is aware of the massive momentum built up around the deployment of the 20th century security solutions using PKI, which he knows already protects transactions worth trillions and investments worth tens of billions. In spite of the latest cybersecurity risk analysis activities in the USA, and the identified and known risks to PKI, John knows that PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU. [PKI-029]

He knows that PKI is the main interoperable solution in most security vendors arsenal. It could be economic market suicide for any PKI vendor to advertise that their own products are at high risk of security failure due to multiple single points of potential failure and the advance of quantum computers. This industry stance is evident from the minimal corrective actions taken after the MD5 Rogue Certificate Authority attack. Vendors will rarely seek to point out the

---

[34] Makarov, V., Anisimov, A., and Sauge, S. *Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by eve*. In arXiv.org quant-ph (March 2009). Available at http://arxiv.org/abs/0809.3408v2

[35] Gerhardt, I., and Makarov, V. *How we eavesdropped 100% of a quantum cryptographic key*. In Hacking At Random (Har2009.org) (August 2009). Lecture video available at https://har2009.org/program/events/168.en.html.

[36] Gates, R. M. *Establishment of a subordinate unified U.S. cyber command under U.S. strategic command for military cyberspace operations*. Department of Defense memorandum, June 2009.
Available at http://publicintelligence.net/?p=1010

[37] Chabrow, E. *CNCI budget request set at $3.6 billion*. In www.govinfosecurity.com (February 2010), GovInfoSecurity.com an ISMG Corp. media property.
Available at http://www.govinfosecurity.com/articles.php?art_id=2151&rf=020210eg

[38] Strategy Page. *The U.S. Navy Cyber Warriors Step Up*. In StrategyPage.com (October 2009).
Available at http://www.strategypage.com/htmw/htiw/articles/20091006.aspx

[39] O'Connor, F. *Political cyberattacks to militarize the web*. In PC World - Business Center (March 2009), IDG News Service. http://www.pcworld.com/businesscenter/article/161142/political_cyberattacks_to_militarize_the_web.html

[40] Barker, E., Branstad, D., Chokhani, S., and Smid, M. Cryptographic key management workshop summary (draft). Interagency Report 7609, National Institute of Standards and Technology, June 2009.
Available at http://csrc.nist.gov/publications/nistir/ir7609/nistir-7609.pdf

almost total lack of resilience and distributed trust, or the major problems, faced by all organisations, with public key management. John knows they will not wish to point to the fact that, while PKI can reach to service millions of users, the US NIST has already published in the CKM Workshop Report that new solutions must be found that will allow it to scale several magnitude more in the near future. [PKI-030]

John however was working in the EU and he believed that the USA led the security agenda and that much of the US cybersecurity activity was largely unknown to his associates in Europe. There was new legislation being rapidly advanced in the USA that would require the US NIST to lead the USA's international cybersecurity standards initiative[41] [CYBER-006], but John was unaware of an equivalent high level co-ordinated (or equivalently funded) response in Europe.

**John was also aware of the need to protect individuals against erosion of liberty due to National Authority's being single points of control over their citizens participation in international systems.** This dependency could be exploited to coerce other nations (for example if one nation through certain proprietary banking activity had access to much of another nations banking data), or to create cyber war against the globe, or could be used as a tool by an authoritarian power or Government against its citizens. [SPOTF-001] [SPOT-002]

John, like many security experts, was aware of this range of risks and threats but knew that due to the economic climate and entrenched interests, most security vendors would not be willing to allocate funds to the study and trial of new designs. [PKI-031] Rather they would want to maximise sales of their existing solutions, even though the UN Telecommunications Chief has publicly warned of the risk of the next world war being in cyberspace where there are no superpowers, because every citizen can be a super power[42].

In short, John recognised that the magnitude of the issues is beyond the study and reach of any player, even a leading nation. It will be difficult for countries to make the necessary changes, for a globally appropriate system, when national self-interest is in play, and particularly for those countries militarising their cyber interests.

To provide one recent example of this type of governance difficulty, according to Peter Eigen (previously a director of the World Bank in Nairobi): "*In Germany there is a system where you are not allowed to bribe a civil servant, but you are allowed to bribe a deputy. This is under German Law allowed. And the members of our parliament don't want to change it. And this is why they cannot sign the U.N. Convention against Foreign bribery. One of the very few countries that is preaching honesty and good governance everywhere in the world, but are not able to ratify the convention.*" (2009).[43]

John agrees with the President of the USA when he stated publicly recently, an international effort is required to create new cybersecurity standards. **But, in the absence of the highest level of leadership in Europe (and other regions), without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community. With the militarisation of the Internet by foreign Governments, many of the "new standards" may become weapons of coercion and not tools of global social empowerment for the other 98% of the world's population.** [CYBER-007]

So right now, John has to focus on how we will manage this complexity with regard to the services and advice he will deliver to the security group which carries responsibility for a small but important part of the €2.1 billion SESARJU development phase. He knows that he took the simplest and most expedient path when he agreed to have his biometrics recorded and archived for his new passport and UK NIC, in spite of his own real and justified concerns and fears. John asks himself how he can morally argue that SESARJU should address these problems when he himself has subscribed to the system by choice driven by expediency. He knows that the major security vendors will probably be driven by prevailing economic conditions to promote existing certified solutions, rather than try with a limited budget to address the real issues and risks that apply to an international 30+ year project. Given the complexity and international scope of the risks and issues, is it even reasonable to expect that one project should try?

---

[41] Lipinski, D. H.r. 4061: Cybersecurity enhancement act of 2009. Available at http://www.govtrack.us/congress/bill.xpd?bill=h111-4061.

[42] Walker, G. ITU chief stresses need for cooperation to protect cyberspace. In United Nations Radio (October 2009). Article available at http://www.unmultimedia.org/radio/english/detail/83203.html, audio: http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-itucyberspace.mp3?save and http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-toure2.mp3?save.

[43] http://www.ted.com/talks/peter_eigen_how_to_expose_the_corrupt.html (13 minutes into talk).

## 5.2 Scenario: 2015 (Future Risks)

John is sitting nervously at the Heathrow Airport, waiting to board his plane (an impressive Boeing 747-8 [44]). With the international financial markets still recoiling from the second round of property mortgage write downs in the United States[45], the airport remains busy, however one imagines that there used to be more tourists at this time of year.

John is on his third espresso for the morning and distressed about the series of technical and political problems emerging against his SESARJU project. He was still in shock at how quickly these issues had moved from the background to become active threats.

John did win the job at Thales in 2010 and has been travelling internationally between the countries participating in the SESARJU and FAA NextGen Project to work on the identity management and cryptographic security aspects of the project.

His team had been assigned to work on P14.2.2[46] which was tasked to ensure that the System-Wide Information Management component of the SESARJU project was safe and secure. John and the other security experts had recently signed off a security standard based on US NIST public key cryptography. It was the available compromise option under the existing circumstances, acceptable as long as the SESARJU security parameters were limited to allow single points of potential failure, to allow a lack of resilience and redundancy and distributed trust, and to require only cryptographic security against classical attacks, and not security against known quantum computing threats. After accepting these parameters, it was relatively easy and affordable for John's P14.2.2 project to reapply vendors popular 20th century solutions. A predictably short sighted approach that, like the lack of security in the first deployment of the Internet [CYBER-009], was now starting to become painful [CYBER-008].

In his initial after-hour meetings with his new peers, John had raised the risks surrounding PKI. Some of his peers frowned, and the team leader politely advised John that "*of course*" it was only possible to use already accepted standards and that he would receive no support from his team if he raised it. [PKI-011]

John asks him self rhetorically what more could he have done?

John already knew, when started on the project in 2010, about the 2009 US NIST call for new solutions that were resilient against quantum computers and that did not rely on PKI. Now he is concerned that their new PKI based security architecture, targeted as it is to a 30+ year critical infrastructure project [PKI-003], might not see the light of day. If it does get deployed, John's stress levels will not diminish. He wonders how long it will be before the entire system may well need to be radically reworked, perhaps in a very costly rip and replace scenario. John is very aware that the old approach of trying to upgrade and add security on later was a losing game. *But he felt that he had been railroaded* by circumstances since 2010, and in particular he needed to keep his employment. John recalls that, like his colleagues, he had come to the conclusion that it was not possible to tackle the international issues of critical single points of control and potential failure, and they had rationalised that maybe large quantum computers would never come.

Taking another sip of his coffee, John recalled that the topic of quantum computers somehow never really emerged in any of the project discussions. There was he felt an institutionalised blindness on this subject and some vague expectation that quantum cryptography may evolve to one day provide the security solution to the quantum computing threats. [PKI-033] The SESARJU security team had taken the '*safest*' approach and applied the current US NSA Suite B standards to the letter, which included PKI.

But 2 months ago, the problems had started.

---

[44] http://www.boeing.com/commercial/747family/

[45] Big Banks in Trouble: Huge Mortgage Write-Downs Seem Inevitable, http://seekingalpha.com/article/144554-big-banks-in-trouble-huge-mortgage-write-downs-seem-inevitable?source=article_sb_popular

[46] http://www.sesarju.eu/programme/workpackages/wp-14-swim-technical-architecture--201

At that time ECRYPT III (European Network of Excellence for Cryptology[47]) published their Yearly Report on Algorithms and Key Lengths (2015). It was the first time it has been significantly revised since it had started in 2004[48]. In all ECRYPT key-length Reports up until this one, the 12+ authors had side-stepped the issue of future computing capabilities with a disclaimer buried deep in the text around page 24 of the 71 page document: [PKI-034]

"*The recommendations in this report assumes (large) quantum computers do not become a reality in the near future.*"

In this revision of the ECRYPT Report, which was uncharacteristically 6 months late, the text was effectively rewritten to elevate the threat of quantum computer attacks to become a mid term risk that must be addressed in the immediate future. The paper reports that a joint effort between the US Quantum Information Program[49] at NIST and the EU Future and Emerging Technologies (FET) Proactive Initiative in Quantum Information Processing and Communication[50] had made a significant advance in ion-trap based quantum computation.

The unofficial word on the grape-vine is that the quantum information processing community advised certain cryptographic security advisors of the full significance of their discoveries behind closed doors, to permit them some time to search for a coherent strategy to recommend to their respective communities. The quantum information processing group advised that while the remaining steps are rather expensive, and will require a good number of person-hours, the remaining technical barriers appear to be surmountable. Furthermore, in light of the code breaking capabilities and also other benefits offered by large quantum computers, they advise that they have received priority "defence" funding to proceed. ECRYPT didn't put a time frame on when they would arrive, however experts like Professor Seth Lloyd of MIT, who co-invented the world's first (public) quantum computer in 1996, had never been afraid to make a prediction. In 2008 he had estimated code breaking computers could arrive after 2018. Professor Lloyd now publicly advised that, based on his information, code-breaking quantum computers may arrive after 5 years[51] and that it is possible China could already be some way ahead. John wonders if maybe the breakthrough was made by, and then subsequently gleaned from, the Chinese?

John has now read the ECRYPT Report twice. It is well thought out and full of carefully worded disclaimers. It brought no joy to John. The ECRYPT Report advised that the international cryptographic community had made no focussed effort to evaluate candidate "post quantum secure" public key cryptography [PKI-036]. The very first conference focusing on the problem was held in 2006, then only every two years up until 2014. The progress was slow and there simply was not enough publications available nor sufficient interest to run the conference every year. Even as late as 2012 well over 90% of the papers on public key cryptography published on EPRINT[52] were still based on constructions that could be attacked by code-breaking quantum computers.

ECRYPT advised in this Report that it can take up to 10 years of intense international study for the community to identify, test and hopefully accept a new quantum resilient public key algorithm, providing of course that one can be identified that can also survive the new quantum algorithms discovered over that period. This time projection is based on solid experience learned in other cryptography contests, for example the recent US NIST SHA-3 hash function competition had taken approximately 7 years to develop and gain consensus about a selected candidate in the international cryptographic community. The NIST hash function competition was a simpler process in that it was looking for stronger ways to randomly mix data together. Developing any new public key algorithm requires identifying new mathematical equations with very particular algebraic properties. Even without the added complexity of achieving resilience against quantum computers, these particular properties unfortunately already increase the difficulty in achieving assurance that there isn't some 'simple solution' to breaking them. This problem was experienced with the classically secure ECC algorithm, which though being significantly more efficient, has taken years

---

[47] http://www.ecrypt.eu.org/

[48] Gehrmann, C., Naslund, M., Babbage, S., Catalano, D., Granboulan, L., Lenstra, A., Paar, C., Pelzl, J., Pornin, T., Preneel, B., Robshaw, M., Rupp, A., Smart, N., and Ward, M. Ecrypt yearly report on algorithms and keysizes (2004). Deliverable D.SPA.10, IST-2002-507932 European Network of Excellence in Cryptology (ECRYPT), March 2005. Available at http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.10-1.0.pdf.

[49] http://qubit.nist.gov/

[50] http://cordis.europa.eu/fp7/ict/fet-proactive/qift_en.html

[51] Lloyd, S. *Riding d-wave*. In Technology published by MIT Review (May 2008). Available at http://www.signallake.com/innovation/RidingD-Wave042408.pdf. Quote: "At current rates of progress, big, code-breaking quantum computers are at least a decade away."

[52] Cryptology ePrint Archive, IACR. Available at http://eprint.iacr.org/

to win acceptance and only recently has begun to be deployed widely in the community. [PKI-035] The US Government was spending large sums to deploy ECC particularly for applications with its allies but it was an already well established fact that the ECC algorithm, like all other existing deployed public key algorithms, completely failed to code breaking quantum computer attacks. Unlike most systems, the US cleverly left themselves an insurance policy – ALL the US security modules replacing legacy systems in the field were required to support remote programming, so they could upgrade their field deployed security technologies.

One of the problems ECRYPT highlighted was that insufficient experts in the cryptographic community had taken the Government and privately funded research into code-breaking quantum computers seriously. It was also very unpopular to go around saying "*the systems we have will break*" when it was obvious to the community that there was no public key alternative available for the "*prime-time*" ready to promote. Entrenched interests ruled the waves and the dominant need to satisfy harsh economic realities had prevented a strong focus in the study of quantum resilient public key algorithms. Proposing new public key algorithms was also not very popular among cryptographers, as many attempts before hand been broken, and the chances of their proposals failing was also high.

The ECRYPT Report listed a handful of existing candidates, and advised that the EU had funded them to organise a 3 year fast-track program of testing to select the best public key candidate. [PKE-007] [PKE-008] Worse still, most cryptographers did not understand the full range of computing capabilities expected from quantum computers, and so could not evaluate the potential risks for the next generation public key candidates. [PKE-009] The US NIST made a different decision. The 2004 US ARDA Report had advised that new quantum algorithms would continue to be discovered, and that some of these could be expected to be relevant to the existing hard problems candidate public key algorithms are based on. That Report pointed to the theoretical existence of hard problems (random permutations) that were resilient to quantum computing era. The US already had one symmetric encryption (shared-key) algorithm that was conjectured to be secure under this model (AES-256). Furthermore the US and NIST were heavily invested into Quantum Key Distribution (Quantum Cryptography), a special type of symmetric (shared-key) cryptography. Of course a different division of NIST also performs advanced quantum computing research, and so results internal to NIST may have advised them of future risks. Therefore the NIST continued and escalated their 2009 call for designers to develop new symmetric key capabilities that did not rely on public keys. The global security community was now split. [PKE-002]

**Free to use** proposals supporting key distribution using symmetric systems in a way that employed multiple servers and distributed trust was proposed[53] in 1976 by the co-inventors of public key cryptography before the arrival of public key cryptography! This technology could have be adapted to build international key distribution systems of modest scale.

John was personally aware of proposals since 2007, based on the techniques in the 1976 proposal, that could enable a shift away from public key encryption for key distribution even in very large scale international systems. This could be achieved using just the AES-256, or AES-256 in combination with quantum key distribution (QKD) networks. NIST researchers clearly continue to receive funds to create advanced QKD systems, however NIST does not have to rely exclusively on this research to create a classically and quantum secure key distribution replacement. NIST can design new Cryptographic Key Management Solutions that use both techniques when available in a redundant manner, and fall back to use just AES-256 for Internet applications. Of course the dual model first required the discovery of a robust implementation of QKD, a solution that was free from attacks against the QKD implementation.

This shift away from public key encryption for key distribution can be achieved using just AES-256 for key distribution, or AES-256 in combination with QKD networks for key distribution. NIST researchers are clearly continuing to be funded to advanced quantum key distribution, however NIST does not have to rely exclusively on this research to create a classically and quantum secure key distribution replacement. NIST can design new Cryptographic Key Management Solutions that use both techniques when available, and fall back to just AES-256 otherwise. This way if a robust manner of implementing QKD was finally discovered, a solution was free from attacks against the implementation, the NIST research could be rapidly integrated by the CKM solution they designed and was already in production use in parts of the globe.

However, like the majority of cryptographers at the time, John was on a team that felt it had no option but to adopt the existing Government standards based public key cryptography. After all, it was what he knew from his earlier work in TSCP, it was what the US and EU Governments were using at the time, and it was the politically safe decision.

---

[53] Diffie, W., and Hellman, M. E. Multiuser cryptographic techniques. In AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (New York, NY, USA, June 1976), ACM, pp. 109–112. Availableathttp://doi.acm.org/10.1145/1499799.1499815. Available at: http://portal.acm.org/citation.cfm?id=1499815

But now PKI was a political land mine...

Last month, the Transport Committee urgently rushed an agenda item on to the European Parliament agenda to exchange views on the security of SESAR against quantum computer attacks over its 30+ year operational life span. The primary focus of this agenda item was, "what defensive actions would be taken by SESAR" and most importantly "what would it cost". Once again, the failure to build in long term security from the outset had committed the SESAR project to the old cycle of trying to add in the necessary security later!

Patrick Ky, Executive Director of SESAR (illustrated as the speaker to the right[54]), said this was the first time he had personally heard of this risk. Like others big projects being called to account, Patrick asked for time so that he could organise a comprehensive report to be compiled that could be understood by himself and the members of Parliament.

John took another sip of his coffee.

John knew that he, his team, and the organisations they worked for, would probably be able to side-step responsibility for the problem. [PKILS-001] This potentially catastrophic problem effected every standards based security system on the planet, and his organisation wasn't the only one under the gun.

The issue his team faced now was the same issue that they could have begun to address at the beginning of the project, but hadn't. They were now under pressure to seriously begin looking for a cost-effective and rapid solution. The purpose of the meetings in the USA was not to identify who was accountable, but to evaluate the different recommendations of ECRYPT and the US NIST, and to search for a suitable solution. However, the team was having difficulty defining "suitable". Suitable cryptographically, financially or politically?

In critical infrastructure projects the development process is undertaken at more rigourous levels. Comprehensive risk models are developed and studied.

In spite of certain levels of risk management process, the US cybersecurity initiatives had conclusively established that this is not the case for cryptography. Certain assumptions and practices are simply carried forwards from the past. Brian Snow was Senior Technical Director of the Information Assurance Directorate of the US NSA. Snow is on public record since 1999 stating that we need assurances in the civilian security industry[55]. Speaking at international conferences around the World, Snow stated in 2005:

> "*The software security industry today is at about the same stage as the automobile industry in 1930; it provides performance but offers little safety,* ***and that is the security industry***."
>
> "*Looks nice, goes fast, but in an accident,* ***you die!***"


Now John and his team needed to look carefully at the symmetric solution approach being advocated by the USA. There are significant structural differences between a public key cryptosystem to a symmetric key solution. The cost of now rigourously developing either approach would be about the same. However, at this late stage in the project, the shift from public key to symmetric key would be effectively the same as restarting the analysis in this aerospace application from scratch. This would be politically very unpopular.

---

[54] Image courtesy – http://www.sesarju.eu/news-press/news/hearing-sesar-european-parliament--488

[55] Snow, B. *We need assurance*. In Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems (January 1999), vol. 1717 of Lecture Notes In Computer Science, Springer Berlin / Heidelberg Springer Berlin / Heidelberg, p. 725. Available at http://www.springerlink.com/content/33qe0m8c8ahlthmr/.

If his team adopted the NIST "symmetric key approach" at this late time, it would mean that most of the work based on "public key technologies" completed since 2010 would effectively be discarded and could not be significantly reused. John new that this was a predictable problem that now faces every EU funded security project. John didn't want to think about how low the return on investment for projects that continued to press ahead with at risk public key cryptography when they could have used robust alternatives.

Given the known difficulties with, and risk of not, actually discovering a trustworthy public key solution that might be resilient against quantum computers, John expected that ultimately the US preference for symmetric based solutions would take precedence over Europe's preferred path. However right now there were urgent time-line pressures.

John knew that with the tight financial economic times they were in, and with such a late correction in the development process, schedules might be delayed, and the immediate and short term costs could be significant. However, if the system is not secure in practice, you may as well not have put in any security mechanisms in the first place.

John was torn between the two choices: Commit to using experimental next generation public key cryptography based on the pending 3 year EU competition [PKILS-001] and reuse the teams existing work and ignore the single point of trust failure issues, or rework the solution to use the more conservative symmetric key solution with its higher up-front costs at this time in the development life cycle. He didn't like either choice under the current political circumstances.

**John receives a one-line SMS on his iPhone from one of his international colleagues.**

It reads "*Visit Cryptome before you arrive and be ready.*"

John turns on his second Generation Apple iPad and opens up the page to Cryptome, the security and Government watchdog site[56]. John can't find any new articles on quantum computing, but finds a prominent new link regarding the US Federal PKI Bridge.

John taps on the link and begins to read the page.

Apparently one of the many servers in the US Federal PKI Bridge system (as currently used by the aerospace sector) was hacked from a computer in America that was controlled remotely from a computer in China. [PKI-020] Apparently the electronic identity of a highly skilled contractor working on a military jet navigation system was hijacked, as was the identity of the system administrator for that project by breaking this one node. Together the two identities were used to capture the intellectual property of the navigation system, and then to add insult to injury, the data was deleted from the US servers. To make things worse, the attacker was able to also delete the online remote backup server which was physically located in a building in a different state. In this project, apparently there were no "offline" backups because they felt remote site online mirroring was previously assessed to be sufficiently secure, because the risks in the current identity management system were not accurately taken into account.

While the attack appeared to come out of computer run in China, and there is a history of such attacks http://www.militaryphotos.net/forums/showthread.php?172973-The-top-10-Chinese-cyber-attacks-(that-we-know-of) there are some pundits arguing that maybe the computer in China was also remotely controlled, this time by a small, politically motivated cyber-terror group interested in increasing trade difficulties between China and the United States for their own advantage. China was also refusing to co-operate with US investigations because of posturing with regard to international cyber-security policies.

Unlike the Rogue Certificate Authority Attack which broke the hash function used in the certificates to exploit a single point of trust failure in the certificate authority system, this attack did not break any crypto. Instead, the attacker exploited a buffer overflow problem in the operating system of a computer that had software that talked with a network attached hardware security module to sign identity certificates. The attacker was able to remotely gain access to the computer, and then by pretending to be the authorised software, forged a request to the hardware security module managing the private keys of the certificate authority to sign new identities on behalf of the attacker.

Just like the Rogue Certificate Authority Attack, the attacker exploited the system-wide single point of trust failures in the US Federal PKI, Certipath, TSCP security model to attack other users. [PKI-020]

John stares blankly at the ground, wondering how he can side-step addressing this latest issue in his next meeting…

---

[56] http://www.cryptome.org/

"*Given their power to intercept and disrupt secret communications, it is not surprising that quantum computers have the attention of various U.S. government agencies. The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.*"

– Professor Seth Lloyd of MIT 2008
co-inventor of the first quantum computer [PKI-036]
*(Image: http://www.edge.org/documents/life/life_index.html)*

## 5.3 Scenario: 2019 (Known Future Risks)

John Smith is reclining in his seat in the business class of an Airbus A380-900[57], flying at an altitude of 30,000 feet, heading towards to Los Angeles Airport. John is still working for Thales in security, but no longer on the SESARJU project. John is working on a new project.

After the second suite of mortgage write-downs that happened around 2014, there was increased pressure to independently audit the US Federal Reserve for the first time in its history. A revised version of the H.R. 1207 Federal Reserve Transparency Act of 2009[58] was signed into Law in 2016. The transparency, accountability and 'independent audit' trail fever flowed on to other unrelated industries, including the information technology security sectors. John had been called on to participate in an international expert panel to independently audit and sign-off on a highly technical but unclassified component of a large report on the "state of affairs" of the US Critical ICT Infrastructure.

**John's mind wanders back to the SESARJU and NextGen meetings of 2015.** John recalls how these meetings were more political than technical. The technical options available were reasonably clear, the path forward was not. Slowly a strategy emerged. There were two options: (a) adopt the public key algorithm selected by the 3 year fast-track program to evaluate candidates when it became available or (b) rework the analysis to use symmetric key techniques. Both techniques would be 'computationally secure' in the short term. Option (a) would be cheap to adopt, and *might* be secure into the future. Option (b) would require reworking the security model at about the same cost as already incurred but would provided significantly higher assurance in the long-term. [PKI-037]

The security team did not want to be responsible if the public key algorithm selected under stress by the ECRYPT failed in the future, furthermore they didn't want to be responsible for rocking the boat with the rework option this late into the project. The strategy that emerged in the security group was to shift the hard decision away from themselves towards upper management and investors in a way that they (and their security organisations) could later take advantage of, irrespective of the selection made by management. After all, if the public key algorithm failed, they could say that they offered the most cost conservative solution, but management did not listen to their warnings that the cheaper option of public key algorithm may fail. [PKILS-003]

With the help of the desktop publishing team, and a graphic artist, a short glossy report was prepared. The two options were presented side-by-side, with the positive and negative points listed side by side. Technical terms like "Computationally secure against *best known* attacks" were used to describe both options. The financial costs and timeline extensions were listed for both options.

The glossy short paper was indeed visually impressive, *appeared* comprehensible to the lay-man and was supplied to the administrative team. The paper was crafted so that cryptographers could later argue they accurately presented the risks, but they knew that executives and managerial staff would read both options as being adequately secure. Management and investors would immediately identify that the first option was far less costly, apparently less risky at at project execution level and it was clear to management and the investors that their liability might be shifted away from the project and towards ECRYPT if the new cipher turned out to be a dud. Also, it was politically expedient for the SESARJU project to rally behind ECRYPT. Of course ECRYPT had made the hard and unpleasant decision to rapidly find a replacement public key algorithm because they felt intense pressures from industry to find a low cost solution.

---

[57] http://en.wikipedia.org/wiki/Airbus_A380#Improved_A380-800

[58] http://www.govtrack.us/congress/bill.xpd?bill=h111-1207

Not surprisingly, the SESARJU project selected to replace the NIST approved ECC public key algorithm with the risky ERYPT public key alternative. Furthermore, the single-point of trust failure was pushed aside again. In this way, 95% of the original work-effort was salvaged, at the expense of much lower assurances.

**The fasten seat belt sign lights up and the plane begins to reduce altitude.**

John's gut clenches a little with the shift in pitch. As an air traffic consumer John had hoped that the very best long term security was being deployed to ensure the safety of his journey. After all, safe air travel was also essential for tourism in Europe. Today, John is not feeling safe during his flight. The original proposed minimum key lengths had to be increased due to advances in cryptanalysis against ECRYPT's initial parameters on the new public key cipher they had selected, and John is among those who feel a general unease that maybe someone might see a fatal flaw that would be obvious in hindsight (e.g. when you rewrote the mathematical problem in another way). [PKE-008] John thinks of the all electronic cyber enabled ground-to-air forward trajectory planning that has been implemented to enable a lower noise, low power aircraft approach. John knows that more planes are flying on the same efficient flight trajectories because the flight plans are managed electronically. There is less margin for error now.

The safety of the flight depends in part on the security of the cryptographic algorithms. With the reduction in air-traffic management costs, there has been a direct reduction in the number of human controllers. If the system has to return to manual control with the 2x increased traffic density, there will be a much higher risk of a mistake in the intense confusion and density of incoming flights.

Worse, if during that time an attacker could alter the flight plans undetected by performing a man-in-the-middle relay attack, the chance of a collision increases significantly. The lack of distributed trust, redundancy and resilience in the PKI dependent air traffic control systems makes a catastrophic attack possible. John recalls the public prediction voiced by Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence that a catastrophic event will happen and that we will all be screaming. John is feeling decidedly queasy.

John's plane lands safely.

John grabs his 9 year old biometric passport and proceeds to clear himself through customs.

John waits in queue to be processed by the "*millimeter wave*" scanner (illustrated to the right) that effectively performs a virtual strip search[59] to check for substances such as weapons, undeclared money and drugs[60], [61].

John follows the guidance of the Transportation Security Administration officer, moving his arms in ways to maximally expose his body to the 3 dimensional imaging system.


[59] Image to right and information from: http://publicintelligence.net/scanner-porn/

[60] Kodo Kawase, Yuichi Ogawa, Yuuki Watanabe. "Non-destructive terahertz imaging of illicit drugs using spectral fingerprints" Available at: http://www.riken.go.jp/lab-www/THz/71_k02.pdf

[61] http://www.kwicksoft.com/html/millimeter_wave.html

John then proceeds to the "Rogue DNA 9000 eGate Automated Border Control Gates" illustrated to the left[62].

The eGate instructs John to scan his passport, then his fingerprints and then look into the high resolution video camera so that facial and eye recognition can take place. John is instructed to show the front and side profiles of his face.

The process is completely automated without human intervention.

However, even with the central ICAO PKD in place, **John knows that this border control step is only as strong as the security of the public key cryptography.** If the private key of a country's root certificate authority is recovered, the electronic data can be forged. The forgery could only be detected if the data being signed is checked against a remote database (there by completely undermining the purpose of public key crypto in the MTRD project).

With the advance of quantum computing progressing strongly, there is discussion of a large scale international recall of all ICAO e-Passports that use at risk public key cryptography. This is roughly estimated at well over 80% of all issued passports at this time. The whole ICAO MTRD scheme is up for redesign, with the US pushing for a system that does not rely on public key cryptography at all.

The insider security news is that a small quantum computer probably exists "somewhere". According to sources in the defence community there have been at least 3 detected security breaches of access control systems that cannot be otherwise explained. It appears systems that are relying on the modern NSA Suite B 256-bit or smaller Elliptic Curve public key algorithms may be subverted at will and if that is the case, then it won't be long before 512-bit ECC and 1024-bit RSA and D&H algorithms will also fall. [PKE-010]

| **Classical security rating in bits** | **Factoring algorithm (RSA)** | | | **EC discrete logarithm GF(p) (ECC)** | | |
|---|---|---|---|---|---|---|
| | **$\log_2(N)$** | ≈ # qubits | **≈ time** | **$\log_2(N)$** | ≈ # qubits | **≈ time** |
| | | $2(\log_2 N)$ | $4((\log_2 N)^3)$ | | $\approx 6(\log_2 N)$ | $360((\log_2 N)^3)$ |
| **80** | **1024** | 2048 | $\mathbf{2^{32}}$ | **163** | 1000 (1200) | $\mathbf{2^{30.5}}$ |
| **112** | **2048** | 4096 | $\mathbf{2^{35}}$ | **224** | 1300 (1600) | $\mathbf{2^{31.9}}$ |
| **128** | **3072** | 6144 | $\mathbf{2^{36.7}}$ | **256** | 1500 (1800) | $\mathbf{2^{32.4}}$ |
| **256** | **15360** | 30720 | $\mathbf{2^{43.7}}$ | **512** | 2800 (3600) | $\mathbf{2^{33}}$ |

Table 1. Comparison of breaking RSA and EC using a quantum computer under equivalent classical security

As the table above illustrates[63], [64], code-breaking quantum computers easily solve the hardness of the mathematical problems that all Government standards public key crypto relies on. This cannot be fixed by increasing key lengths. Increasing the ECC key size from 163 to 512-bits results in a negligible increase in work difficulty. Simply speaking, these standards become useless and breakable in practice.

**And it is this very issue that John and other experts have been called to advise on in an international expert panel.**

---

[62] http://www.roguedna.com/egate.htm

[63] Lov K. Grover, Jaikumar Radhakrishnan, "Quantum search for multiple items using parallel queries", http://front.math.ucdavis.edu/0407.4217

[64] John Proos and Christof Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves", Quantum Information and Computation, 3 (2003), pp. 317-344. http://citeseer.ist.psu.edu/proos03shors.html

The technical but unclassified component of the report on the "state of affairs" of the US Critical Infrastructure that John is working on studies the implications of these attacks on sensitive data that has already been transmitted over these networks using these security technologies.

The problem is that all captured and archived "ciphertext" can be decrypted at will to expose the original messages. Nobody knows for certain how long the quantum computers have existed for, or how much sensitive data this attacker (or their network of associates) has access to. It can be reasonably assumed that many hackers will be discretely advertising their archived data, recorded in 'wait-and-see' attacks, and so now it is desperate scramble to try to prevent the quantum enabled attackers from systematically receiving all such data.

The first concern is that an attacker may be systematically exposing US classified data and intellectual property.

The second concern is that they may use this computer to create undetectable fake electronic identities and remotely access critical infrastructure systems to disrupt them.

One of the scenarios the U.S. is worried about is that a co-ordinated attack might simultaneously shut down the majority of power stations in the U.S and open up the dams… John wonders if this is what Mike McConnell, the Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence was thinking in his Keynote Speech at the NIST CKM Workshop (2009) when he predicted ***"that we're going to have a catastrophic event, and then we're going to be screaming."***

John knows that if the existence of the quantum computer, and the vulnerability of most existing security systems and the conclusions of this report were leaked, it would undermine the security of both the US and EU internal markets.

**END SCENARIO**

# 6. Rationale / Significance of proposed scenario

## 6.1 Why study public key cryptography?

The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to the development of e-commerce. As early as 2002 many leading security experts wrote an open letter to President Bush [65] and advised that the US ICT infrastructure was at grave risk. Today their opinion is publicly confirmed.

To quote extracts from the 9 June 2009 Keynote Speech by Vice Admiral J. Mike McConnell (USN Ret)[66] at the USA NIST National **Cryptographic Key Management** (CKM) Workshop:

"*The Internet has introduced a level of vulnerability that is unprecedented. ...*
***The nation is at strategic risk**. ... I was in a group that had an opportunity to brief then-candidate Barack Obama on security on the 2nd of September 2008. ... **President Obama is now addressing cybersecurity at the most senior level.** The Cyberspace Policy Review that was just issued attests to that. However, the Cybersecurity Initiative is primarily to protect .mil and .gov information. **Somebody should worry about .com.** Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet. ...* [CYBER-007]

***My prediction is that we're going to have a catastrophic event, and then we're going to be screaming**. We have an opportunity to address and solve Internet problems before we have that anticipated catastrophic event. **We now have the attention of the new President.** ...*

***We must design and build security into the new Internet.** We must include countries such as Russia and China in creating the design. **We have to do this because the globe could be so advantaged by this secure Internet capability and is currently so vulnerable.** Something big must be done now.*"

> – Mike McConnell is a Senior Vice President of Booz Allen Hamilton and a former Director of US National Intelligence. He previously served as Director of the US National Security Agency. President Obama has asked McConnell to continue to serve on his President's Intelligence Advisory Board (PIAB) which advises the President on all matters related to intelligence.

McConnel is stating that the status quo with regard to security is a risk that could undermine the smooth functioning of the Internal Market. McConnel is calling for action now to ensure that the integrity and security of public communications networks for 98% of the world is ensured. This 98% of the world includes Europe.

***Identity Management is an emerging focal point in both the EU and the US political agendas as a critical component of cyber security that must be improved.*** [PKI-038]

***Identity Management and Cryptographic Key Management are tightly interrelated.***

***Public key cryptography is the dominant technology used in cryptographic key management and identity management today.***

***Public key cryptography and public key infrastructures are known to be at risk.***

The RSA (Rivest-Shamir-Adleman) Algorithm is an example of the most popular Public Key Algorithm deployed in public key infrastructure. It already protects transactions worth trillions and investments worth tens of billions. The recent alternative to the RSA algorithm is another type of public key cryptography based on Elliptic Curves. Elliptic Curve Cryptography (ECC) is increasingly being used instead of RSA in new applications because it is more efficient.

---

[65] http://www.uspcd.org/letter.html

[66] Public domain image and wikipedia article on http://en.wikipedia.org/wiki/John_Michael_McConnell

Taken together the RSA and ECC public key algorithms, and the public key infrastructure that uses them, are employed in virtually all eCommerce and all eGovernment, in all eID schemes such as ePassports.

They are the dominant technology that is used TODAY to offer Identity and Key Management on the Internet. Both algorithms are vulnerable to code-breaking quantum computers.

Massive investments have been made into PKI, today the global society (including Europe) has a dependency entirely on PKI, and the dependency is growing with massive further PKI rollouts planned. [PKI-001] [PKI-029]

Examples of ongoing and planned rollouts:

a) Fraunhofer, one of the largest research institutions in Europe is just now implementing its public key based eID;

b) the UK government intends to link all UK Government departments using PKI (CIPHER Project);

c) PKI will be used in major long term (30 + year) future critical infrastructure projects such as SESAR/NextGen;

d) Galileo;

e) EC requires biometrics by law in many areas e.g. biometric ePassports, nuclear power stations (biometric systems rely on PKI); and

f) many more examples.

**What are the risks associated with this massive global dependency on Government sponsored PKI?**

- The US NIST has identified major risks with today's PKI [PKE-002] and says CKM must be part of the US and international cybersecurity initiatives (discussed in section 6.4.3.2);
- NIST has already launched a major CKM Project [PKI-005];
- the US Federal Government is now advancing new Laws that will authorise and require NIST to co-ordinate the USA's international cybersecurity collaboration to create new international cybersecurity standards [CYBER-006];
- The US NIST publishes "*We know how to handle (cryptographic) key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future*" [PKI-030]

**Risks identified by NIST and others:**

The whole world is already gambling with global stability, and is continuing to do so in its next generation major projects, by depending on a global security system:

- that has no resilience or redundancy;
- that uses one algorithm and what if it breaks!!
- no separation of powers,
- does not distribute trust across separate powers,
- any one PKI authority can go rogue and disrupt the entire global system [PKI-021];
- quantum computers expected in 9+ years according to the United States Advanced Research and Development Activity[67] (ARDA) report[68] and other experts [PKE-003].

International trade and communications needs resilience and distributed trust to prevent single points of control and potential global failure, etc. These features are absent in the current PKI infrastructure.

Large organisations and government bodies require a >5 year duration of data security and may take more than a decade (such as EMVco) to upgrade their computing systems. These organisations require known catastrophic future risks to be comprehensively addressed in their production systems well before those risks could threaten the operation and survivability of that organisation, and to protect third party sensitive data they are entrusted to manage.

---

[67] http://qist.lanl.gov/

[68] Hughes, R., Doolen, G., Awschalom, D., Caves, C., Chapman, M., Clark, R., Cory, D., DiVincenzo, D., Ekert, A., Hammel, P. C., Kwiat, P., Lloyd, S., Milburn, G., Orlando, T., Steel, D., Vazirani, U., Whaley, B., and Wineland, D. A *Quantum Information Science and Technology Roadmap, Part 1: Quantum Computation, version 2.0*. Tech. rep., Advanced Research and Development Activity, 2004. Available at http://qist.lanl.gov/pdfs/qc_roadmap.pdf

***"The next world war could taken place in cyberspace and this needs to be avoided. The conventional wars have shown us that first of all there is no winner in any war and second the best way to win a war is to avoid it in the first place. So we need to plant the seeds for a safer cyberspace together. It can only be done at a Global level because the criminal no longer needs to be on the crime scene and you can attack many places at the same time in cyberspace"*** [69]

***"There is no such thing as a superpower in cyberspace, because every individual is one superpower in itself, because it is the human brain that makes a difference in this field. This is one natural resource that is equally distributed in the world."*** [70] [CYBER-001]

– Dr. Hamdoun Toure, UN Telecommunications agency chief, 6 October 2009
*(Image from http://www.unmultimedia.org/radio/english/detail/83203.html )*

**"A decade into a new century, this old architecture is buckling under the weight of new threats. The world may no longer shudder at the prospect of war between two nuclear superpowers ... but modern technology allows a few small men with outsized rage to murder innocents on a horrific scale."**
-President Barack Obama, Nobel Peace Prize Ceremony, Oslo, 10 December 2009

**"From now on, our digital infrastructure ... will be treated as a strategic national asset ... we will develop a new comprehensive strategy to secure America's information and communications networks."**
- President Barack Obama,
Remarks by the President on securing our nation's cyber infrastructure, 29 May 2009

These issues all amount to being multiple single points of potential global catastrophic failure, pose risks to the European community in the broadest sense and to the individual citizen, and all business and the safe development of the Union; PKI with all these risks can be exploited to create cyber war where one party can hold the world to ransom, or one party can singled out as a target; and it IS impossible to reduce this global dependency on PKI overnight or to guarantee the long term safe operation of critical infrastructures programs and projects...

**Therefore ENISA needs to recommend to the EC that it launch an urgent study on these risks, and how to protect against them...**

This is a low risk step as some of these risks are now being openly discussed now in the US cybersecurity initiatives and in particular in the US NIST CKM Project.

> "*Recommendation 6:*
> *The EC should recognise that, in order to be effective,* ***it should address the global dimension and foster engagement in international discussions, as a matter of urgency****, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.*"
> – "Trust in the Information Society"
> a report of the advisory board RISEPTIS in collaboration with Think-Trust.

> "*The United States must work actively with countries around the world* ***to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations***".
> – U.S. President's Cyberspace Policy Review, 2009

---

[69] http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-itucyberspace.mp3?save

[70] http://downloads.unmultimedia.org/radio//en/ltd/mp3/2009/n-toure2.mp3?save

# 6.2 US is drafting new laws to give NIST authority to interact with international standards organisations

## House panel OKs law addressing cyberstandards

Angela Moscaritolo

November 05 2009

A draft bill approved Wednesday by a House subcommittee **would require the National Institute of Standards and Technology (NIST) to facilitate U.S. involvement in the creation of international cybersecurity standards.**

The proposed *Cybersecurity Coordination and Awareness Act*, approved Wednesday by the House Subcommittee on Technology and Innovation, would also require NIST to develop and implement a cybersecurity awareness and education program and **engage in research and development to improve identity management systems.** Also, it would amend the *Cybersecurity Research and Development Act* to update technical terms.

The proposed legislation was **drafted by staff of the House Committee on Science and Technology to implement some of the recommendations in the 60-day Cyberspace Policy Review**, a report released this May that outlines the federal government's new approach to securing cyberspace. According to the review, **international standards are needed for the investigation and prosecution of cybercrime, the approaches for network defense and response to cyberattacks.**

"The Cyberspace Policy Review recommended coordination of U.S. government representation in international cybersecurity technical standards development," Subcommittee Chairman Rep. David Wu, D-Ore., said in his opening statement Wednesday. "Currently, responsibilities are parsed among different agencies without any consistent policy. A coordinated policy will ensure that these representatives operate with the overarching need of the U.S. infrastructure in mind."

**The proposed legislation would require NIST to coordinate U.S. representation with regard to international cybersecurity standards development and create a plan to engage with international organizations to develop standards.**
**...**

**The proposed legislation now will move to the full House Committee on Science and Technology.**

http://www.scmagazineus.com/house-panel-oks-law-addressing-cyberstandards/article/157153/

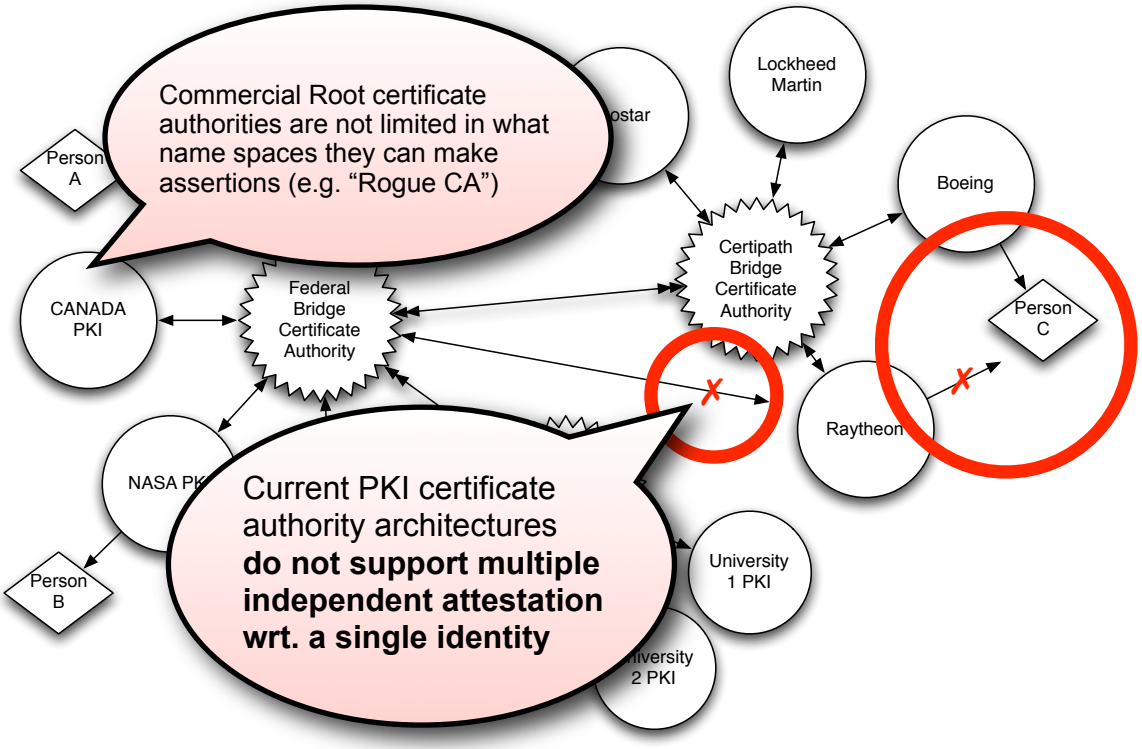
The above proposed legislation was then combined with a draft bill to address cybersecurity research and development and is now called the Cybersecurity Amendment Act of 2009. The combined draft rapidly passed the full House Committee on 4 Nov 2009. [CYBER-006]
http://www.scmagazineus.com/house-committee-passes-cyber-rd-standards-bill/article/158110/

At the time of this publication H.R. 4061 has not yet been signed into law.
See this link to check its current legal status: http://www.govtrack.us/congress/bill.xpd?bill=h111-4061.

# 6.3 High level explanations of the technical problems found in the scenario and identifying future solutions

## 6.3.1 What does a single point of trust failure in ID systems look like?

Below we illustrate the US Federal PKI Bridge and its extension into international Aerospace and Defence organisations through the Certipath bridge.




In the illustration above Person C is attested to by Boeing. If person C is a contractor, Raytheon cannot attest to the same identifier created for Person C by Boeing. Raytheon needs to assign a new identifier to Person C. Because of the lack of redundancy in the attestation process, the identifier associated with person C by Boeing can be falsified to any organisation within the federated system if Boeing's Identity Management processes are compromised. [SPOTF-003]

This problem is most visible in the next section where we talk about the Rogue Certificate Authority Attack demonstrated at the beginning of 2009.

> As an aside, we note that the identity assertions are not connected back to the authorities responsible for managing their respective name spaces. A PKI certificate for "John Smith" is not connected back to the Birth, Deaths and Marriage Registries of any nation. We have no way of validating that a "John Smith" born in London in 1950 is a real identity, and if that person is actually alive. In much the same way, if we receive a PKI certificate for a web server "MyBank.com" there is no way to validate that the certificate authority provider was permitted to make an assertion regarding "MyBank.com". We argue that it is not sufficient to validate a path back to a single root certificate authorities such as Verisign or Canada PKI. There must be multiple assertions, made from different authorities, regarding any given certificate.

The US Federal PKI bridge illustrated above to the left is an existing technology. The process of bridging through Certipath started "*about 5 years ago by the MoD and the UK Council for Electronic Business (UKCeB). At the Outset the DoD joined together with a number of Aerospace and defence companies in Europe and the U.S. The objective was to solve a number of problems concerning security of information when undertaking collaborative activities between companies, governments and individuals in a post 9/11 world.*"

TSCP now promotes a new secure email standard that is based on the use of the Federal PKI Bridge and Certipath. The proposed new standard was completed in September 2007 and is now an emerging technology in the Aerospace and Defence community.

### 6.3.2 Costs associated with security failures of a single certificate authority

We quote the section "*Risks Associated with Certification Authorities*" on page 8 of the following letter[71] by the United states Government Accountability Office:

> Certification authorities, when used to bind agencies, their employees, and others contracting with agencies for financial management transactions, are a critical component of a PKI regardless of whether a federal or commercial entity operates the certification authority because of the importance that the certification authority has in the PKI trust model. [... The] certification authority is the entity that the other users of the PKI trust to guarantee the association between a public key and a specific user or entity. Accordingly, **if the certification authority is compromised the impacts can be catastrophic to an agency's operations.** [PKI-021] **This is especially true if the compromise is not immediately detected for some period of time since improper certificates could be issued to individuals or organizations that could be used to make improper payments for one or many improper transactions.** [PKI-025]
>
> Since all parties trust the certificates issued by the certification authority, an undetected compromise may, depending on what other controls are present, result in the systems that rely on those certificates making improper payments.
>
> For example, a financial management system may rely on a contracting officer's certificate to ensure that an obligation is valid before entering it into its records. The financial management system may also rely on a certificate issued to another individual to validate that the goods and services associated with that contract have been received and accepted by the agency. Once the financial management system is notified that an invoice has been received for these goods and services, it may automatically generate a payment since (1) a valid obligation has been recorded, (2) the goods and services called for in the obligating document have been received and accepted, and (3) an invoice has been received. This is a classic automated three-way match that leading financial management systems perform to reduce the costs associated with payment processing.
>
> Simply stated, because of the trust the system places in the certificates issued by the certification authority, the system may securely transmit an improper payment based on the compromise. Once an agency has detected the compromise, it must take actions to attempt to collect any improper payments.
>
> **Even if the compromise is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of funds occurs from the compromise.** [PKI-039] As we have noted, systems must be set up to positively identify internal and external users, issue them digital certificates, and manage the exchange and verification of certificates. Should the certification authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the agency's policies and procedures.
>
> Certificates used for critical financial management applications should be issued based on split knowledge and dual control concepts and the individual's identity should be validated by personally appearing before the registration authority. **For some agencies a compromise could mean reissuing tens of thousands certificates. If an agency has integrated its PKI into its systems, a significant disruption can result if the agency has to shut down associated systems because of a compromised PKI.** For example, users may not be able to use those systems until they have received new certificates. In a non-PKI context, when one agency decided to shut down its financial management operations so that it could convert to a new system, we understand that the agency incurred over $1 million in late payment penalties as a result of the financial management system not being available. When the system has PKI, even if the agency bypasses the existing control process, the agency exposes itself to other attacks since the system is no longer using one of its critical control techniques to ensure data integrity—the PKI. Regardless of the decision, the agency is exposing itself to increased risks by (1) not processing transactions or (2) processing transactions without an adequate level of data integrity. ...
>
> **In cases where a certification authority is compromised, the agency should have recovery plans in place to mitigate the damage.** As a part of each agency's information security program which OMB

[71] Rhodes, K. A. *Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities*. Tech. Rep. GAO-04-1023R, United States Government Accountability Office, Washington, DC 20548, August 2004. Available at http://www.gao.gov/new.items/d041023r.pdf

must approve, agencies are required to have plans and procedures to ensure continuity of operations for information systems that support agency operations and assets, regardless of whether those operations and assets are managed by another agency, contractor, or other source.

**Though necessary to ensure continuity of operations, the implementation of a plan to address the compromise and recover the necessary PKI functionality may likely cause an agency to incur significant costs.**

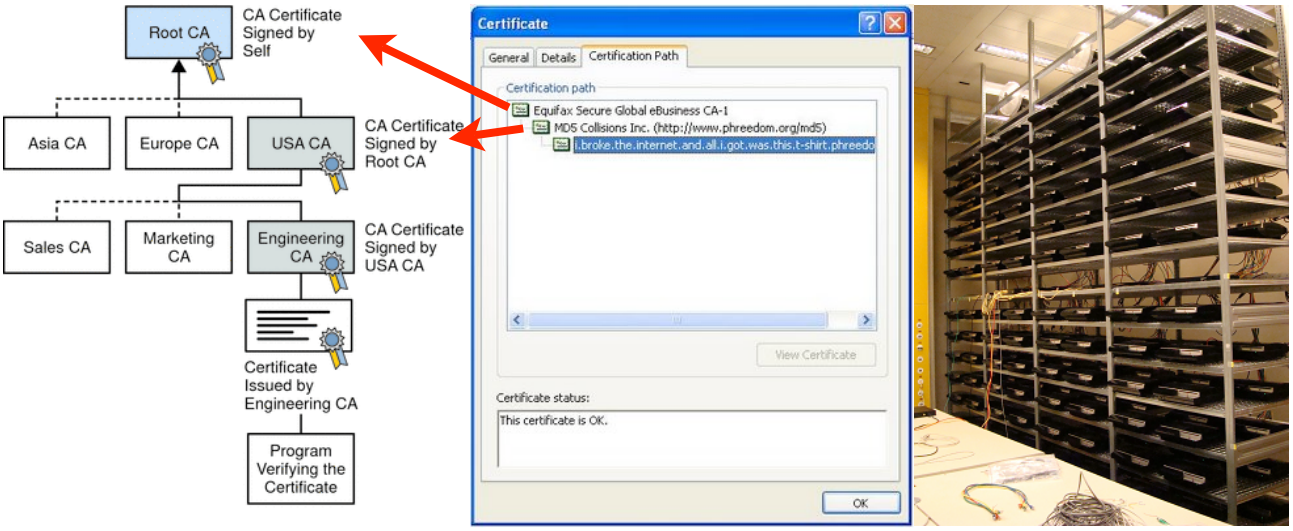
We observe that in the case of civilian PKI systems: "**Any Certificate authority can usurp a certificate issued by any other CA. The overall security is that of the least trustworthy CA**"[72]. [PKI-021] More on this below.

## 6.3.3 Has the exploitation of a single-point of trust failure in PKI Based ID systems been demonstrated in the real world?

**YES.**

Many commercial Certificate authorities, each with "GLOBAL" name-space authority, emerged. Instead of having a single point of trust failure in Kerberos like SKD systems, we now have well over 20 root certificate authorities, and **if any of those 20+ authorities goes rogue it can undermine and attack any website, in any nation, in any domain name space (.eu, .ru, .cn, .mil, …). The global civilian community can be held to ransom if one authority is for whatever reason caused to go 'rogue' and through one authority one party can wage cyber war against the majority.** [PKI-021] [PKI-024]

This vulnerability in the current public key infrastructure was clearly demonstrated with the well published MD5 rogue certificate authority attack.




*The middle panel above shows a forged Certificate, which is accepted by the Windows Operating System which states: "This certificate is OK." See MD5 Collisions Inc. (http://www.phreedom.org/md5) The right panel shows the cluster of Sony Playstation 3' devices that were used to find the MD5 collision which led to the rogue Certificate Authority, which in turn could generate fake certificates for any website on the Internet.*

The lack of end-to-end redundancy in modern PKI has led to systems that place the global civilian community at risk of abrupt and potentially catastrophic security failures/attacks at the hands of a few.

This fuels the risk of cyber crime and potentially cyber war.

---

[72] Gutmann, P. *Everything you never wanted to know about PKI but were forced to find out*. Available at http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf, page 21.

There is an obvious need for end-to-end redundancy and this should not just provide multiple independent international service providers for freedom of choice, it should also provide multiple independent national service providers to remove single points of potential catastrophic failure for national and international secure traffic. [SPOTF-003] Currently any business could be a victim of a cyber attack from any other nation which has this unrestricted power to act unilaterally.

We argue that at least in the case of international transactions (and preferably in all transactions), a citizen's or a company's privacy and security should not be subject to any single organisations/nations authority. [SPOTF-001] [SPOTF-002] [SPOTF-004] We argue for a new model that distributes trust with end-to-end redundancy for Identity Management and Cryptographic Key Management, so that an attack against an individual should require international collaboration. This type of technology can also prevent the rise of authoritarian states.

### 6.3.4 Can we defend against single points of potential trust failure?

> "*Research on new approaches to achieving security **and resiliency** in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs **and national security requirements**.*"
>
> – US 60-day Cyberspace Policy Review

**YES.** Today, modern security research agendas in the EU and US are calling for resiliency. Systems with system-wide single point of trust failures (or systems with localised single-point of trust failures that influence hundreds of thousands of users) are not resilient. Unfortunately, as illustrated above today's public key infrastructure falls into this category, including the OpenID and the U.S. Federal PKI bridge initiatives.

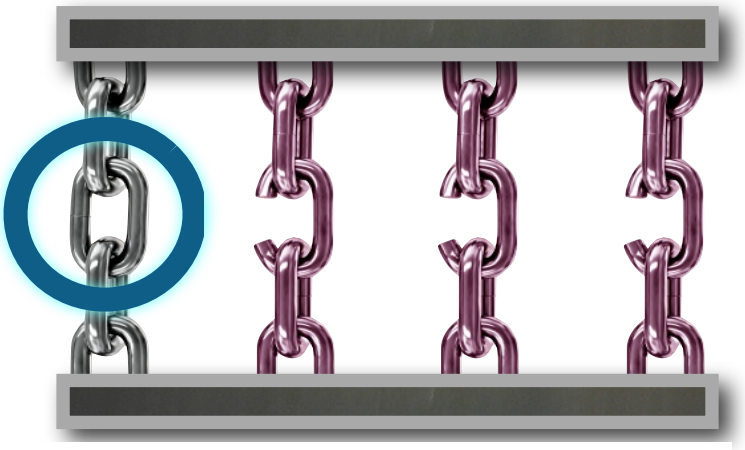
An effective way to achieve resiliency is to consider applying "separation of powers" and distributing trust across those powers by using end-to-end redundancy. This singular design factor radically influences the architecture of information processing systems including ID management, Cryptographic Key Management and all systems that must manage trust.

**Recurring theme:**
**Single point of (potentially system wide) trust failures**

Problem:

System fails catastrophically when one component fails...

Solution:



Use **End-to-End** redundancy with **independent chains of trust**...

> "*In my opinion, using redundant means to produce security is an idea that warrants more attention than it receives -- provided, of course, that the cost is reasonable.*"
>
> – Prof. Martin Hellman, co-inventor of Public Key encryption, personal correspondence, 2010

*Image of chains © iStockPhoto. Used with permission.*

### 6.3.5 What does an end-to-end secure cryptosystem look like?

Traditionally it is said that the strength of a security system is as strong as it's weakest link. Cryptographic systems typically rely on one algorithm (to perform a given function) and for example practically the entire global community gambles the continuity of the Internal/Global Market on public key cryptography. The absence of redundancy means that if that algorithm breaks then the entire global system catastrophically collapses. Furthermore, the current practice that centralises trust (for millions of users or even the entire system) into a single authority or bridging authority limits international collaboration and provides yet another single point of potential catastrophic failure. Previously such systems were preferred to optimise performance but advances in computing efficiency and reducing costs make redundancy far more cost effective today.

Former US NSA Senior Technical Director Brian Snow is on the record as stating that "*today's software security industry can be likened to a car in the 1930's. It looks good, it goes fast, but in an accident you die.*" We all employ redundancy with data backups but we have no redundancy in the cryptography or protocols in our global security systems.

Now of course publications from various US cyber initiatives (such as NIST CKM Workshop) have identified that our 'fast' PKI based key exchange systems have actually resulted in a transfer of various difficult responsibilities such as key management to the end user and the complexities involved are a hindrance to the ubiquitous take up of encryption! [PKI-040]

Reaching agreement between competing nation states and corporations about whose/which cryptographic algorithms to use creates major obstacles to international collaboration, particularly at the Government level [73]. [PKI-041] A multiply redundant international protocol could shift trust from one central point of control and single algorithm that both represent single points of potential catastrophic failure.

Existing international systems such as PKI based certificate authorities are exposed to catastrophic failure because every authority in any country has the ability to falsify any domain name or website across the globe. One nation or service provider should not have the capability to hold the international community to ransom. [PKI-025]

So how might we begin to address these above problems?

In **1976**, the three cryptographers Whitfield Diffie, Martin Hellman and Leslie Lamport wrote a paper called "Multiuser cryptographic techniques" [74], which describes a **free-to-use** ($m$-1) computationally secure symmetric key distribution (SKD) scheme that uses $m$ key distribution centres. This new idea distributed trust across $m$ different servers. As partially illustrated below, the scheme enabled two users to securely distribute $m$ different portions of a key across $m$ different paths, and reconstruct it (using a cryptographic hash to secure mix together the concatenated value of the $m$ keys) so that only the sender and receiver knew the final value, in this case $m$=4.

[73] Ballard, M. *EU crypto project SUPHICE mired in red tape*. SearchSecurity UK (Jan 2008). Available at http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1289573,00.html

[74] Diffie, W., and Hellman, M. E. Multiuser cryptographic techniques. In AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (New York, NY, USA, June 1976), ACM, pp. 109–112. Available at http://doi.acm.org/10.1145/1499799.1499815

As illustrated in the solution on the previous page, this scheme is secure while ever 1 of the *m* servers refuses to collude with the other (*m*-1) servers. This process can be implemented such that each of the servers is owned, run and maintain by a different Nation State. For example, in a hypothetical international scheme the m=6 servers could be run by the competitive states Israel, Palestine, France, Germany, Russia, China. Users of the system may have a reasonably high level of confidence that illegal collusion between the six states is unlikely to occur.

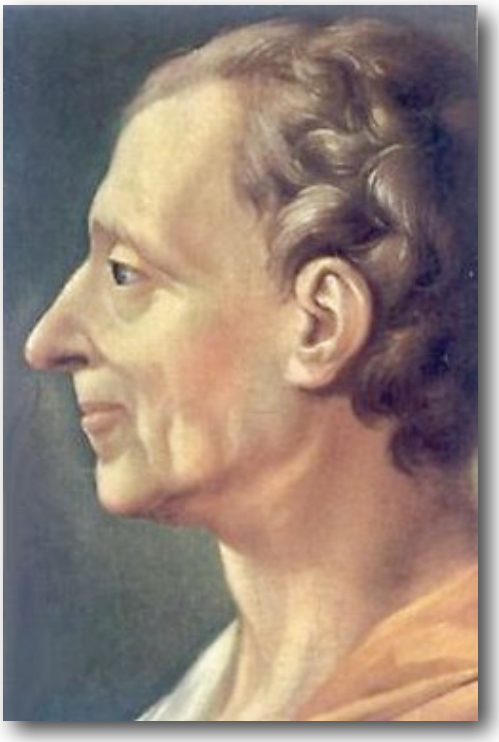
**The concept of (*m*-1) redundancy was known at the time and could have been applied to public key infrastructures when they were introduced.** Unfortunately first generation solutions were either commercially motivated with a view to dominate the market (Verisign was founded by one of the makers of RSA and not Diffie, Hellman, Merkle or Lamport), or based in a Government model of single point of top-down command and control mentality. Computer performance and cost was also issues at the time but these barriers to redundant systems can be shown to be no longer an issue. The benefits of redundancy far outweigh and minor performance reduction.

**Today the retroactive application of (*m*-1) redundancy in public key infrastructures has limited short-term value because of the known quantum computing threats to all standards based public key cryptography which would put a limited life time on this corrective action.** The effort to fix single-point-of-trust problem in an infrastructure that has known catastrophic future risks **is not cost effective**. The known mid-to-long term threats are the reason given by the NIST CKM Project Leader Elaine Barker for her call at the NIST CKM Workshop for the study of symmetric solutions that do not rely on PKI. [PKI-042]

[ Intentionally left blank ]

## 6.3.6 Are there examples of trust models that permit a relatively weak individual to trust a powerful organisation?

**YES.**



We observe that this type of (*m*-1) secure cryptosystem can be seen to be an expression of "separation of powers" and a system of "checks and balances" as articulated in the book "The Spirit of Laws"[75].

The Spirit of Laws (French: L'esprit des lois) is a treatise on political theory **first published anonymously** by Charles de Secondat, Baron de Montesquieu (public domain image illustrated to the right) in 1748. Montesquieu spent nearly twenty years researching and writing L'esprit des lois (The Spirit of the Laws), covering a wide range of topics in politics, the law, sociology, and anthropology. In this political treatise Montesquieu advocates constitutionalism and the separation of powers, the abolition of slavery, the preservation of civil liberties and the rule of law, and the idea that political and legal institutions ought to reflect the social and geographical character of each particular community. All these fundamental principles remain as valid today as they did in 1748.

It is these principles that has led to the design of Governments that permit individual citizens of limited means to have some level of trust in the integrity of their Governing system. It is arguable that these same principles can be applied to next generation security systems to provide trustworthy systems to protect the diversified interests within and across the global community.

In Book III, Part 1, "*Difference between the Nature and Principle of Government*" in comparing the various political models of Democracy, Aristocracy, Monarchism and Despotism, Charles observes:

> "*The nobles form a body, who by their prerogative, and for their own particular interest, restrain the people; it is sufficient that there are laws in being to see them executed. But easy as it may be for the body of nobles to restrain the people, it is difficult to restrain themselves. Such is the nature of this constitution, that it seems to subject the very same persons to the power of the laws, and at the same time exempt them.*"
>
> "*For it is clear that in a monarchy, where he who commands the execution of laws generally thinks himself above them, there is less need of virtue than in a popular government, where the person entrusted with the execution of the laws is sensible of his being subject to their direction*".

**We observe that the design of security systems by financial institutions, very large commercial organisations, national institutions or military institutions may be likened to the systems governed by Aristocracies. These systems tend to shift liability and provide advantage and reduced accountability to the most powerful actor[76].** [SPOTF-006]

In contrast, and in away more akin to that of popular democracy, we assert that to achieve a *virtuous* identity management/cryptographic key management/security system, the policies and procedures codified in their architecture must be designed in a balanced way to take into account the legitimate interests of all stake-holders, to ensure accountability for all stake-holders, and prevent liability shifting or the granting of advantage for commercial or national interests. [PKI-007]

---

[75] de Secondat, Charles, B. d. M. The Spirit of the Laws (Originally published anonymously in 1748). Crowder, Wark, and Payne, 1777. Available at http://socserv.mcmaster.ca/econ/ugcm/3ll3/montesquieu/spiritoflaws.pdf and http://www.constitution.org/cm/sol.htm.

[76] Anderson, R. J. Liability and computer security: Nine principles. In ESORICS '94, Springer-Verlag, pp. 231–245. Available at http://www.cl.cam.ac.uk/~rja14/Papers/liability.pdf.

## 6.3.7 What is the code-breaking quantum computing threat?

### 6.3.7.1 A Preliminary word on the code-breaking quantum computer threat

Many small quantum computers exist today in laboratories around the world. Private investors, Governments and National Security Agencies are funding further research into finding code-breaking quantum computing. [PKI-036]

Code breaking quantum computers are « understood to be an issue that is already visible as a possible future risk to network and information security » and that this threat presents a « significant risk of undermining the smooth functioning of the Internal Market » as it anticipated to undermine the security mechanisms of almost all security systems in the market.

There are NO KNOWN Public Key Distribution schemes currently considered suitable by the international community for use after the arrival of code-breaking quantum computers. This is an OPEN PROBLEM. [PKE-007]

**We advise that addressing the quantum computing threat DOES NOT require quantum key distribution.**

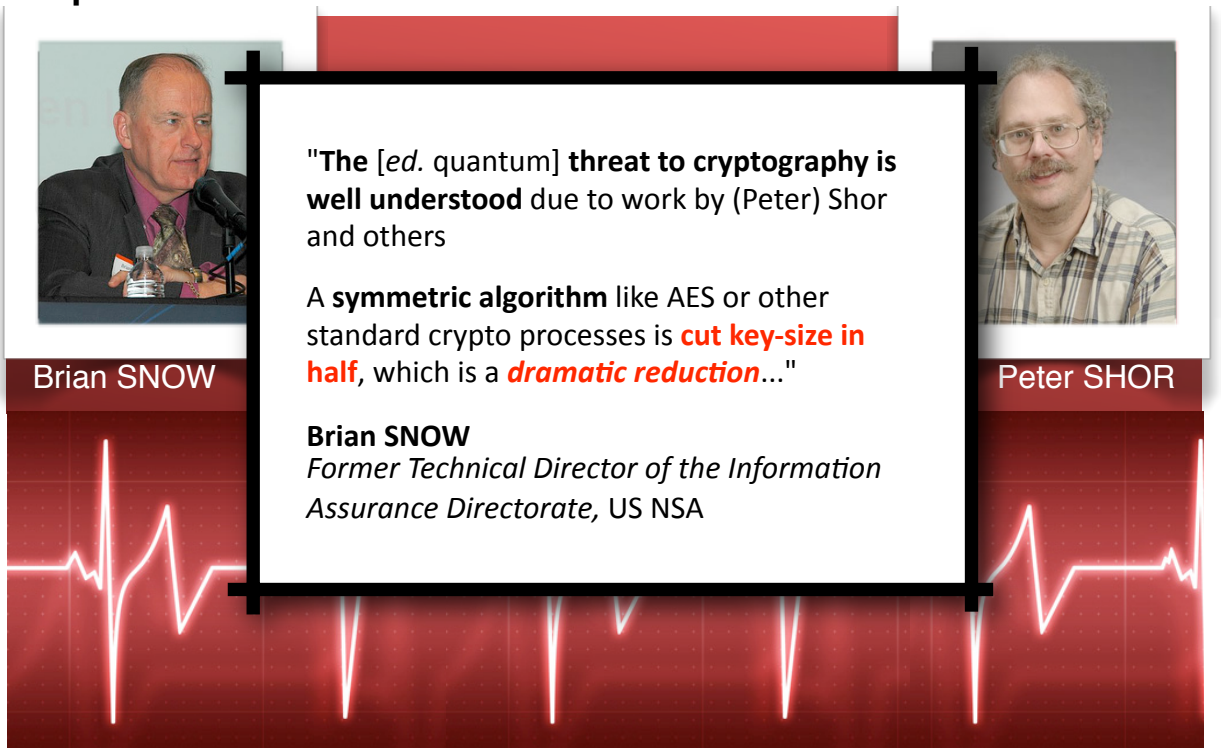
The Quantum computing threat is a long-range event (9+ years) [PKE-003] that could have devastating impact on data generated 5 years from now. Large organisations and government bodies require a >5 year duration of data security and may take more than a decade (such as EMVco) to upgrade to a protect against quantum computing threats.

The code-breaking quantum computing threat is an INDEPENDENT threat that exists OVER-AND-BEYOND the existing Single Point of Trust Failures in public key cryptosystems.

When the two different threats against public key technologies are considered together, there is doubt whether this technology is capable of ensuring the ongoing smooth functioning of the Internal Market in the mid to long-range future.

The risk of code-breaking quantum computers is particularly relevant to long-range EU funded projects such as SESARJU and national security systems.

### 6.3.7.2 What is the future threat posed by code-breaking quantum computers?




Code breaking quantum computers damage all symmetric key algorithms, but this can be compensated for in practice. In *practice* quantum computers are *just another attack* that has to be taken into account when deploying symmetric ciphers like 3DES and AES-256.

*(Image of Brian Snow: http://flickr.com/photos/farber/280651148/, http://www.flickr.com/photos/farber/, http://creativecommons.org/licenses/by-nc/2.0/) (Image of Peter Shor from: http://www-math.mit.edu/~shor/ )*

**This means that addressing the code-breaking quantum computing threat DOES NOT REQUIRE quantum key distribution because we can use NIST ciphers like the Advanced Encryption Standard with a 256-bit key.**

But for Government approved public key cryptography:


*(Image: http://www.flickr.com/photos/63251347@N00/280651254, http://www.flickr.com/photos/farber/, http://creativecommons.org/licenses/by-nc/2.0/)*

**Code breaking quantum computers are a "nightmare" for IT Security. All mainstream public key algorithms are dead. [PKE-001]**

**Professor Johannes Buchmann**:
Technische Universität Darmstadt
***World leading post quantum security expert***
*(Image: TUD)*

**Standards based public key crypto CANNOT be upgraded today:**

**"an open problem**
**... an aching problem"** [PKE-007]

**Brian Snow (2006)**
Former Technical director of the Information Assurance Directorate of the NSA.

*(Image: ZDNet.com.au)*

**Does the EU have a risk management strategy in place to manage the situation when all certification authorities are compromised due to quantum computer so the community can mitigate the damage?**

### 6.3.8 Long range significance of code-breaking quantum computers on National Security Systems

The robust and continued operation of National Security Systems and Critical Infrastructures are necessary to support the European Community. Disruption of these systems could lead to disturbances in global stability. In some cases, such as with nuclear power stations and military Physical Access Control Systems, many lives can be put at risk if the confidentiality, integrity or availability of these systems is compromised.

It is known that the ICAO MTRD (e-passport) program (used by the EU) relies on public key cryptography. The EU STORK[77] program has surveyed the national ID schemes used by member states. Many ID schemes have been identified by STORK to rely on on public key cryptography. It is known that the US Personal Identity Verification card (FIPS 201) relies on public key cryptography. It is known that biometrics are protected using at risk public key cryptography. Also according to Kathleen KRANINGER, Director of Office of Screening Coordination at the Department of Homeland Security in the United States at a presentation at CARTES 2008, access to Nuclear Facilities are secured using public key technologies.

In all these cases, the public key cryptography used is known to be at risk from Shor's quantum algorithm.

**The EU, US and China Governments are actively funding the research and development of code-breaking quantum computers.** [PKI-036] **Yet the EU, US and China continue to deploy security systems that rely on the public key cryptography that the Government funded quantum computing research initiatives are specifically trying to break.** [PKI-003]

**National intelligence organisations such as the US NSA support quantum research:**

> "*And what they do is remarkable. Since one qubit can simultaneously represent two different values, two qubits can simultaneously represent four (00, 01, 10, and 11, in binary notation); four qubits can represent 16 values; eight qubits 256 values; and so on. Even a relatively small quantum computer, one that had a few tens of thousands of qubits, could consider so many different values at once that it would be able to break all known [ed: RSA, D&H, ECC, AES-128] codes commonly used for secure Internet communication. Quantum computers might also be used for faster database searches, or to tackle hard problems that classical computers couldn't solve with all the time in the universe. My colleagues at MIT and I have been building simple quantum computers and executing quantum algorithms since 1996, as have other scientists around the world. Quantum computers work as promised. If they can be scaled up, to thousands or tens of thousands of qubits from their current size of a dozen or so, watch out!*"
>
> "***Given their power to intercept and disrupt secret communications, it is not surprising that quantum computers have the attention of various U.S. government agencies. The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one.***"
>
> – Professor Seth Lloyd of MIT 2008[78]

If just one (open or closed) code-breaking quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. [PKI-043]

At that time, it will be as though there are no confidentiality or integrity mechanisms implemented in national security and critical infrastructure systems. It will be as though no authentication of identities has been performed.

The security of the e-Passports reverts back to the security of un-chipped passports. The security of biometric e-Passports reduces to less than un-chipped passports as fake biometrics can allow users to pass through automated electronic access gates. Remote monitoring and management systems of critical infrastructure will be compromised, exposing the system to the will and caprice of malice agents. These systems may be forced to disable safety mechanisms and fail in physical ways that could harm the lives of those living near these systems.

As President Obama said at the Nobel Peace Prize Ceremony, Oslo, 10 December 2009; "*modern technology allows a few small men with outsized rage to murder innocents on a horrific scale.*"

---

[77] https://www.eid-stork.eu/

[78] http://www.signallake.com/innovation/RidingD-Wave042408.pdf

# 6.4 Background information on current and emerging US and EU research and development agendas

## 6.4.1 RISEPTIS call for a common European ID Framework

### 6.4.1.1 About RISEPTIS

Think-Trust (T-T) ( www.think-trust.eu/ ) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society ) work by providing feedback on priorities based upon input from their various activities, and input from the perspective of participants in the European ICT Framework Programme.

The T-T project includes the support of an Advisory Board, "Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society" - RISEPTIS ( http://www.think-trust.eu/riseptis.html ). RISEPTIS is a high-level advisory body in ICT research on security and trust aiming at providing visionary guidance on policy and research challenges in the field of security and trust in the Information Society. It will do so by formulating recommendations on:

- Policy environment – The development of coherent legal and administrative frameworks, operational environments, and human behaviour relating to security, privacy and confidence, in view of the technological changes leading to and arising from the future Information Society,
- Research Agenda – Future European research and development that can facilitate the creation of an Information Society that will be secure, whilst respecting freedom and privacy of its citizens, with due attention given to the ICT infrastructures, networks, services and applications.

### 6.4.1.2 Recommendations made by RISEPTIS

According to the October 2009 RISEPTIS Report[79] entitled "*Trust in the information society*": "*The trustworthiness of our increasingly digitised world is at stake.*" Furthermore: "*if citizens feel threatened, mistrustful and increasingly hesitant towards innovative applications and services, our whole society may end up being the loser.*"

The Report makes 6 recommendations, and we highlight 2 of those 6 that relate to identity management.

> **Recommendation 1:**
> The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the Information Society. The priority areas are:
>
> - Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
> - Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
> - Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
> - Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management
>
> **Recommendation 3:**
> The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity.

[79] http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html

#### 6.4.1.2 Benefits of a Unified ID framework proposed by RISEPTIS

According to RISEPTIS:

> "*Trust is at the core of social order and economic prosperity. It is the basis for economic transactions and inter-human communication. The Internet and the World Wide Web are transforming society in a fundamental way. Understanding how the mechanisms of trust can be maintained through this transformation, is of crucial importance.*"
>
> "*We see trust as a three-part relation (A trusts B to do X). Parties A and B can, in this respect, be humans, organisations, machines, systems, services or virtual entities. Trustworthiness relates to the level of trust that can be assigned to one party (B) by another party (A) to do something (X) in a given relational context.*"
>
> "*The first steps towards cooperation have already been launched by the Commission to ensure an interoperable and trustworthy ID management platform in Europe*[80]*, following joint efforts of Member States in the project STORK*[81]*.*"

RISEPTIS also quotes "The laws of identity"**:** [82]

> "*1.* ***User Control and Consent****: Technical identity systems must only reveal information identifying a user with the user's consent.*
>
> *2.* ***Minimal Disclosure for a Constrained Use****: The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.*
>
> *3.* ***Justifiable Parties****: Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*
>
> *4.* ***Directed Identity****: A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*
>
> *5.* ***Pluralism of Operators and Technologies****: A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*
>
> *6.* ***Human Integration****: The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*
>
> *7.* ***Consistent Experience Across Contexts****: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.*"

A unified ID framework is required to ensure a consistent experience across contexts.
A unified ID framework is required so that parties can accurately identify each other when required.
A unified ID framework is required to manage the control of personal data through its entire life cycle.
A unified ID framework is required to manage accountability of the actions of humans and devices.

**As illustrated in Section 6.3, an evolutionary approach to identity management using existing standards based security systems as a platform will result in deployment of identity systems that are known to be risk of single points of potential trust failure that could affect the integrity of the global system, and could entirely collapse with the advent of code breaking quantum computers.** [PKI-043]

---

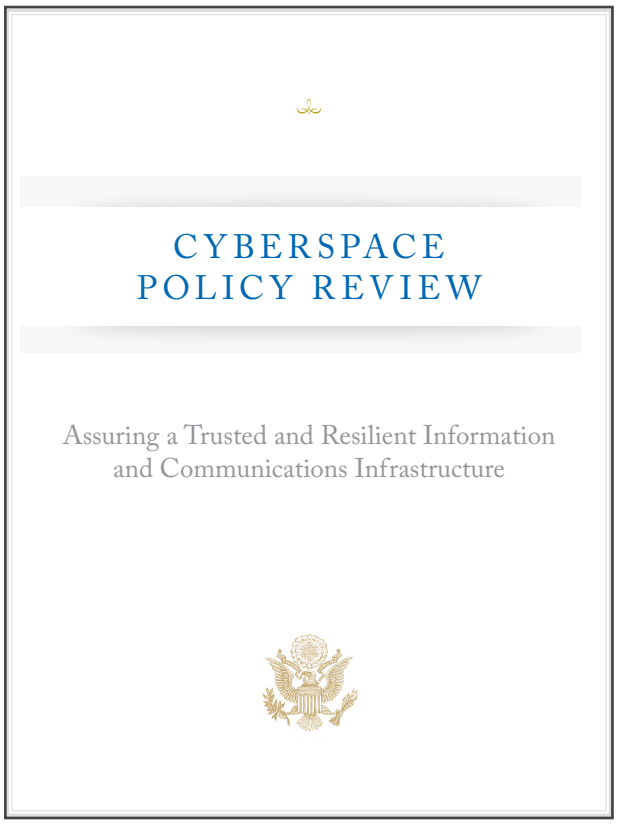
[80] COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game

[81] http://www.eid-stork.eu/

[82] See: http://www.identityblog.com

## 6.4.2 US 60-day Cyberspace Policy Review

One of U.S. President Obama's first acts was to order a 60 Day Cross Government 'clean slate' Cybersecurity Review. On the 29th of May 2009, President Obama presented the US Federal Cyberspace Policy Review Report.




The Report concluded:-

> "*Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But ... great risks threaten nations, private enterprises, and individual rights ... The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient.*"

**The report included a 10 point near term action plan.**

Point 9: "*In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.*"

Point 10: "*Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies* ***for the Nation***."

## Impact of the Cyberspace Policy Review

Two important cybersecurity activities in the United States have followed rapidly on the publication of the Cyberspace Policy Review Report.

Acting on above mentioned points 9 and 10:

- The U.S. Government's National Institute of Standards and Technology (**NIST**) held an official Cryptographic Key Management (CKM) workshop[83] to: [PKI-005]

  > "*improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support* ***a global cryptographic key management infrastructure***".
  >
  > "*There is a major need to support key management as part of the national cyber security initiative*". (June 2009)

- The U.S. Government's Networking and Information Technology Research and Development Program (**NITRD**) held the National Cyber Leap Year (NCLY) Summit on 17 to 19 August 2009 in Arlington, Virginia to find game changing ideas.

⇛ **Key management intrinsically relies on Identity management.**

[83] http://csrc.nist.gov/groups/ST/key_mgmt/

## 6.4.3 United States Cryptographic Key Management (CKM) project
[PKI-005]

### 6.4.3.1 About the National Institute of Standards and technology (NIST) CKM
Quotes from http://csrc.nist.gov/groups/ST/key_mgmt/:

"*There is a major need to support key management as part of the national cyber security initiative*". (June, 2009)

"*Cryptographic Key Management (CKM) is a fundamental part of cryptographic technology and is considered one of the most difficult aspects associated with its use. Of particular concern are the scalability of the methods used to distribute keys and the usability of these methods.* [PKI-030]

*NIST has undertaken an effort to improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure.*"

"*A CKM Workshop was held at NIST on June 8-9, 2009. Approximately 100 people participated in the Workshop at NIST on-site and approximately 90 people participated via a Webcast service. The program consisted of five keynote speakers addressing various aspects of future electronic communications, computing, and cryptography. Another twenty-five speakers addressed various technical aspects of current and future key management systems including key management policies, algorithms, distribution methods, and user control software interfaces.*"

"*The CKM workshop was initiated by the NIST Information Technology Laboratory's Computer Security Division to identify technologies that need to be developed that would allow organizations to 'leap ahead' of normal development lifecycles to vastly improve the security of future sensitive and valuable computer applications.*"

### 6.4.3.2 Requirements and Anticipated Benefits of the NIST CKM initiative
We have identified the following 5 core points articulated by senior NIST representatives at the Workshop as the reason for the CKM Project. Many of these core points are also expressed by industry at the NIST CKM Workshop.

1. **New and improved solutions that are focused on the user**
   NIST Quotes: "*user friendly*", "*easy to use*", "*plug and play*", "*user driven*"
   NIST Quote: "*It is not acceptable to only have a choice between usability with little security and security with little usability. A CKM system designer has to know the prospective user and to understand that security is not the primary task of the user. A system must be efficient, effective and understandable. There is no complex system that is secure.*"
2. **Scalable solutions**
   NIST Quote: "*We know how to handle key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future*"
   NIST Quote: "*Identity based symmetric keys may reduce the scale of symmetric key distribution problem*"
3. **Vastly improved security**
   NIST Quote: "***We're not going to accept high risks in the future Internet**, because we don't want the adversaries to have high payoffs.*" [PKI-030]
   NIST Quote: "***We need resilience against quantum computing attacks***" [PKE-002]
   NIST Quote: "*... to identify technologies that need to be developed that would allow organizations to 'leap ahead' of normal development lifecycles **to vastly improve the security** of future sensitive and valuable computer applications.*"
   NIST Quote: "*We also need key inventory control, accountability/auditing of the keys, policies for managing the keys and metadata, and safety requirements for certain applications*"
   NIST Quote: "*... must be secure, cost-effective, **fault-tolerant, and highly available***"
   NIST Quote: "*... **must look at means other than using public key-based key management systems***"
4. **Fault-tolerant, highly available**
   NIST Quote: "*Survivable key management systems*" [SPOTF-003] [SPOTF-004] [SPOTF-006]
5. **Cost-effective**
   NIST Quote: "*Executive and legislative oversight and resource allocation must be in the proper context. Expectations must be consistent with technical reality. We must work with industry, not just from the standpoint of innovation and technical expertise, but making sure the standards that result will be implemented, not just can be implemented.*"

## 6.4.4 SESARJU and NextGen

### 6.4.4.1 About SESARJU and NextGen

SESAR (Single European Sky ATM Research) http://www.eurocontrol.int/sesar/public/subsite_homepage/homepage.html marks the planned shift from radar to global positioning air traffic control amongst many other technological advances. The equivalent U.S. Next Generation Air Transportation System (NextGen), like SESAR, is a transformation of national airspace systems, including the system of airports, using 21st century technologies to ensure future safety, capacity and environmental needs are met. SESARJU and NextGen are future technologies under development today.

> « *SESAR is one of the most important research and development projects ever launched by the European Union - While the Single European Sky's regulations will provide a revised legal framework for a more efficient, performance driven, safer and greener procedures for the air traffic management, the SESAR programme will deliver technological solutions, functionalities, systems and standards which will be deployed in Europe.* »
>
> – Daniel Calleja – Director Air Transport Directorate – European Commission

Cyberspace security will be even more critical than ever before in future air traffic control. As a very expensive long term critical infrastructure project it is essential that equally long term high assurance cybersecurity is deployed to protect the massive investments required and all air travel consumers. Cybersecurity initiatives in the US are already identifying risks and future needs that must be recognised and accommodated in this project to ensure international co-operation and acceptance and to ensure that the project remains secure during its projected 30+ year serviceable life.

| Single European Sky ATM Research – Joint Undertaking | | |
|---|---|---|
| Started | 2004 | |
| Definition Phase | 2006 → 2008 | |
| **Development Phase : TODAY** | **2008 → 2016** | **€ 2.1 billion** |
| Deployment Phase | 2013 → 2025 | |
| Operational Life | **AT LEAST 30 YEARS** | |

This is not the "full" cost to the global community. According to Luc Lallouette, SESAR Programme Director for the R&D phase at Thales, the SESAR project must be applicable globally. This includes the requirement that SESAR and US NextGen initiatives must be interoperable with each other.

The US Federal Aviation Authority (FAA) is soliciting bids from companies interested in competing for NextGen support contracts with an approximate combined value of **$7 billion**, the largest award in the agency's history. Under the umbrella awards, called System Engineering 2020 (SE2020), the FAA will award as many as five separate contracts for **research and development** and **systems engineering** work that will help the agency deliver NextGen.

### 6.4.4.2 Benefits of SESARJU and NextGen

The high level goals of these two project are to:

- Increase capacity and reliability
- Improve safety and security
- Minimise the environmental impact of aviation

These are quantified as:

- An improvement in safety by a factor of 10
- Support 3 times more traffic
- Cut ATM costs by 50%
- Reduce environmental impact 10% per flight
- A 8 to 14 minutes reduction in flight time on average
- Cut air traffic management costs by 50%

These improvements to the air transportation system will be achieved by applying:

- Space-based navigation and integrated surveillance

- Digital communications
- Layered adaptive security
- Weather integrated into decision-making
- Advanced automation of Air Traffic Management
- Net-centric information access for operations

These projects are seeking to reduce the amount of manual labour required to manage air traffic. Features of the new **electronic** systems include new Trajectory Management functions, Separation Modes, Controller Tools and Safety Nets, Airspace Management supporting functions, Management Complexity tools, Queue Management and Route optimisation features. This also includes functions such as Optimized Profile Descent for aircraft seeking to land, which also requires synchronisation movement of flight in air and on ground.

The number of flights is rising rapidly and the European future economy is based heavily on tourism which relies on flights.

**The integrity and availability of flight control systems is critical to ensuring the increased capacity can be managed safely.**

These flights must be safe, otherwise the stability of the Internal Market may be damaged.

### 6.4.4.3 Known Security Risks in existing Aviation systems

**TODAY:** Under the auspices of the Air Transport Association (ATA), the aviation industry has standardised security credentials for authentication, digital signatures, and encryption. The ATA's Digital Signature Working Group (DSWG) has created an aviation industry wide public key infrastructure (PKI) standard, ATA Specification 42. Specification 42 defines a PKI certificate standard for the aviation industry, using a type of public key encryption called Elliptic Curve Cryptography. This is part of the US NSA Suite B[84] set of international security standards promoted by the America for securing up to CLASSIFIED information. ECC is known to be at risk from code-breaking quantum computers. [PKE-010]

The ATA DSWG has also established a PKI bridge under CertiPath to allow any two members of the aviation industry to exchange security credentials. The group has done extensive work on defining the exact format of the digital certificates that are used by the Certificate Authority in order to maximise interoperability and aviation functionality.

All air and ground technologies using PKI is known to be at risk. The PKI bridge is known to be at risk from single points of potential trust failure. Furthermore, the PKI technologies uses are at risk from code-breaking quantum computer attacks that experts such as Prof. Seth Lloyd (who led the team to build the first quantum computer) may arrive in approximately 9 years.

**TODAY:** System-Wide Information Management (SWIM) is an information technology program that identifies industry standards and commercially available products to ensure interoperability between National Airspace System systems. This will improve operational decision making because it will be easier to share data between systems. SESAR-WP8 is responsible for Information Management Work Package and concerns the "Intranet for ATM". SESAR-WP14 is responsible for defining the SWIM technical architecture. WP14 is required to support WP8. P14.2.2 will have to face the challenge of making the SWIM network safe and secure.

One of the known SWIM Challenges[85] is that selected military ground systems lack the required level of interoperability to provide connectivity and exchange services with the IP-based ground communications Pan-European Network Services (PENS). This type of interoperability problem between new and legacy systems will increase with the mandatory upgrade of security protocols in response to known quantum computing threats.

**If the SWIM security model takes an evolutionary approach using existing aerospace security standards based on Public Key Cryptography and Public Key Infrastructures, then the SESARJU and NextGen cryptographic security components will known to be at risk before they were developed.** [PKI-003]

---

[84] http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[85] Altran Group. *Feasibility studies on the integration of military ground and aircraft systems in the SESAR concept and architecture, "Capability gabs between military systems and SESAR"*. Executive summary, Eurocontrol, October 2008. Available at http://www.eurocontrol.int/mil/gallery/content/public/milgallery/documents/ALTRAN%20brochure%20Final_OCT08.pdf

# 7. Benefits

*Brief description of the benefits likely to emerge from this assessment report.*

## 7.1 The empowering benefits to the EU community of a comprehensive risk management report on PKI

**THE EU COMMUNITY IS MARGINALLY SECURE TODAY**

**THE EU COMMUNITY IS TOTALLY UNPREPARED FOR THE FUTURE COMPUTING TECHNOLOGIES THE EU COMMUNITY IS FUNDING AND DEVELOPING**

To the best of our knowledge, a comprehensive study of the RAMIFICATIONS of the current deployment and continued deployment of PKI systems to the stake holders in the EU community has not been performed.

### Current and immediate future (Public Key Infrastructure + Single point of trust failure)

1. It would provide an **authoritative, independent establishment and confirmation of the known weaknesses of PKI**. It would **highlight the unacceptable risks and ramifications of relying on security systems with system wide single-point-of-trust failures** that can effect the entire EU community.

2. The report would **mitigate continued non-action by calculating and articulating the risks and potential negative impacts** from the loss of security and privacy, and the roll-on negative economic impact to EU Nations and stakeholders as a result of not immediately addressing the known weaknesses posed by PKI.

   There are no known approximations of how much each stakeholder stands to lose due to a requirement or component of the system failing on account of the various known risks to PKI. [PKI-044]

   The value of a risk management report of this nature is that it can identify vulnerabilities and provide options to mitigate these vulnerabilities at their earliest stages before they become more pernicious. In addition such a study could provide a quantitative indication of reliability, performance, and/or safety of a system accounting for the criticality of each requirement as a function of one or more stakeholders' interests in that requirement[86], [87].

3. Once we are able to consider **the mean failure cost for each stakeholder** (which is the cost we expect to incur as a result of the lack of security), this loss **can be balanced against the cost of improving system security**. In this way a well-formed risk assessment report can provide an estimate of an appropriate amount to spend to address the known threats.

   The report should enable a clear return on investment for the different proposals to be calculated.

4. A risk management study **would support the existing EU calls (SecureIST) for the development of a universally acceptable hardened information technology infrastructure** that can provide MEDIUM to LONG-TERM assurances (50-to-100 years).

5. The outcome of such a study by ENISA on PKI **would feed into the Unified Identity Framework proposed by the RISEPTIS, and influence the design of security mechanisms in SESARJU development efforts** and could potentially influence every segment of the European and the electronically connected Global community.

6. The ensuing benefits from a report that **instigates change in the EU Community includes a vastly improved ICT security infrastructure for future** sensitive and valuable computer applications, systems with higher availability, greater survivability from targeted attacks, improved stability during periods of aggressive behaviour by any nation providing a certificate authority.

---

[86] Sheldon, F. T., Abercrombie, R. K., and Mili, A. Methodology for evaluating security controls based on key performance indicators and stakeholder mission. In HICSS '09: Proceedings of the 42nd Hawaii International Conference on System Sciences (Washington, DC, USA, January 2009), IEEE Computer Society, pp. 1–10. Available at http://www.csm.ornl.gov/~sheldon/public/PID736557-Methodology%20for%20Evaluating%20Security%20Controls%20Based%20on%20Key%20Performance%20Indicators%20and%20Stakeholder%20Mission.pdf

[87] Sheldon, F. T., Abercrombie, R. K., and Mili, A. Evaluating security controls based on key performance indicators and stakeholder mission. In IEEE Intelligence and Security Informatics 2009 (2009), vol. June. Slideshow available at: http://www.isiconference.org/2009/FrederickSheldon.pdf

### Short-Medium Future (Public Key encryption & Quantum Computers)

7. The additional benefits from a report which instigates change in the EU community with respect to quantum computer attacks is:
   a. **a significant reduction in the amount of intellectual property/sensitive personal data that will be at risk of exposure,**
   b. **a reduction in the severity of ICT exposure to real-time attacks against access control systems,**
   c. **the avoidance of "reworking" expensive EU funded critical infrastructure projects from known anticipated attacks, and**
   d. **improved design and reduced operational costs** by avoiding rip-and-rapidly-replace scenarios that would otherwise occur by non-action today.

   With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively affect the data security of every European citizen.

   We are not suggesting that the fundamental research into quantum computing should be reduced, or slowed, particularly as this is an internationally competitive research agenda. What we are arguing is that there has been insufficient co-ordinated effort by the EU to ensure adequate guidelines are in place and enforced within EU funded research and development programs to address the known risks. The EU call for 50-to-100 year security was displaced and ineffective in inducing change of behaviour.

   To our mind it is incomprehensible that the EU has not funded, at least to an equivalent level, the RESEARCH, DESIGN, DEVELOPMENT and DEPLOYMENT of appropriate low-risk countermeasures at the READY to ensure the global community can protect against the negative side-effects of the EU research initiatives in quantum computing.

We assert again that a risk management study on all the known weaknesses of PKI is the first step that will allow the EU community to begin making a comprehensive risk management strategy as a result of deploying and relying on PKI

## 7.2 Some issues that need to be studied regarding the presence of single point of trust failures rampant throughout modern globally deployed security systems

To the best of our knowledge, there has not been a comprehensive report identifying the security risks to the European community from the known weaknesses in the trust model of PKD systems.

A risk assessment report may consider:

*) Establishing the extent of dependence on standards based PKI.
*) The potential impacts of an identity management failure by a PKI vendor
*) The vulnerability level and potential impact of European Citizens and commercial organisations to International PKI cyberwar by a foreign Root Certificate Authority
*) A study on the prevalence of insider attacks in the ICT community as a whole, and compare that with the prevalence of insider attacks in the Root Certificate Authority community, and the ability of the providers of PKI infrastructure to adequately mitigate, detect, and repair from insider risks.

## 7.3 Some issues that need to be studied regarding the impact of quantum computing advances

To the best of our knowledge, there has not been a comprehensive report calculating the full potential impact of the arrival of quantum computing. A risk assessment report may consider:

*) The costs to the EU community with 10 years data confidentiality of sensitive data
*) The costs to the EU community with only 5 years data confidentiality
*) The costs to the EU community with only 1 year data confidentiality
*) The costs to the EU community in the face of an abrupt loss of all confidentiality
*) The costs to the EU community if 100% of the identification and authentication systems fail
*) The costs to the EU community if 50% of the identification and authentication systems fail
*) The costs to the EU community if 10% of the identification and authentication systems fail
*) The cost to study the readiness of SKD and PKD countermeasures.
*) The cost to deploy experimental next generation PKD countermeasures over a 5 year period
*) The cost to deploy experimental next generation PKD countermeasures over a 1 year period
*) The cost if the deployed experimental next generation PKD countermeasure fails due to the required globally focussed cryptanalysis finding at catastrophic weakness 5 to 10 years after its full deployment
*) The cost to develop robust SKD countermeasures, at the ready
*) The cost to deploy robust SKD countermeasures over a 5 year period
*) The cost to deploy robust SKD countermeasures over a 1 year period

# 8. Key Points in Tabular Form

In this section we have numbered 90 issues in the following 8 subjects:

- ( 6) Single Point of Trust Failure
- (10) Public Key Encryption
- (45) Public Key Infrastructure
- ( 3) PKI - Liability Shifting
- ( 2) QKD - Quantum Cryptography
- ( 9) Cyber Security / Cyber War
- (13) Biometrics
- ( 2) Panopticon

| Single Point of Trust Failure | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| SPOTF-001 | 5, 6.3.3 | Systems with SPOTF may be sought by countries seek to be a single point of control over all data exchanged to gain advantage over other countries |
| SPOTF-002 | 5, 6.3.3 | Systems with SPOTF may be sought by countries seek to be a single point of control over all data exchanged to oppressively control their citizens and prevent political dissidents |
| SPOTF-003 | 5.1, 6.3.3 | Systems need to be designed to mitigate inappropriate behaviour from occurring, for example through models that offer redundancy and distributed trust, and that enable its detection when it does occur |
| SPOTF-004 | 5.1, 6.3.3 | The majority of fraud is perpetrated by insiders. KPMG's 2007 "Profile of a Fraudster Survey," based on actual cases in Europe, the Middle East, and Africa, found that 86 percent of perpetrators in the cases studied held management positions; 60 percent of those were members of senior management or board members. Eleven percent were chief executive officers. |
| SPOTF-005 | 5.1, | "In Germany there is a system where you are not allowed to bribe a civil servant, but you are allowed to bribe a deputy. This is under German Law allowed. And the members of our parliament don't want to change it. And this is why they cannot sign the U.N. Convention against Foreign bribery. One of the very few countries that is preaching honesty and good governance everywhere in the world, but are not able to ratify the convention." **Self-regulation is difficult.** |
| SPOTF-006 | 6.3.6 | We observe that the design of security systems by financial institutions, very large commercial organisations, national institutions or military institutions may be likened to the systems governed by Aristocracies. These systems tend to shift liability and provide advantage and reduced accountability to the most powerful actors.<br><br>To prevent this, the policies and procedures codified in a security systems architecture must be designed in a balanced way to take into account the legitimate interests of all stake-holders, to ensure accountability for all stake-holders, and prevent liability shifting or the granting of advantage for commercial or national interests. |

| Public Key Encryption | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| PKE-001 | 5, 6.3.7.2 | The risks of quantum computer attacks against PKE was described as a "nightmare" as early as 2004, with the potential for countless amounts of past and present secure data being exposed and a vast array of critical systems put at operational risk |
| PKE-002 | 5, 5.1, 5.2, 6.1, 6.4.3.2 | NIST has stated "*that in the light of quantum computing CKM system designers MUST look at means other than using public key-based key management systems*", so that these systems can achieve "*resilience against quantum computing attacks*". |
| PKE-003 | 5, 6.1, 6.3.7.1 | It is a fact that some internationally recognised quantum computing experts have warned that quantum computers may grow to a size that will catastrophically break all existing deployed public key cryptography, include key exchanges and digital signatures, possibly within 10 years |
| PKE-004 | 5 | PKE is typically deployed in ways where the PKE is a brittle single line of defence that offered no resilience or possibility for recovery. |
| PKE-005 | 5 | The use of at-risk PKI encourages attackers to perform "wait-and-see" attacks in which an attacker archives encrypted ciphertext and waits a short while for the arrival of code-breaking quantum computers become available and then decrypts the archived ciphertext exposing the original content. |
| PKE-006 | 5.1, | A CKM system that meets the requirements raised by NIST during the CKM conference does not exist and needs to be developed. |
| PKE-007 | 5.2, 6.3.7.2 | There has not been significant focus in the cryptographic community to find new public key algorithms that are both classical secure and secure against quantum computers. There has not been sufficient cryptanalysis of existing proposals. This is currently considered an OPEN PROBLEM. |
| PKE-008 | 5.2 | The risk of fast-tracking a competition to pick a new public key algorithm that is both classical and post quantum secure is that this algorithm will not have had sufficient cryptanalysis to build confidence in the algorithm. It may be discovered shortly after that the solution was not secure in practice. |
| PKE-009 | 5.2 | The field of quantum computation is very new and new algorithms are still being developed that may be of reference to candidate. Many classical cryptographers are not aware of the range of existing quantum algorithms. |
| PKE-010 | 5.3, 6.4.4.3 | For every classical security rating, Elliptic Curve Cryptography (ECC) is more vulnerable than RSA/D&H public key algorithms on account of the shorter key lengths in ECC. The quantum computer does not need to have as many 'qubits' of memory and the number of quantum operations required is less. ECC may die first. ECC is promoted by the NSA Suite B algorithm for securing Classified International Government Traffic. |

| Public Key Infrastructure | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| PKI-001 | 5, 6.1 | PKI already protects transactions worth trillions and investments worth tens of billions, almost the entire globe is betting the whole shop on PKI |
| PKI-002 | 5, | PKI is a brittle single layer of defence with many known complex problems and limitations |
| PKI-003 | 5, 6.3.8, 6.4.4.3 | The global community knows that fact that Government standards based PKI could catastrophically fail within ten years, but the EU continues massive PKI rollouts even in long term (10-30+ year) critical infrastructure projects |
| PKI-004 | 5, | The extent of PKI dependency and the complexity of the issues/problems and their international scope, relate to and threaten the heart of EU principles, Market future, and stability |
| PKI-005 | 5, 6.1, 6.4.2, 6.4.3 | USA has already started a major project (NIST CKM project) to look for an alternative to public key infrastructure (symmetric key system) |
| PKI-006 | 5, | The issue of finding a replacement to PKI affects all of Europe. |
| PKI-007 | 5, 6.3.6 | A PKI replacement must be balanced so that it takes into account the legitimate interests of all stake holders and does not favour the (political, commercial, military) interests any one nation or group |
| PKI-008 | 5, | A PKI replacement must be internationally acceptable to enable inter-operability of future global ICT systems |
| PKI-009 | 5, | There is a growing massive global reliance upon public key cryptography and the momentum in both Government and commercial deployments continues to build, in spite of the known complex and potentially catastrophic risks and limitations |
| PKI-010 | 5, | When this momentum [PKI-009] and complexity is coupled with the constraints caused by the current harsh economic times, it is obvious that it is not economically viable to research, develop and trial new solutions, even to protect against potentially catastrophic known risks, unless there is already an identified buyer |
| PKI-011 | 5, | For the buyers their reticence to support the development of new solutions is compounded by the already existing problems with interoperability and standards compliance. Consequently designers will not explore alternative approaches. |
| PKI-012 | 5, | The lack of adequate research and analysis on these known risks can trigger a chain of side-stepping and liability shifting |
| PKI-013 | 5 | Europe must co-ordinate with the US efforts or, as we will show, massive fractures in the international markets can occur. |
| PKI-014 | 5, | USA has already started a major project (NIST CKM project) to look for an alternative to public key infrastructure that is resilient to quantum computer attacks |
| PKI-015 | 5.1, | Civilian PKI systems exhibit system-wide (global) single points of trust failure, that permit several parties to create cyber war or to conduct fraud. |
| PKI-016 | 5.1, | In the ICAO Machine Readable Passport scheme, there are over 183 ICAO members, and each ICAO member needs to run their own Root Certificate Authority. If a reader does not have the current certificates for the RCA, it is not possible to validate the integrity of passports from the country. Currently only 17 out of the 183 ICAO members are using a common public key directory. |

| Public Key Infrastructure | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| PKI-017 | 5.1, | The forgery of RFID MRP has been convincingly demonstrated when the self-signed certificate in the RFID chip is not validated against an external database. |
| PKI-018 | 5.1, | To improve the security of the ICAO MRTD/MRP scheme, the UK NIC uses an online registry to validate that details of the passport. The system does not rely on the passport/id card being cryptographically secure in its own right. |
| PKI-019 | 5.1, | It is difficult to promote new approaches to replace PKI, because at least in the aerospace and defence community it took 5 years just to agree how to implement an existing US Government standard for PKI. |
| PKI-020 | 5.1, | The MD5 Rogue Certificate Authority attack demonstrated that a security weakness in one Root Certificate authority can be exploited to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol. |
| PKI-021 | 5.1, 6.1, 6.3.2 | PKI is only as strong as the weakest root certificate authority, and there are more than 20 different root certificate authorities run by 20 different organisations distributed across the globe. Why was it designed this way? Who gains from this architecture? Who is put at risk by this architecture? |
| PKI-022 | 5.1, | Some prominent root certificate authorities, such as Versign, operate multiple independent root certificate authorities at different levels of quality, with the inside knowledge and comprehension that this behavior weakens the security of the global PKI. |
| PKI-023 | 5.1, | If the existing system wide single point of trust failures inherent in PKI were accurately presented and comprehended to the wider community, would this undermine confidence in eCommerce, and the acceptance of eGovernment initiatives, where the guarantee of authenticity of certificates is critical? |
| PKI-024 | 5.1, | The weakness in the architecture of PKI permits one country to force a Root Certificate Authority operating in its country to conduct cyber-war against other countries. |
| PKI-025 | 5.1, 6.3.2, 6.3.5 | The weakness in the architecture of PKI permits internal fraud to be perpetrated by one RCA against the global community. |
| PKI-026 | 5.1, | Incrementally upgrading the Existing PKI Standards would meet with great resistance from virtually all fronts. |
| PKI-027 | 5.1, | A corrective replacement to PKI must take all known factors into account, and offer a technology and service that is aligned to the welfare of the global community and not just the interests of any one commercial/national organisation |
| PKI-028 | 5.1, | "*Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation (of the United States)*" fails to take into account legitimate international interests, and fails to mitigate Militarisation, Cyberwar or designs that favour the "*National Interests*" of one Nation over another Nation. |
| PKI-029 | 5.1, 6.1 | With the massive momentum built up around the deployment of the 20th century security solutions using PKI, at-risk PKI is the main contender to protect all the latest European Government ICT initiatives and major infrastructure projects such as SESARJU. |
| PKI-030 | 5.1, 6.1, 6.4.3.1, 6.4.3.2 | NIST has identified that current PKI can reach to service millions of users. However, new CKM solutions are required to scale several magnitude more in the near future. |

| Public Key Infrastructure | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| PKI-031 | 5.1, | Due to the economic climate and entrenched interests, most security vendors would not be willing to allocate funds to the study and trial of new designs, unless there is strong Government backing. |
| PKI-032 | 5.1, | The magnitude of the issues is beyond the study and reach of any player, even a leading nation. It will be difficult for countries to make the necessary changes, for a globally appropriate system, when national self-interest is in play, and particularly for those countries militarising their cyber interests. |
| PKI-033 | 5.2 | There is institutionalised blindness on the known risks inherent to current PKI standards. |
| PKI-034 | 5.2 | Key length advisors traditionally make recommendations with explicit the explicit proviso that "code-breaking quantum computers do not become a reality in the near future". The same advisories do not provide adequate advice or alternatives for institutions seeking to address the code-breaking quantum computer threat. |
| PKI-035 | 5.2 | There are no Government standards for public key algorithms that are both classically secure and secure against quantum computers (2010). Searching for such a standard will at the very shortest require 7 years and could require 8 to 10 years. There is no guarantee an acceptable candidate would be found from this competition due to the special properties required by public key cryptography and the future anticipated quantum algorithms. |
| PKI-036 | 5.2, 6.3.7.1, 6.3.8 | The EU, US, and China Governments are funding research into code breaking quantum computers. "*The National Security Agency, which supports research in quantum computing, candidly declares that given its interest in keeping U.S. government communications secure, it is loath to see quantum computers built. On the other hand, if they can be built, then it wants to have the first one."* |
| PKI-037 | 5.3 | The design and analysis of a PKI based systems cannot generally be applied to Symmetric Key Infrastructures because they are fundamentally different approaches to the same problem. Money spent developing PKI solutions is wasted if the global community shifts to SKI in the future. |
| PKI-038 | 6.1 | Identity Management is an emerging focal point in both the EU and the US political agendas as a critical component of cyber security that must be improved.<br><br>Identity management and Cryptographic Key Management are tightly interrelated.<br><br>Public key cryptography is the dominant technology used in cryptographic key management and identity management today. |
| PKI-039 | 6.3.2 | "*Even if* [ed: *a*] *compromise* [ed: *of a certificate authority*] *is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of funds occurs from the compromise.*" … "*Should the certification authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the agency's policies and procedures.*" |
| PKI-040 | 6.3.5 | Current PKI based key exchange systems have resulted in a transfer of various difficult responsibilities such as key management to the end user and the complexities involved are a hindrance to the ubiquitous take up of encryption! |

| Public Key Infrastructure | | |
|---|---|---|
| **Issue** | **In Sections** | **Description** |
| PKI-041 | 6.3.5 | Reaching agreement between competing nation states and corporations about whose/which cryptographic algorithms to use creates major obstacles to international collaboration. The fear is that one country may be able to decrypt data from an algorithm that it promotes others to use. |
| PKI-042 | 6.3.5 | Today the retroactive application of (m-1) redundancy in public key infrastructures has limited short-term value because of the known quantum computing threats to all standards based public key cryptography which would put a limited life time on this corrective action. The effort to fix single-point-of-trust problem in an infrastructure that has known catastrophic future risks is not very cost effective. The known mid-to-long term threats are the reason given by the NIST CKM Project Leader Elaine Barker for her call at the NIST CKM Workshop for the study of symmetric solutions that do not rely on PKI. |
| PKI-043 | 6.3.8, 6.4.1.2 | If just one (open or closed) code-breaking quantum computing research project is successful, that group can provide code-breaking and forgery services to Governments, national intelligence organisations, military organisations, or terrorists anywhere in the world. |
| PKI-044 | 7.1 | There are no known approximations of how much each stakeholder stands to lose due to a requirement or component of the system failing on account of the various known risks to PKI. |
| PKI-045 | 7.1 | With regard to PKI and quantum computing, in our opinion, it is a risky strategy for the EU to aggressively fund codebreaking research and development without adequately preparing for the arrival of these machines. This is particularly the case given quantum computing research has the potential to negatively affect the data security of every European citizen. |

| PKI - Liability Shifting | | |
|---|---|---|
| **Issue** | **In Sections** | **Description** |
| PKILS-001 | 5.2 | The scale of the problem with PKI will make it easy for each group to shift liability away from itself. The Standards bodies can say that the cryptographic community had not focussed sufficiently on providing them candidate algorithms. The Cryptographic algorithm designs can argue that there was not sufficient confidence on when quantum computers will arrive, so it wasn't worth their time studying. The organisations implementing cryptography can assert they simply followed Government Standards to the letter and could not be responsible if the standards body didn't provide sufficiently secure algorithms and infrastructure. … and so on. |
| PKILS-002 | 5.2 | There is the risk that if a comprehensive solution is not designed and proposed BEFORE the urgency of quantum computer attacks becomes critical, the community may be forced to rapidly select a plug-and-play public key alternative of unknown security. This may result in a global replacement of an algorithm that might be no more secure (or even less secure) than the algorithms they replaced. |
| PKILS-003 | 5.3 | Security teams may try to shift the responsibility of making difficult choice between a low-cost risky upgrade to an experimental PKI solution, and a more expensive upgrade to a robust Symmetric Key Infrastructure solution. Given two "short-term secure solutions", one vastly cheaper than the other, investors and management are inclined to go with the cheaper solution. This scneario does not need to be occur if the security issues are addressed now, rather than mid-way through a project. |

| QKD - Quantum Cryptography | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| QKD-001 | 5.1 | An attack recently eavesdropped 100% of a quantum cryptographic key due to weakness due to a photon detector vulnerability. |
| QKD-002 | 5.1 | SECOQC advises that current QKD networks are not suitable for use as large scale public networks such as the Internet. |

| Cyber Security / Cyber War | | |
|---|---|---|
| **Issue Number** | **In Sections** | **Description** |
| CYBER-001 | 5, 6.1 | According to the United Nations Telecommunication Chief's warning in 2009 the risk of the next world war being in cyber space. "*There is no such thing as a superpower in cyberspace, because every individual is one superpower in itself, because it is the human brain that makes a difference in this field. This is one natural resource that is equally distributed in the world.*" |
| CYBER-002 | 5.1 | The Internet is becoming increasingly Militarised by Governments. The U.S. Air Force is advocating more Cyber War attacks by American Cyber War organizations. |
| CYBER-003 | | The U.S. has already conducted cyberwar in IRAQ. Attacks exploited the mobile phone network. |
| CYBER-004 | 5.1 | The U.S. Cybersecurity Initiative is primarily to protect .mil and .gov information. Somebody should worry about .com. Ninety eight percent (98%) of the world is .com or .edu or .org or a foreign segment of the global internet. |
| CYBER-005 | 5.1 | What the cost will be to support the necessary research and development, and globally coordinated efforts for that remaining 98%, and what role Governments, United Nations, and the Organisation for Economic Co-operation and Development will play |
| CYBER-006 | 5.1, 6.1, 6.2 | There is new legislation being rapidly advanced in the USA that would require the US NIST to lead the USA's international cybersecurity standards |
| CYBER-007 | 5.1 | New Identity Management and cyberspace security standards may become weapons of coercion and not tools of global social empowerment for the other 98% of the world's population.<br><br>Without international participation at the highest level, without a system of checks and balances, global identity management issues may not be addressed in a way that is appropriate to the European or global civilian community. |
| CYBER-008 | 5.2 | Fixing security issues after deployment is extremely expensive and may not work comprehensively, such as with the deployment of the Internet. |
| CYBER-009 | 5.2 | When security is not mandatory in ICT systems, cryptography is used as a pricing differential, which results it the bulk of systems not deployed with security. Then we have the situation today, where everyone begins to panic about insecurities which could have been prevented. Panic shifts quickly to offensive militarisation to 'deter' attacks, which leads to cyber war. |

| Biometrics | | |
|---|---|---|
| **Issue** | **In Sections** | **Description** |
| BIO-001 | 5.1, | The set of biometrics captured for the UK Identity card is the same set of biometrics that they capture when enrolling convicted criminals into prison |
| BIO-002 | 5.1, | Do we created a government controlled Panopticon when we combine the biometrics of every citizen with CCTV and other systems? |
| BIO-003 | 5.1, | Biometric data does not change significantly over the life time of an individual, however the cryptographic mechanisms to protect biometrics are not rated for 100 year security. |
| BIO-004 | 5.1, | Algorithms that are known to be at risk of catastrophic security failure after 10 years are used to protect biometrics. |
| BIO-005 | 5.1, | The United States is trading biometrics with other countries. According to one source, approximately 25 countries have bilateral biometric trading agreements in place with the United States. |
| BIO-006 | 5.1, | India has explicitly declared it wants to capture the biometrics of every citizen. The UK appears to be going in this direction with the National Identity Card program. |
| BIO-007 | 5.1, | The United States captures the biometrics of everyone entering the country. |
| BIO-008 | 5.1, | EU citizens are having their biometrics permanently captured and used or passed on in ways that they can not audit, or control. EU Citizens have lost self-determination over their captured biometrics. |
| BIO-009 | 5.1, | Biometric data may be used in identity fraud attacks. |
| BIO-010 | 5.1, | Biometric data is being managed by Government systems and Government approved protocols. These systems are using brittle cryptographic protections that are vulnerable to single point of trust failures. Furthermore, Governments have a bad track record of protecting sensitive data. |
| BIO-011 | 5.1, | Newly acquired biometric information can be used to retro-actively track an individual. |
| BIO-012 | 5.1, | Biometric enabled passports and ID cards may need to be valid for 10 years, even though the security of the cryptography in that document may fail within that time due to code breaking quantum computer attacks. |
| BIO-013 | 5.1, | PKI encrypted biometrics may be exploited within the life-time of their owner, even if those biometrics are later encrypted using stronger cryptography. |

| Panopticon | | |
|---|---|---|
| **Issue** | **In Sections** | **Description** |
| PAN-001 | 5.1 | The definition of “a dangerous person”, or “terrorist”, is very flexible and open to different political interpretation. |
| PAN-002 | 5.1 | By correlating mobile phone cell data in combination with extensive CCTV networks and facial recognition systems supplied with civilian biometric data, it may not be possible, in the near term future, for anyone to move outdoors in city areas with any privacy from Governments |

**Before the**
**DEPARTMENT OF COMMERCE**
**Internet Policy Task Force**

| | | |
|---|---|---|
| In the Matter of | ) | |
| Information Privacy and | ) | Docket No. 100402174-0175-01 |
| Innovation in the Internet Economy | ) | |

# COMMENTS OF TECHAMERICA

Chris Wilson, Esq.
TECHAMERICA
601 Pennsylvania Ave, NW
North Building, Suite 600
Washington, D.C. 20004
(202) 682-4451

June 14, 2010

TechAmerica hereby submits these comments to the Department of Commerce ("Department"). TechAmerica's members have a vested interest in the success and future of the Internet and TechAmerica is pleased to be able to file comments on their behalf in this proceeding.[1]

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association (AeA), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics and Information Association (GEIA).

TechAmerica's members include: manufacturers and suppliers of broadband networks and equipment; consumer electronics companies; ICT hardware companies; software and application providers; systems integrators; Internet and e-commerce companies; Internet service providers; information technology government contractors; and information technology consulting and sourcing companies.

TechAmerica welcomes this opportunity to provide the Department's Internet Policy Task Force with a viewpoint shared by such a diverse membership.

**The U.S. Privacy Framework**

TechAmerica is pleased to provide the Department with some important concepts that its Internet Policy Task Force must consider in its deliberations and its external advocacy.

First, any privacy regulatory framework adopted in the United States must be technologically neutral. Technology neutrality ensures that any prospective regulatory model will provide sufficient flexibility to allow Internet-related technology companies the ability to innovate and respond effectively to consumer needs into the future. In that vein, TechAmerica does not believe there is a "one-size-fits-all" approach to privacy policy. Second, we understand that "customary notice and choice" may be outdated in certain contexts, but TechAmerica believes that notice and choice should still maintain a foothold in any comprehensive privacy policy. In addition, TechAmerica believes that additional privacy models can and should be considered to complement the traditional notice and choice system. Indeed, as Web-based services become more interactive and information-intensive, some form of a "use-based" model, for example, could very well be applicable. Simply put, TechAmerica recognizes that the dynamic and ever-changing Internet economy and infrastructure requires an equally flexible and dynamic privacy regime.

Further, as the Department reviews various privacy models and their efficacy in the future, it should strongly consider, and encourage, two core guiding privacy principles currently at work. The first, "accountability," is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation. The second, "privacy by design,"

asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation.

"Accountability" requires an organization to make responsible, disciplined decisions regarding privacy and security. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles that have privacy and security integrated as foundational elements. Several companies are currently committing significant resources to "being accountable" in this way now.

With regard to "privacy by design," the principle should encourage the implementation of accountability processes in the development of technologies. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a "privacy by design" accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

TechAmerica requests that the Department, in its report, encourage organizations to take steps towards accountability and to ensure that privacy is included as a principle in product and service development processes.

**International Privacy Laws and Regulations**

As the Department is well aware, there are a variety of foreign laws governing how companies collect, use, and disseminate consumer data. Unfortunately, this matrix of laws has served as an unnecessary, if not intentional, barrier to effective trade in the digital economy. For example, the European Union's data privacy laws, in contrast to the U.S.'s more flexible standards, have proven to be not only burdensome in compliance but also inefficient in implementation.

For example, as defined by the European Data Protection Directive 1995, "personal data" is data that relates to or can identify a living individual. This threshold for protection, based on mere identity and rooted in the jurisdiction of "collection," contrasts sharply with the privacy laws of some other countries, such as in the U.S., where data use and the risks attributable to misuse is the basis for sector-specific regulations.

To be sure, however, TechAmerica and its member companies applaud the Department's efforts to mitigate the impact of the EU privacy laws, especially the Department's role in negotiating the U.S.-EU Safe Harbor Framework. This Framework has facilitated the rapid development of a global Internet economy.

In addition to the U.S.-EU Safe Harbor Framework, the APEC Privacy Framework has been extremely helpful for U.S. technology companies seeking to do business globally. TechAmerica commends the leadership of the Department on the

development of the APEC Cross Border Privacy Rules (CBPR). Since the APEC Privacy Framework was endorsed by APEC Ministers in 2005, the Department, in conjunction with other U.S. agencies, has been instrumental in working with its counterparts across APEC economies on a series of Data Privacy Pathfinder projects to develop a system in the APEC region that ensures accountable cross-border flows of personal information for the protection of consumers while facilitating business access to the benefits of electronic commerce. TechAmerica member companies are of the view that the APEC Privacy Framework and the Data Privacy Pathfinder projects represent an important step forward in privacy protection in the 21 APEC economies in which new and flexible approaches to accountability and compliance are envisioned.

Further, notably, we are thankful that the Department has striven to include opportunities for the business community to engage and provide input throughout the APEC CBPR development process. This collaborative effort has been essential given the pace of innovation in electronic commerce. The Pathfinder projects enable a system that allows businesses to create their own CBPRs and consumers to rely upon 'accountability agents,' as well as regulators, in the APEC region to make sure businesses are held accountable to their privacy promises. This self-regulatory "trustmark" model has proven effective in a number of economies to date. As the APEC Privacy Framework demonstrated, a voluntary set of common and broadly-applicable principles can coincide with self-regulation and a risk-based approach to compliance obligations and enforcement.

With the APEC success in mind, TechAmerica believes a strong consistent global framework is needed in order for the digital economy to truly flourish. Without

such a harmonized framework, technology companies will be forced to make difficult decisions as to whether or not to do business in certain countries for fear of being held civilly or even criminally liable for actions that would otherwise be lawful in the U.S. and elsewhere. Such uncertainty would inevitably lead to less investment and, subsequently, less economic growth. Considering how interconnected the global economy already is, the repercussions of such choices will be felt throughout the world.

This global interconnection is especially true with regard to cloud computing, for example. As cloud computing continues to grow, so too will the amount of data crossing national borders. If divergent claims to jurisdiction over user content remain, then it becomes quite difficult for providers to manage their legal obligations and their global technology operations while at the same time protect their consumers.

**The Role of Government/Commerce Department**

The Department, with its history of working with the global community on privacy matters, is uniquely positioned to lead the way in developing a consistent privacy model. TechAmerica stands ready to assist the Department as it moves forward in this regard, especially as the U.S. hosts APEC next year.

Further, one factor often cited by data protection regulators as a weak point internationally of the U.S. privacy regime is the lack of a central U.S. authority on privacy issues. As the Department gathers input on whether or how to strengthen our own regime in the U.S., it would be helpful for U.S. positioning on privacy to receive greater and more focused representation internationally by the U.S. government. International coordination will continue to be key to free flows of information and deployment of new and innovative services. Whether the U.S. chooses to develop new

broadly-applicable privacy rules or revisits the application and scope of existing privacy laws, there are four key principles that should help guide this effort:

- **Flexible Compliance Options** – Continue to favor self-regulatory approaches, but where rules are deemed necessary, enable authorities to approve appropriate industry and NGO-developed compliance contracts, codes and procedures;
- **Relevant Risks** – Where rules are necessary, they must focus on the risk attributable to misuse of certain types of data in setting the level of protection for that data;
- **Consistent Implementation** – Seek a consistent approach to principles that put the onus on data users to take accountability – not added protections that frustrate the possibility of cross-border compliance;
- **Consultation** – Industry understands that its role in protecting privacy supports its mission to achieve and retain customers, and thus, industry consultation at all levels of this continuing dialogue will improve compliance and enforcement.

Further coordination among governmental and non-governmental entities domestically is also an area where the Department can be helpful. For example, the Federal Government's Information Security and Privacy Advisory Board and the President's National Security Telecommunications Advisory Committee each released reports last year outlining important information security and management issues deserving of fuller consideration, including how to treat metadata, cookies, and other tags that may be shared. These efforts, as well as the efforts of non-governmental

entities, such as the Kantara Initiative, and other governmental efforts, such as the White House's National Strategy for Secure Online Transactions, illustrate how scattered and varied the review of information security and privacy practices is throughout the country. As much as possible, these efforts should be coordinated and the Department should assist in this regard.

**Conclusion**

TechAmerica thanks the Department for creating its Internet Policy Task Force. A committed and focused effort by the Department with regard to the development of the digital economy is welcomed and appreciated. The Department can and must play a key role in developing a unified privacy regime. Consumer privacy protection will require a multi-faceted solution that includes industry commitments and government involvement. To be sure, privacy is vitally important to not just consumers, but to Internet technology companies as well. Entire business models are built on the trust established between a company and its customers. Industry principles such as transparency, user control, and security in Internet services should and must remain at the foundation of any privacy model going forward. TechAmerica looks forward to working with the Department in the months and years ahead as it plays a role in achieving a comprehensive and flexible privacy plan.

---

[1] *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 FED. REG. 21226 (April 23, 2010).

**Before the**
**National Telecommunications and Information Administration**
**Washington, DC 20230**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0175-01 |
| | ) | |
| | ) | |
| | ) | |
| | ) | |
| | ) | |
| | ) | |

To: National Telecommunications and Information Administration

# COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President, Government Affairs
**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

## TABLE OF CONTENTS

Before the
National Telecommunications and Information Administration
Washington, DC 20230

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0175-01 |
| | ) | |
| | ) | |
| | ) | |
| | ) | |
| | ) | |
| | ) | |

To: National Telecommunications and Information Administration

**COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

The Telecommunications Industry Association ("TIA") hereby submits comments to the National Telecommunications and Information Administration ("NTIA") in the above-captioned proceeding. TIA, on behalf of its members, appreciates NTIA's interest in the important area of the interplay between information privacy and innovation in the Internet economy. TIA believes that an appropriate privacy framework balances consumer privacy concerns with the consumer benefits arising from technological innovation and business model flexibility in communications and Internet commerce. Thus, as explained below, TIA supports the privacy framework now in place in the United States, which focuses on notice, choice, appropriate data protection, and robust enforcement. To the extent NTIA believes that additional protections are required, it should work to facilitate the expansion of self-regulatory regimes, which have already proven successful in structuring providers' conduct, rather than supporting new prescriptive requirements, which would threaten innovation and undermine consumer welfare. Moreover, any modifications to the existing privacy framework must be technology-neutral, focusing on how information is used and protected, rather than the specific means by which it is collected and used.

TIA represents the global information and communications technology ("ICT") industry through standards development, advocacy, trade shows, business opportunities, market intelligence and world-wide environmental regulatory analysis. Its 600 member companies manufacture or supply the products and services used in the provision of broadband and broadband-enabled applications. Since 1924, TIA has enhanced the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market,

including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment.

## Summary

Effective privacy protections are important for consumers and the ICT industry, particularly in an era of rapid technological change. Consumers will only adopt new information and communications technologies if they trust that their personal privacy preferences will be respected and that their personal information will remain secure. Innovations in information use and technology, coupled with effective privacy protections, have greatly enriched consumer choices and experiences and benefitted our economy.

There is an extensive body of state and federal law to safeguard consumer privacy, including Section 5 of the Federal Trade Commission Act. This provides a strong but flexible privacy framework based on consumer notice and choice, as well as reasonable security measures to protect consumers' personal information from unauthorized access or release. Certain types of information are subject to additional protections, such as those set out in the Communications Act of 1934, as Amended ("Communications Act") and the Health Insurance Portability and Accountability Act ("HIPAA"). By accounting for consumer demands, sensitivity of information, and other relevant factors, this existing framework has proven effective in addressing privacy challenges arising from innovations in information use and technology.

Industry has strong incentives to protect consumer information, particularly sensitive consumer information, and thus self-regulation has been an effective complement to governmental action, particularly for new and evolving technologies. Examples of self-regulation include the Mobile Marketing Association Code of Conduct, the Better Business Bureau Self-Regulatory Principles for Online Behavioral Advertising, and CTIA-The Wireless Association Best Practices and Guidelines for Location-Based Services. Industry members are well positioned to understand technological and business needs and to propose solutions that protect consumer privacy while allowing market and technical innovations to continue.

Appropriate collection, sharing, and use of consumer information provide many benefits to industry, the economy, and consumers. It is thus vitally important that privacy protections maintain flexibility for different business models and technologies to ensure that these benefits continue. Businesses may collect and use information to provide more convenient services or to improve products or customer service. Information about consumers may also be used for marketing purposes, which permits more targeted marketing and also underwrites the provision of free content and services on the Internet and other channels thereby making services more affordable for all consumers.

Of course, the collection, sharing, and use of consumer information also raise concerns about privacy. Consumers are concerned that their personal data may be collected without their knowledge, used in a way they do not expect or desire, or misused to invade their privacy. They may also be placed at risk of harms such as identity theft if their personal information is not secured adequately. Privacy protections should provide users clear notice about what information will be collected, how it will be used, and by whom, as well as reasonable security for their personal information. These protections should not, however, replace consumers' *own*

choices, which may favor innovations that provide convenience, speed, or easier communication. Such protections also should not dictate which technologies may be used, as long as consumers receive appropriate notice and can exercise choice about how these technologies collect, use, and share their information.

Finally, privacy protections should not impose onerous requirements on business or consumers, which may retard the development or uptake of new technologies and services to the detriment of consumers and our economy. For example, although the European Privacy Directive 95/46/EC has benefits in terms of applying a unified approach that reduces confusion about which standards apply, it is also highly bureaucratic and its burdens may outweigh the privacy benefits for individuals. By contrast, the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework and the Cross Border Privacy Rules reflect an approach to privacy regulation that protects privacy while preserving the flexibility necessary for innovation. TIA members applaud the Department of Commerce's leading role in the APEC process and the development of these Rules.

## Discussion

## I. TIA Members Support Privacy Protections for Consumers.

Industry, including the ICT industry, needs information about customers' needs and interests to create and offer products and services that best meet those needs and interests – services and products which, in turn, produce substantial benefits for consumers. As the ability to collect, use, and store information about consumers has increased, however, so have consumers' concerns about privacy. It is in the interest of the ICT industry to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information in exchange for benefits such as greater convenience, increased safety, or enhanced communications.

### a. Consumer Privacy is Important to the Adoption of Technological Advances.

The use of consumer information to design products and improve services, as well as to fund free services and content, has produced substantial benefits for consumers.[1] Consumers justifiably

[1] *See, e.g.*, Jon Leibowitz, Chairman, Fed. Trade Comm'n, Keynote Address at the National Cable & Telecommunications Association Cable Show 2010 (May 12, 2010) (stating that targeted advertising is "usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects"); *see also* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 112 (2008) ("It is not obvious, however, that better information about consumer behavior increases the amount of marketing. It clearly leads to more targeted
(continued on next page)

have concerns, however, about how their data is collected, stored, and used.[2] If consumers do not trust that new technologies and business models will respect their privacy preferences or keep their sensitive information secure, however, they will be hesitant to use such technologies, thus foregoing benefits for themselves and ultimately slowing innovation.[3] It is thus in the interest of the ICT industry to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information to receive benefits such as greater convenience, increased safety, or enhanced communications.[4]

**b. TIA Members Support the Current Privacy Framework Based on Notice, Choice, and Data Security, which, Coupled with Robust Enforcement, will continue to be Effective in Protecting Consumer Privacy.**

There is no single source of privacy law in the U.S. The Federal Communications Commission ("FCC") administers Consumer Proprietary Network Information ("CPNI") regulations[5] that protect certain subscriber information held by communications providers and Congress has also enacted sector-specific laws governing sensitive personal data, such as HIPAA's protections for health records.[6] The FTC, however, provides general oversight for much of the collection, use, and sharing of consumer information for most businesses through application of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices.[7] The FTC's longstanding approach rests primarily on efforts to ensure (1) that consumers are afforded notice of what

---

marketing -- there is a higher probability that the consumer will find the message relevant if information about past behavior helps to predict preferences.").

[2] *See* Fed. Trade Comm'n Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology*, at 1 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (discussing consumer concerns over personal data collection).

[3] *See, e.g.*, Ctr. for Democracy & Tech., *Health Information Privacy: Current Trends, Future Opportunities*, at 1 (Mar. 2010), *available at* http://www.cdt.org/files/pdfs/FTCRoundtableTestimony.pdf (citing survey data suggesting that consumers who do not trust privacy and security protections for electronic health records will not use them and noting that this may affect individual patient care and overall public health).

[4] *See, e.g., Data Accountability Act and Informed P2P User Act: Hearing on H.R. 2221 and H.R. 3224, Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (May 5, 2009) (statement of Federal Trade Commission) ( "If companies do not protect the sensitive consumer information that they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace.").

[5] *See* 47 U.S.C. § 222 (establishing duty of every telecommunications carrier to protect confidentiality of customers' CPNI).

[6] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264(c)(2), 110 Stat. 2033–34 (1996); Social Security Act, 42 U.S.C. § 1320d-2 (2009).

[7] Federal Trade Commission Act, 15 U.S.C. § 45.

information is collected about them and how it will be used (notice), (2) that they can choose whether to allow collection and use of their personal information (choice), and (3) that the entity that collects personal consumer information uses reasonable measures to secure it against accidental or unauthorized access or release (security).

TIA members support this framework of notice, choice, and security. Consumers should be able to access clear descriptions of the types of personal data collected and the purpose for which that data is being used and to exercise choice about whether to permit their personal information to be collected and used as described. In addition, any company that collects and maintains such information must take reasonable security measures to guard against unauthorized access to it. Finally, robust enforcement of privacy protections is very much in the interest of the ICT industry to guard against consumers losing confidence in the market and failing to embrace new communications technology. In fact, the self-regulatory programs that TIA members support that are described in the following subsection all use a framework based on notice, choice, and security backed up by enforcement to ensure accountability.

### c. Where Additional Protections are Necessary, Self-Regulatory Regimes are an Effective and Flexible Complement to Government Regulation.

Industry members are necessarily sensitive to consumers' demands. They are also well positioned to understand providers' technological and business needs and to propose privacy-protective solutions that offer an effective sector-wide response while allowing market and technical innovations to continue.[8] Given the providers' interest in marrying strong privacy protections with consumer choice and innovation, self-regulatory regimes are a powerful tool for use in developing appropriate privacy norms. Self-regulation also offers greater flexibility in responding promptly to new concerns to better meet emerging threats.

Accordingly, the ICT industry has participated in a variety of self-regulatory efforts to address privacy concerns and enhance consumer confidence in new technologies and business models. For example, many TIA members follow the Mobile Marketing Association Code of Conduct, which requires companies to provide consumers notice about how their information will be used; choice (based on obtaining customer consent, offering customization by consumers, and requiring constraint by marketers); and security for consumer information.[9] TIA Members have also participated in the development of the cross-industry Self-Regulatory Principles for Online Behavioral Advertising issued by the Better Business Bureau and leading advertising industry associations.[10] The Principles aim to provide consumers greater transparency, choice, and

---

[8] *See, e.g.*, Leibowitz, *supra* note 1 ("We know that those of you in the industry are much better positioned to understand the threats to consumer privacy – and to put in place the technical safeguards that I believe we all want.").

[9] Mobile Mktg. Ass'n, *Global Code of Conduct* (July 2008), *available at* http://mmaglobal.com/codeofconduct.pdf.

[10] Better Business Bureau et al., *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.bbb.org/us/Storage/0/Shared%20Documents/online-ad-

(continued on next page)

control regarding the collection and use of their information for online behavioral advertising purposes. In addition, CTIA has also promulgated Best Practices and Guidelines for Location-Based Services, which are based on the fundamental principles of user notice and consent regarding their location information and which aim to facilitate consumer use of new and exciting location-based services.[11]

## II. It is Vital That Consumer Privacy Protections Maintain Flexibility for Different Business Models and Technologies to Promote Innovation, Which Will Ultimately Benefit Consumers and Our Economy.

It is crucial for policymakers not to focus exclusively on the privacy risks associated with new technologies and services, thereby overlooking the tremendous increase in consumer welfare such technologies can offer, including some capabilities that actively promote consumers' privacy interests. Because many useful products and services rely on consumer information, it is vital to strike a careful balance so that privacy-based restrictions do not unduly burden industry's ability to offer these products, services, and capabilities.

### a. Consumer Demand for Technological Innovation has Resulted in Greater Consumer Choice and Significant Benefits to Consumers and the Economy.

Consumers have embraced new technologies and business models that provide improved capabilities and greater value. For example, all of the applications and services that are the subject of self-regulation discussed above – mobile marketing, targeted advertising, and location-based wireless services– offer consumers enormous benefits. These include improved personal safety and security through easy access to maps and directions and the ability to locate children and friends throug location-based services; more efficient shopping and searches through advertising that is better targeted to the recipient's interests; and savings and convenience through offers such as mobile coupons provided through mobile marketing. There are also innovative business models that use consumer information to support an array of new goods and services, often provided to consumers free of charge. For example, search engines give users access to a universe of information at speeds and scales that were previously unimaginable. In addition to benefits to individual consumers, the collection of data in anonymized form can provide societal benefits, such as epidemic detection and other medical insights, or improvements in urban planning.

Innovation has also increased the amount of control consumers can exercise over their personal information. New technologies often offer a consumer the opportunity to choose the level of

---

principles.pdf. *See also* Leibowitz, supra note 1 (expressing support for self regulation in this area).

[11] CTIA-The Wireless Ass'n, *Best Practices and Guidelines for Location-Based Services* (Apr. 2008), *available at* http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

information gathering with which he or she is comfortable. For example, many search engines allow users to delete cookies or to opt out of behavioral targeting. Technological innovation can also actively improve consumer privacy through a variety of ways. Everyday examples range from being able to use a mobile phone rather than a home or office phone to have a private conversation, to the opportunity to use a search engine to gather information about a medical or psychological condition without having to ask an individual. A more advanced example is the ability of health information technology to limit access to electronic medical records to authorized users and to create a tracking system indicating when records have been accessed and by whom.[12]

### b. Unduly Burdensome Restrictions Related to Consumer Privacy May Impede Technological Innovation and Reduce Consumer Choice.

Privacy regulations that greatly hinder the availability of information would be costly to consumers, who would receive fewer of the resulting benefits, such as improved services and products and greater convenience. For example, free services and content may become less widely available or suffer a reduction in quality because a critical source of their funding — targeted advertising—may become less valuable.[13] Also, onerous restrictions on behavioral advertising would likely *increase* the volume of unwanted marketing messages, imposing exactly the harm avoided by the highly popular "Do Not Call" rule.[14] Finally, if members of the ICT industry are required to implement burdensome technical safeguards as part of their product specifications, the costs will invariably be passed on to consumers, which will likely raise the price of new products and thereby deter adoption.

### c. Privacy Regulation Should be Technology Neutral.

As noted above, the current privacy framework is based on providing the consumer notice about what information is collected and how it will be used, choice about whether to provide personal information, and security for the personal information that is collected. This framework is based on the consumer's expectations about how his or her personal information will be treated[15] and

---

[12] *See* D. Gilman and J. Cooper, *There Is a Time to Keep Silent and a Time to Speak, The Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. TECH. L. REV. 279 (forthcoming 2010) (discussing impact of information technology on health care industry).

[13] This effect is not simply speculative; the FTC is conducting an inquiry into the future of journalism, spurred by the decreasing ability of advertising to fund the news reporting function of newspapers. *See* FTC Workshop: New Media Workshop, http://www.ftc.gov/opp/workshops/news/index.shtml (last visited June 2, 2010) (describing FTC workshop entitled "How Will Journalism Survive the Internet Age.").

[14] Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 (1994).

[15] *See, e.g.*, Fed. Trade Comm'n Staff Report, *supra* note 2, at iii (noting that principles do not need to cover "first party" behavioral advertising because such activity by and at single website "is more likely to be consistent with consumer expectations.").

thus the focus of privacy protection should be on how information is used, collected, and safeguarded, not on which technology is used for those functions. For example, if a consumer chooses to provide personal information online pursuant to a privacy policy that promises that such information will not be shared with third parties for marketing purposes, it matters little to the consumer if the privacy promise is broken through a cookie that collects the information as he types it in, through a technology that intercepts the message while it is traveling over the network, or through the later release of that information from the recipient's database. Privacy protection should focus on how information is used and protected, rather than the means of information collection, whether it is through cookies, deep packet inspection, or paper records.

It is notable that the FTC's recent series of cases addressing failures to maintain personal information securely did not differentiate based on the technology used to safeguard the information. The FTC brought actions against companies that failed to secure their networks, as well as against a drug store chain that disposed of pill bottles with sensitive medical information by throwing them into the trash.[16] The focus was properly on the violation of the privacy protections promised to consumers, not on which technology was used to collect or store the consumer information.

## III. The United States Leads the World in Technological Innovation, Due In Part to Flexible and Balanced Privacy Laws. When Looking to Privacy Laws and Regulations in Other Countries as Models, it is Important to Focus on Models that Preserve Flexibility while Protecting Privacy.

U.S. industry has been at the forefront of innovation in information and communications technology. As detailed above, the existing U.S. privacy framework based on notice, choice, and security has permitted the development of innovative consumer products that provide safety, convenience, and easy communications, as well as business models that offer consumers access to informative and diverse content and useful services at no cost.

### a. Highly Restrictive Privacy Requirements may Hamper Innovation.

One straightforward way to reduce threats to privacy is to make the costs of information gathering, usage, and sharing prohibitive. Privacy protections must be balanced, however, to ensure that consumers and society continue to receive many of the benefits provided by information and communications technologies and that providers retain the ability to develop innovative methods of funding free content and services.

The European Privacy Directive 95/46/EC is a central example of privacy protection that contains some useful elements but also some elements that are unnecessarily burdensome. The Privacy Directive generally prevents the collection and processing of personal information unless

[16] *See Genica Corp*., FTC File No. 082 3113, Decision and Order (Mar. 2009); *DSW Inc*., FTC File No. 052 3096, Decision and Order (Mar. 7, 2006); *CVS Caremark Corp.*, FTC File No. 072 3119, Decision and Order (June 18, 2009).

the subject has provided unambiguous consent, and it also imposes significant use and retention standards on entities that collect or process personal data. Like the U.S. privacy framework, it contains the elements of notice, choice, and security, and one of its main benefits is that it applies a unified approach that reduces confusion about which standards apply to what activities. The Privacy Directive also imposes substantial costs on businesses, however, such as compliance and opportunity costs, that are ultimately borne by consumers.[17] Notably, a recent study commissioned by the European Information Commissioner's Office found that the Directive has become outdated in terms of technology, reflects an insufficient focus on harms and risks, is seen as bureaucratic, burdensome and too prescriptive, focuses on process rather than outcomes, and has become a rigid control mechanism over otherwise unobjectionable data processing.[18]

Unfortunately, examples of well-intentioned but overly burdensome regimes are not limited to Europe. A second cautionary example of the risks of onerous privacy protections is in the area of health information technology, where studies suggest that burdensome consent requirements have retarded hospitals' adoption of health information technology, with associated negative effects on patient health outcomes.[19]

**b. APEC's Privacy Framework and the Cross Border Privacy Rules Represent an Appropriate Model For Protecting Privacy While Preserving The Flexibility Necessary For Innovation.**

The APEC Privacy Framework, which was endorsed by APEC ministers in 2005, is an example of a successful international model that protects privacy while preserving the flexibility

---

[17] *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 20 (2000) ("There are, in short, identifiable costs to recognizing stringent data privacy rights, both in terms of efficiency and equity. For businesses, these costs include compliance, transaction, operating, and opportunity costs. Businesses ultimately factor these costs into the prices charged consumers. The prices of goods and services on the EU market are, in principle, higher on average than they would be without the EU data privacy requirements.").

[18] Neil Robinson et al., Info. Commissioner's Office, *Review of EU Data Protection Directive: Summary* (May 2009), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf. *See also* European Privacy Officers Forum, *Submission on the Review of the Data Protection Directive* (2009), *available at* http://www.huntonfiles.com/files/webupload/EPOF_Submission_on_DP_Directive_Dec_09.pdf (stating that European privacy notification requirements have become excessively bureaucratic and require considerable resources to manage, which is disproportionate to benefit brought to individuals.).

[19] *See* Gilman & Cooper, *supra* note 12, at 328-29 (discussing study documenting relationship between increased infant mortality and privacy requirements that suppress adoption of electronic health records by healthcare providers).

necessary for innovation.[20] The Framework takes into account the enormous benefits new technologies and business models offer consumers, government, and the economy, and seeks to enable data transfers, while "recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region." The Framework includes the principles of notice where reasonable, collection by lawful and fair means, use of the information only for the purposes collected unless consent for other uses is given, choice where appropriate, data accuracy and consumer access, reasonable security, and accountability. The Framework also supports imposing remedies that are commensurate with the extent of the actual or potential harm to individuals resulting from privacy violations.

The APEC Privacy Framework also supports the cooperative development by APEC members of Cross Border Privacy Rules that adhere to the Framework's principles. The Framework encourages the members to work with stakeholders in this process to create effective privacy protections without creating unnecessary barriers to cross-border information exchanges, including unnecessary administrative and bureaucratic burdens for business and consumers.

TIA members recognize that the Department of Commerce, along with other U.S. agencies, has been instrumental in working with counterparts across the APEC economies to develop a system in the APEC region that ensures the protection of consumers through accountable cross-border flows of personal information while facilitating business access to the benefits of electronic commerce. TIA members particularly commend the Department of Commerce for including opportunities for the business community to engage and provide input throughout the APEC Cross Border Privacy Rules development process. This collaborative effort has been essential given the pace of innovation in electronic commerce.[21] When the U.S. hosts APEC next year, TIA members stand ready to help showcase the success of the APEC Privacy Framework and the potential of the Cross Border Privacy Rules to address data privacy issues across APEC member economies.

---

[20] Asia-Pacific Economic Cooperation, *Privacy Framework* (2005), *available at* http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

[21] In particular, TIA members support the U.S. Government's efforts within the APEC E-Commerce Steering Group in organizing capacity building workshops on data protection legal regimes for important emerging APEC economies, including the Philippines, Vietnam, and Indonesia. Such workshops provide an important avenue for government and industry best practices and information sharing.

## Conclusion

TIA welcomes NTIA's inquiry on the interaction between consumer privacy and technological innovation and, for the foregoing reasons, urges NTIA to support privacy protections that maintain flexibility for different business models and technologies, including technology neutrality, and thereby promote innovation.

**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

By: /s/ Danielle Coffey_____
Danielle Coffey
Vice President, Government Affairs
**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

June 7, 2010

Office of the Secretary;
National Telecommunications and
Information Administration;
International Trade Administration
U.S. Department of Commerce,
1401 Constitution Avenue, NW., Room 4725,
Washington, DC 20230

**Re: Department of Commerce Notice of Inquiry**
**Information Privacy and Innovation in the Internet Economy**
**Docket No. 100402174–0175–01; RIN 0660–XA12**

***TRUSTe Comments***

On behalf of TRUSTe, I thank you for the opportunity to share our reflections on the Department's core inquiry concerning the nexus between privacy policy and innovation. Our intervention reflects the experience that we have gained in helping more than 5,000 companies over the course of a decade build trust with consumers online through our certification programs and addressing privacy through best practices.

Our experience and research shows that consumers are more comfortable with innovation and new business models on the Internet when their privacy expectations and protection of personal information is considered in the design and rollout of services. Consumers look for signs of trustworthiness of companies they may deal with online, including by looking for trustmarks and third party certification programs. They are more likely to register at websites, complete e-commerce transactions, and engage in internet use for social networking, e-mail, entertainment, or for general information gathering purposes when they see one or more seals that they trust on a website. It should come as no surprise then that 71 percent of consumers said they look for trustmarks before doing business online.[1]

Businesses that are sophisticated and care about demonstrating privacy accountability to consumers look for opportunities to meaningfully differentiate their practices based upon best privacy practices and outward demonstrations to consumers, such as through trustmarks and third party certification programs. They do so because it builds and retains consumer relationships and generates a

[1] "Trust Marks: What's Behind the Label Counts". Yankee Group. 2009. http://us.mcafee.com/en-us/local/docs/LR-51384.pdf

positive return on their investment through higher registrations, transactions, and more accurate data. Smaller and medium-sized businesses (SMBs) need greater opportunities, at affordable prices, to leverage privacy as a part of their brand differentiation and to build consumer traffic online. TRUSTe is innovating to fill that gap in the online market place. We appreciate the positive role of government to encourage forward leaning privacy policy nationally in order to assist all U.S. businesses to be competitive in the global online marketplace.

**What is the impact of current privacy laws in the U.S. and around the world on the pace of innovation in the information economy?**

Businesses and consumers are confused about varying privacy requirements across global jurisdictions, as well as differences presented with respect to specific business sectors. In many instances, business and consumers do not know or understand what protections are required or avenues of privacy recourse available. The cost of business compliance with such a wide range of legal and regulatory requirements may actually limit consumer choice because of slower innovation of online services caused by reticence. Innovative ideas may be sidetracked simply because businesses cannot interpret a patchwork of privacy laws. By example, crowd source, data such as individual reviews of businesses voluntarily provided by individuals, may be helpful to consumers in determining their own choices around specific stores, goods or online services. However, restrictions on data flows of crowd source data provided in one global jurisdiction from free transfer to another jurisdiction may inhibit such sharing and the accuracy of research and representations of overall consumer experiences and, thus, impact negatively on consumer choice and limit business opportunity. Harmonization of privacy frameworks and policy approaches to privacy online would assist businesses in delivering communications, products and services to consumers and assist with their efforts to be accountable for consumer privacy.

**Do current U.S. laws serve consumer interests and fundamental democratic values?**

The free flow of information on the Internet is important to fundamental democratic values, as is the protection of individual privacy. With regard to individual privacy, we believe that an improvement for the protection of users globally would be greater access to independent dispute resolution for their privacy concerns and complaints with commercial entities. Mechanisms for promoting more efficient, effective and low cost complaint resolution for consumers through non-governmental programs, regardless of borders, could improve consumer satisfaction, advance public policy for a fair and open online market place and would engender greater trust online. It remains important for consumers to have access to government redress, but those processes are often too time consuming, expensive, and as a result, ineffective for addressing privacy issues where harms can be mitigated by early resolution. Other self-regulatory mechanism that provide monitoring of practices online will also keep businesses accountable to consumers in actual practice.

**Specific Areas of the Department's Inquiry:**

1. **U.S. Privacy Frameworks Going Forward**

**TRUSTe POV:** We believe that promoting an understandable roadmap of best practices principles for businesses and signs for consumers on the Internet, short and easily recognizable – through seals, icons, symbols, will prove most helpful on websites and interactive or mobile tools that link users to the internet.

Strong Notice remains essential and we believe that there are new ways to deliver recognizable messages and signs about privacy to busy consumers who may be looking at very small screens on devices and choosing to make an e-commerce or communication decision. Some mechanisms deserving consideration include browser embedded notices, much like SSL padlock icon for e-commerce; new short notice formats for mobile devices and smart phones; Ad unit notices, and movements back to machine readable policies, learning from the P3P experience.

Businesses need incentives and help in ramping up to use short disclosures and seals so that consumers will easily understand them. By example, among other incentives, tax credits to businesses might help spur the uptake of privacy awareness and best practices that can be independently assessed by third parties. The net result could grow and preserve the online market for U.S. innovation around privacy and build consumer confidence in not only in the U.S. but also globally.

We also believe that there remains a place for longer privacy policies that make full representations that consumers can study and rely upon for enforcement of commercial promises.

Separately, consumers are looking for more accessible means of indicating their choices around privacy preferences, both in and outside of the privacy policy, as most visibly indicated in recent reactions to changes in Facebook's privacy controls.

**What is the current state of privacy self-regulation? Should there be minimum requirements for self-regulatory programs? If third parties conduct those programs, rather than as a company's own internal operations, what mechanisms should there be for users and civil society to provide input?**

**TRUSTe POV:** TRUSTe has been an independent third party provider of privacy and trust certifications for online services for more than a dozen years. We are supportive of proposals for the enactment of a federal law requiring privacy disclosures online in order to enhance business and consumer awareness of privacy protection. A federal law would extend the impact of certain state laws, like California's, that require privacy disclosures and advance opportunities for consumer choice, and would provide a recognized national standard. Self-

regulatory programs can work in tandem with legislation in this area, strengthening implementation and effectiveness.

TRUSTe, is an independent third party whose privacy certifications are criteria-based, built around solid program requirements that incorporate the fair information practices principles and international privacy principles and best privacy practices. While those requirements evolve with changing business models, new technology approaches and privacy risks online, we believe that self-regulatory programs are best when they are criteria based. As a baseline, they should include thorough certification practices, ongoing monitoring of business practices against their policy statements and self-regulatory program requirements, compliance and enforcement mechanisms, and means for dispute resolution. All stakeholders, including users and civil society are able to provide input into privacy self-regulatory programs when the programs are sufficiently transparent with the ongoing development of requirements and reporting on operations, consumer complaints and effectiveness in responses, and compliance and enforcement activities. Self-regulatory programs are strengthened with this input. Third parties need to publish their program requirements, much like SSL certification authorities publish their Certification Practices Statement. Eventually, it may be possible to establish some technical audit mechanisms, including browser audits of certification authority privacy program requirements, following recognizable standards, similar to the audit model for SSL certification authorities.

Self regulatory programs can support the current notice and choice approach in the U.S., modifications on it, or approved uses of information under a use-based approach that some are currently advocating. TRUSTe believes it will remain essential for consumers to have clear privacy disclosures, easily readable privacy signs (seals and symbols), and consumer opportunities for access to information use by companies and preservation of consumer choice around information use.

We also believe that positive incentives, for example the benefits that organizations enjoy with a credible trustmark (higher registrations, transactions etc.) provide a positive incentive for strong privacy programs.

2. **U.S. State Privacy Laws – Whether the diversity of state privacy laws has a positive, negative, or neutral impact on the privacy rights of Internet users and presents hurdles for businesses**

**TRUSTe POV:** TRUSTe works with companies across the United States that participate in interstate commerce via the Internet. The patchwork quilt of privacy and information security and data breach laws across the nation is difficult for many of our clients to navigate. It is also difficult to offer a self-regulatory program that addresses compliance with all of the state laws, so instead, best practices and requirements are targeted to federal standards. We believe greater harmonization would certainly provide clarity for businesses. It would better assist good companies that want to fulfill privacy requirements with a clear path to do so in a

consistent manner across state jurisdictions and affording consumers the same treatment.

3. **International Privacy Laws and Regulations – What challenges do businesses face when trying to transfer data across borders? What lessons have been learned from the U.S. – EU Safe Harbor Framework that could be applied in the global context? What mechanisms do organizations use to enable cross-border data transfers?**

**TRUSTe POV:** Companies are required to honor limitations on cross-border data transfers of personally identifiable information from jurisdictions such as the European Union, and certain non-EU countries with similar restrictions, unless they use legal mechanisms to provide assurances of adequate treatment of the data by the cross-border recipient. This is a complicated process for sophisticated and large global companies and, frankly, we believe not known or understood by small and medium sized companies on the Internet that may also be required to abide by these legal restrictions.

TRUSTe has provided a EU Privacy seal program since 2001 to assist companies in meeting their compliance readiness obligations when they self-certify to the U.S.-EU Safe Harbor Framework with the Department of Commerce. Through our program we provide dispute resolution services, as called for by the Framework. We have learned that nearly every company in our program needed assistance in complying with the Framework's principles, including changes to their processes or consumer disclosures. We also have seen that the Framework is working in terms of consumer knowledge, as the rate of consumer complaints has increased with awareness of the ability to file online complaints and have them resolved.

We believe that the Safe Harbor Framework is a good starting point for other global privacy mechanisms, particularly because it is principle-based and allows for respect for both U.S. and EU legal frameworks and privacy values, with important requirements around notice, choice, and dispute resolution. As additional frameworks are contemplated, we look for them to include workable onward transfer provisions.

TRUSTe is active in ongoing efforts in the Asia Pacific Economic Cooperation forum to advance cross-border cooperation and enforcement of privacy commitments. We support the leadership of the Department in this international effort, including the work that encourages criteria-based self-regulatory programs for qualification as APEC privacy accountability agents. We also support APEC's testing of APEC certification programs that require ongoing monitoring of business practices, have compliance and enforcement mechanisms, a direct means for consumer dispute resolution and encourage transparency on results.

4. **Sectoral Privacy Laws and Federal Guidelines – What can be done to make the current sectoral approach to privacy regulation in the U.S.**

**more conducive to business development while ensuring effective privacy practices?**

**TRUSTe POV:** We believe that it is important to acknowledge specialized expertise of regulatory agencies for specific sectors. At the same time, it is important to distinguish between specialized experience in a particular business area requiring specialized regulation, for example financial services, and common, national priorities and best practices for business protection of consumer privacy.

We are concerned about impediments to innovation in both product delivery and privacy protections, in particular in the financial services sector at a time, when consumer certainty and trust need to be bolstered. Recently the financial services regulators came out with a model privacy statement and an online version that financial institutions must use in order to receive safe harbor regulatory compliance treatment. TRUSTe is particularly concerned because the model privacy policy does not allow U.S. financial institutions to use a seal on their privacy policy. Consumers looking for greater confidence in the financial sector are singularly unable to receive a sign that the policy and practices behind the privacy policy have been reviewed and certified by an independent third party, or that they are participating in a program that offers ongoing monitoring of privacy promises, compliance and enforcement, and third party dispute resolution.

Other sectors receive a competitive advantage by being able to engage more dynamically with consumers online by showing seals on their privacy policies, receiving additional returns on investment and consumer loyalty. TRUSTe believes that it is a mistaken government policy that has no statutory underpinnings. It undermines harmonized privacy protection on the Internet by U.S companies. The policy decision by financial regulators inhibits differentiation of financial brands for businesses and consumers based upon privacy, and results as a restraint on trade for self-regulatory programs like TRUSTe that have a decade of experience in building trust online and promoting U.S. business innovation. This is one example of U.S. vulnerability in a global marketplace where sectoral applications of law and policy around privacy are inconsistent. Those inconsistent applications do not send a harmonized message to raise privacy awareness and may disadvantage the competitiveness of businesses that would like to differentiate their brand based upon privacy practices.

As Congress and policy makers consider federal legislation to address privacy, TRUSTe believes that including a safe harbor concept for companies participating in strong, criteria-based self regulatory programs that demonstrate their accountability for consumer privacy should be a priority. We believe that effective privacy self-regulatory programs also should include substantial monitoring and compliance mechanisms, enforcement authority, and dispute resolution and that program requirements and activities advance consumer confidence through their transparency. To be effective, meaningful incentives for business uptake must also be provided.

## 5. New Privacy Enhancing Technologies and Information Management Processes

**TRUSTe POV:** The need for privacy enhancing technologies, whether built into products, added on to products and services, or used by a third party to manage and monitor commercial activities, has never been greater. With wider use of online services for communication, e-commerce, entertainment, and educational purposes, the impact on individual privacy also continues to grow. TRUSTe supports and encourages the Department in its efforts to promote innovation to support privacy enhancing technologies and information management processes. We believe it would be most effective through the promotion of research, public and private partnerships, and incentives to businesses to develop privacy enhancing technologies writ large.

Much as we encourage green activities with respect to care of our physical environment, now is the time to encourage the use of technology to build in and support consumer privacy choices and business privacy advancement in the online environment. This is particularly needed to assist small and medium sized businesses, as well as to meet privacy issues raised by new and emerging business models that may introduce wider privacy impacts across platforms. With encouragement, a U.S. privacy model that embraces technological innovation to support consumer privacy can result in an expectation of excellence in privacy practices that global participants can count on when they interact online with U.S. companies of any size.

**TRUSTe POV:**

## 6. Small and Medium Sized Businesses – Challenges and Need

**TRUSTe POV: Today**, the majority of businesses online are small or medium sized businesses. TRUSTe's research indicates that the vast majority of these SMBs are unprepared to address privacy or information security. Specifically, we found that a majority of small and medium-sized business websites do not have a privacy policy[2]. Many are unaware of domestic or international privacy laws that may apply to their businesses in the online or offline contexts. And, as with many large and sophisticated organizations, SMBs require capacity building and education in order to address business responsibilities to consumers on privacy and information, although they may be both short on time, money and staffing to do so.

TRUSTe is addressing the particular needs of SMBs by raising their privacy awareness and offering products and services that are affordable and result in an up-to-date and accurate privacy policy, describing their information practices with respect to consumer information. We have invested in innovations that including an interactive privacy generator geared to SMB business models, up front and periodic site monitoring, and mechanisms to provide dispute resolution. As we

[2] TNS – TRUSTe SMB Privacy Assessment, Dec 08

deliver the privacy policy and through customer contact, including due to monitoring, we look for teaching moment opportunities to further build SME capacity around privacy awareness.

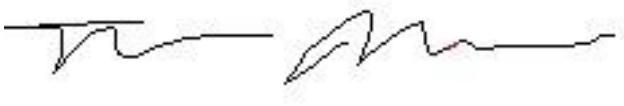
The Department has long included support for SMB training and capacity building. We encourage that continuing role and support through technical assistance. As the Department considers additional ways of building SMB capacity around privacy, it may be helpful for the Department of Commerce and NIST, in particular, to consider the need and utility for a 'PCI'-like standard for SMBs to adopt privacy controls. By example, currently Google Adsense is a good example of a company initiative that requires SMBs advertising through their site to have a privacy policy. But, there is no industry requirement that either requires an accurate statement of privacy practices or that monitors for the existence of policies when requested by company initiatives. There are many avenues for influencing SMB uptake of privacy policies and baseline controls for their online practices, including through ad networks, web hosts, e-commerce sites, and merchant networks. To the extent that consumers have more confidence that SMBs online understand their privacy interests and will be accountable with their data, e-commerce development through U.S. sites could dramatically increase and in a manner that distinguishes U.S. businesses.

### 7. The Role of Government and DOC

**TRUSTe POV:** TRUSTe applauds the recent DOC conference on privacy and innovation, as well as the longstanding leadership and commitment of the Department on privacy, particularly with regard to e-commerce and international frameworks between the U.S. and EU and in the APEC forum. We encourage the Department to continue its efforts to advance U.S. competitiveness in the global marketplace by encouraging government and the private sector to work together to demonstrate U.S. leadership broadly in developing and implementing best privacy practices in the online environment.

We encourage the DOC to continue to actively engage with U.S. businesses to monitor privacy and innovation challenges. We believe that the role of government and the DOC is to advance both goals. TRUSTe stands as a ready partner with the Department in continuing working toward that goal.

Sincerely yours,



Fran Maier
President and Executive Chairman

USCIB
UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

**Peter M. Robinson**
President & CEO

June 14, 2010

National Telecommunications and Information Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams,

We are pleased to provide comments in response to the Notice of Inquiry on Privacy and Innovation. Given our specific mandate and expertise, we have focused our remarks on the portions of the NOI pertaining to the global privacy system and international cooperation to protect privacy.

The United States Council for International Business (USCIB) promotes open markets, competitiveness and innovation, sustainable development and corporate responsibility, supported by international engagement and prudent regulation. Its members include top U.S.-based global companies and professional services firms from every sector of our economy, with operations in every region of the world. With a unique global network encompassing the International Chamber of Commerce, the International Organization of Employers and the Business and Industry Advisory Committee to the OECD, USCIB provides business views to policy makers and regulatory authorities worldwide, and works to facilitate international trade and investment.

USCIB's ICT Policy Committee represents businesses from diverse industry sectors. The committee advocates for sound international policy frameworks, characterized by free and fair competition, targeted government intervention limited to addressing clearly defined market failures, free information flows and a user orientation, that ensure the continued growth of ICTs and extend their benefits around the world. The committee also increases awareness of the potential impact of policies, laws, and regulations related to ICTs and e-business. USCIB and its members work to enhance trust and promote privacy while enabling global information flows by developing solutions to possible restrictions on transborder data flows through the ICC model contracts and other tools, working on the implementation of the APEC Privacy Framework, active engagement on the dialogue around the review of the OECD Privacy Guidelines and general policy debates, providing input on ISO privacy initiatives and continuing to monitor developments worldwide. We promote self-regulation and the application of existing global privacy guidelines to ensure responsible and accountable implementation of new technologies and applications such as radio-frequency identification (RFID) and social networking. We promote a global culture of cyber-security through ICC and BIAC, and in regional fora. USCIB has a long history of working through the ICC to communicate business views to the EU, and recently concluded a new model contract for controller to processor transfers.

1212 Avenue of the Americas
New York, NY 10036-1689
212.354.4480 tel
212.575.0327 fax
www.uscib.org

USCIB encourages the Department of Commerce to take a proactive role promoting the US privacy regime as a part of a global privacy system that works for U.S. companies. As the Department gathers input on our own regime, it would be helpful for U.S. positioning on privacy to receive greater and more focused representation internationally by the U.S. government. International coordination will continue to be key to free flows of information and deployment of new and innovative services. In that regard, we also welcome continued involvement by other governmental agencies and appreciate the international efforts of all USG agencies over the past several years.

Industry understands that its role in protecting privacy supports its mission to achieve and retain customers, and thus, industry consultation at all levels of this continuing dialogue will improve compliance and enforcement. We hope to continue our dialogue on these issues with the Department and the Internet Policy Task Force on the NOI responses.

**I. Impact of diverse privacy laws and obstacles to cross border data transfers**

The sheer complexity associated with understanding and implementing policies and practices that are compliant with multiple laws, regulations and case law across multiple countries, languages and cultures increase the difficulty and cost of doing business internationally. Conflicting privacy and data protection laws across different countries, and the impact of laws and regulations in other areas that conflict with domestic or foreign privacy laws further hamper international trade and investment and the general economic growth they contribute towards. Prescriptive international standards make it difficult to create a global company wide solution without adopting the most restrictive standard. Currently, companies employ a variety of mechanisms, discussed below, to try to overcome these obstacles.

Variations in laws and compliance requirements can result from:

- technical specificity (Italian Data Protection law specifies an 8 digit alpha numeric passcode),
- compliance architecture (the need in some countries for a local data protection officer, creating a compliance position that replicates global or regional staffing)
- variations in definitions (what is sensitive information)
- variation in substance and bureaucratic processes (recent court decision in Dusseldorf which questions whether safe harbor certification provides evidence of compliance with legal requirements).

Given the borderless nature of the Internet, it is often difficult to determine the location of a person or entity, and thus to establish jurisdiction or applicable law. Disputes often arise as a result of different interpretations. Moreover, some countries are aggressive in claiming jurisdiction, subjecting companies to laws they were not expecting. For example, the EU Article 29 Working Party has issued opinions that assert that the use of cookies, commonly placed on end user computers for a range of purposes, is considered 'equipment located in the EU' to establish jurisdiction. Companies that have no physical presence and are not necessarily knowingly doing business within the EU do not expect to be subject to EU jurisdiction or have the Directive apply over websites find that they are.

Jurisdiction also comes into play with the complexity of information flows. For example, US-based companies that have posted privacy policies are subject to enforcement by their U.S. regulators. If they use a service provider in the EU they are also subject to EU Member State laws. So, to the extent that they have a follow-the-sun service model, they may also be subject to the procedural and substantive aspects of the laws of the various support locations that may be involved. Further complexity is involved for companies providing third party services, who may also have to consider issues of multiple sectors which may have varying or additional restrictions. Another layer of complexity comes from legal and investigatory issues which might not be purely related to privacy; these include whistle-blowing and conflicts between SOX and EU privacy law as well as discovery requests from the US to EU or other countries related to non-US citizens that conflict with local law. Discovery is especially relevant as the discovery regimes in the EU are much more limited; thus, the more expansive discovery rights under US law are difficult for EU DPAs to understand and recognize.

As global information flows expand and remote services such as those facilitated by cloud computing expand, the question of jurisdiction and its resolution will become even more important. Cloud services may rely upon multiple data centers with geographical spread. They will of necessity require fluid ability to move information for optimization, security and business continuity/disaster recovery. Actual and constructive limitations on such transfers, assuming that systems are in place to assure compliance with obligations, are artificial rather than substantive or effective. More and more consolidated data centers are accessed globally – making the notion of location of data less relevant over time.

Many laws, either in letter or spirit, favor local storage of information and limitation on access to information based on geography rather than need. They are a vestige of the time the law was developed when information flows were based on EDI and processing was often point to point batch processing. These restrictions may currently require the creation of redundant facilities to meet legal requirements imposing geographical limitations, or the difficulty in creating a system where consent is needed due to the location. How do you deploy a centralized HR system when a handful of employees may object to the transfer of their information? Such a limitation would mean having an automated system supplemented by multiple manual systems.

Economies of scope and scale are achieved through centralization of resources and expertise. They are also optimized when you can take advantage of pools of skilled labor that are either more cost effective or provide the needed geographical dispersion to create a 24 hour service platform (follow-the-sun model). Furthermore cloud computing has created significant cost benefits by allowing individuals, SMEs, companies and governments to access platform, software and hardware in an on demand environment for a tiny fraction of what those resources cost to implement by any one entity. All of these services are predicated on information flows that must be agnostic to location. Location is determined by need and availability. Laws should not be focused on perpetuating requirements of location.

We continue to believe that existing legal and other requirements –including robust enforcement – have been effectively protecting customer privacy interests in the U.S. The U.S. regime has undoubtedly fostered a more robust environment for free information flows and rapid deployment of services than many if not most of its counterparts.

Laws that permit governments to have access to personal information can be an impediment to innovation or global trade and investment. For example, concerns over access to SWIFT data and expanded access under the PATRIOT Act have created a backlash in the EU and British Columbia, Canada respectively, which have led to increased sensitivity to US data transfers and have led to the prohibition of transfers of British Columbia provincial information to the US. Additionally, while India is currently developing rules related to access to information, concerns still exist that companies may be caught between other countries' privacy rights and due process restrictions and Indian requirements related to the production of information. Also, the IRS interest in assuring compliance with US tax laws may become an issue due to other countries' privacy and bank secrecy laws. These requests create situations where companies are the battleground between multiple countries and their customers. There is no positive outcome for the company in this kind of dispute, and yet the company is merely a custodian of the information unable to resolve the equities of the dispute as they may involve the legitimate laws of the counties and the personal interests of the customer.

Despite the necessity of data flows across borders in today's global business environment, businesses face internal compliance and regulatory challenges when trying to do so. Companies must deal with differing or conflicting laws in multiple jurisdictions where data is collected and transferred. In some cases, laws prevent or limit the cross border transfer of data.

Finally, not only are there a plethora of differing and conflicting laws, there are also an abundance of unnecessary requirements. A prime example of such unnecessary requirements are those restricting cross border data flows. These restrictions are a burden on commerce and in some cases reflect an unachievable goal. Moreover, the original rationale for these restrictions are outmoded and unworkable in today's networked world. It is noteworthy that the body of law otherwise generally applicable to electronic

commerce and the internet has been developing successfully without such restrictions. In addition, some of the more recent privacy laws adopted in other countries recognize these cross border restrictions as obstacles and have not included such restrictions in their laws.

**II. Business Solutions**

In order to address privacy regulations, requirements and cross border restrictions, businesses implement a variety of solutions which must be maintained and managed both in parallel and in combination in order to create a compliance infrastructure. While solutions have been created to permit the continued and vital cross border transfer of personal information, none are perfect and some actually hamper international trade and investment.

The complexities of the global privacy regime, with diverging approaches and different requirements and standards, necessitates that companies establish an internal structure and employ resources specifically to handle privacy issues, which may entail establishing one or more internal data protection officers.

Companies often use contracts when transferring personal information to ensure accountability or to satisfy specific regulatory requirements, though when this mechanism is used to satisfy EU cross border requirements, it has become increasingly complex and difficult to implement.

In the EU, some companies are eligible to self-certify under the Safe Harbor to permit transfers from the EU to the US and are also increasingly relying on binding corporate rules. In addition, companies use master contract architectures, policies and compliance programs, and emerging accountability mechanisms such as private sector Trust- marks and seals.
Companies address jurisdictional conflicts and any resulting conflicting legal and regulatory obligations in several ways. Companies work with local regulators and various global, regional or local bodies that bring economies together, directly or through various intermediaries, to discuss and address policy issues.

**III. Conclusion**

Core privacy principles are similar around the world, however, based on region and country specific histories and customs, local jurisdictions have developed and applied privacy requirements in different ways. Therefore, any cooperative approaches to privacy must recognize the economic, legal and social contexts of the economies in which they operate. We believe that any workable business solutions must facilitate cross border transfers, permitting companies to transfer and access data globally for business purposes without additional cross border restrictions.

We look forward to a continued dialogue on these issues.

Regards,

Peter Robinson

**Before the**
**DEPARTMENT OF COMMERCE**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Information Privacy and Innovation in the Internet Economy | ) | Docket No. 100402174-0175-01 |
| | ) | RIN 0660-XA12 |
| | ) | |
| | ) | |
| | ) | |

## COMMENTS OF VERIZON AND VERIZON WIRELESS

Verizon and Verizon Wireless ("Verizon") appreciate the opportunity to provide input to the Department of Commerce ("Department") Internet Policy Task Force as it launches its Privacy Innovation Initiative. In its Notice,[1] the Department has appropriately recognized the importance of establishing an environment consistent with longstanding information use practices and individual privacy expectations while encouraging innovation and increased participation in the Internet.

At Verizon, protecting the privacy of customer information is an important and well-established priority. Consistent with the Notice's focus, Verizon recognizes that consumers will use the full capabilities of its communications products, services, and networks only if they trust that Verizon will respect their privacy preferences and use their information in accordance with their expectations. Verizon remains committed to maintaining strong and meaningful privacy protections for consumers as communications technologies and services rapidly advance.

[1] Department of Commerce, *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 FR 21226 (2010) ("Notice").

Fundamentally, privacy protections should include a clear disclosure of what information is being collected, how it is used, and with whom it is shared. Consumers should also have ready access to tools that allow them to control the use of their information for certain purposes. In recent years, privacy requirements that attempt to apply these principles have proliferated in the form of state and federal laws and regulations, international in-country and region-specific requirements, and self-regulatory programs. However, as the Department has acknowledged in the Notice, the existence of multiple approaches and requirements can complicate consumers' ability to understand how their information is being protected and companies' ability to implement all applicable rules, especially where rules may conflict or where technologies and services converge such that jurisdiction is difficult to determine.

Accordingly, a unified approach to privacy protection that incorporates the principles of consumer transparency and control and applies them equally – regardless of the particular technology or business model used in the collection of such data – would improve consumer knowledge while creating efficiencies for companies. Such an approach would allow businesses to devote greater resources towards innovative business models, to the benefit of consumers who could take advantage of new services with a clear understanding of the data security and privacy controls available to them.

As such, the Department should continue to identify and examine whether domestic and foreign privacy laws conflict with each other in a manner that imposes undue compliance burdens for business or where barriers to commerce exist in specific states or countries. The Department should promote flexible programs that meet consumers' privacy expectations while allowing for continued innovation in the

information economy. In addition, the Department should encourage the development and use of tools that enhance individuals' ability to control their private information and support programs that increase consumer education around privacy protections and controls.

## DISCUSSION

### I. The Harmonization of International, Federal, and State Privacy Requirements Would Benefit Consumers and Businesses.

#### A. International Laws

In the international environment, privacy laws tend to be based on the location of the data subject or where the data collection occurs. Yet these bases for differing laws make little sense in today's business environment. Verizon, which operates in 159 countries on six continents, serves customers on its own network and also manages network capacity obtained from dozens of other carriers on behalf of its business and multinational customers. To most efficiently serve its customers, Verizon, like many other multinational businesses, deploys central servers and host computers that facilitate remote access by authorized persons located around the world. As a result, the notion of "where data collection occurs" is difficult to fix for purposes of a national law's definition, and there are substantial administrative burdens attendant to deploying services under this type of collection-based privacy system.[2]

Moreover, existing national and multi-national legal treatments of cross-border data flows – and related privacy implications – vary greatly and impact both privacy

[2] The extent of this problem is increasingly apparent in the context of cloud computing. Cloud computing involves the exchange of data in the IP cloud among myriad systems and databases within that cloud and therefore does not lend itself to geographic and jurisdictional certainty.

compliance and businesses' approaches to service deployment. In some cases, this balkanization impedes communications, trade, the free flow of information, and certain business activities. The EU Data Protection Directive was enacted to remove such obstacles to the flow of data among member states, but has requirements that differ from those in the rest of the world.

Attempts to overcome jurisdictional differences – through bi-lateral and multi-lateral agreements and commercial terms – have been slow to develop and are not always uniformly effective. One of the seminal efforts in this area was the Department's negotiation of the EU-U.S. Safe Harbor Framework to ease compliance with 1995 EU Data Protection Directive.[3] This Framework has been successful in facilitating global commerce for some industries transferring data between the U.S. and EU. However, the Safe Harbor rules cover only some commercial organizations, while other entities, including telecommunications service providers, are not presently eligible and must implement European standard commercial terms (or certain other approved terms) between and among entities collecting or processing data in the EU.

Moreover, the Safe Harbor rules only address data flows between the U.S. and EU countries. For organizations that engage in multi-regional data transfers, there is no single privacy paradigm that provides a global set of rules and protections. This gap can be a substantial obstacle to innovation and the advancement of new services.

[3] The Safe Harbor Framework consists of seven privacy principles, 15 frequently asked questions and answers (FAQs), the European Commission's adequacy decision, the exchange of letters between the Department and the European Commission, and letters from the Department of Transportation and Federal Trade Commission on their enforcement powers. The documents are listed and published at http://www.export.gov/safeharbor/eu/eg_main_018493.asp.

The recently developed Binding Corporate Rules (BCRs) also serve as an important tool for compliance with national data protection rules under the EU Directives. BCR negotiation and implementation remain, however, member state-by-member state tasks, without the benefit of mutual recognition among national data protection authorities for nationally-approved BCRs.

Finally, the Asia Pacific Economic Cooperation (APEC) Privacy Framework requires that a company bind itself publicly to adhere to agreed principles for cross-border flows of personal information. APEC's use of flexible principles designed to facilitate cross-border transfer among APEC member countries is a welcome development for U.S. companies seeking to do business globally. The Department's role in developing the APEC Cross Border Privacy Rules and working with its counterparts across APEC economies on a project to implement the framework, known as Data Privacy Pathfinder, has been particularly helpful to the business community. The Pathfinder's illustration of how APEC's principles should be applied benefits both national authorities and entities seeking to conduct cross-border data transfers.

However, the utility of the APEC Framework will only be as strong as national governments' willingness to promote the adoption of its principles and follow through with compliance. While the concept of a mechanism to bridge disparate national laws through cross-border accountability has promise, as a non-legal instrument, it does not offer the certainty often sought by multi-national businesses.

### B. U.S. Federal Laws and Self-Regulation

In the United States, privacy laws have evolved primarily from concerns about specific types of information and its collection and use in specific industry segments or

sectors. This approach seeks to protect particular categories of data for which sensitivity and risk are believed to be the highest. For instance, laws governing health, financial, and communications information were enacted to provide heightened treatment for this sensitive information.

The sectoral approach, however, may lead to consumer confusion. Consumers may become accustomed to certain aspects of the sector-specific requirements they encounter, such as medical privacy notices with which they are presented when they visit a doctor or credit card privacy statements they receive in the mail. In most cases, though, consumers lack a clear sense of what particular information is protected under which set of rules or what their rights are with respect to the use of their data by the specific entities covered by the applicable sectoral privacy rule.

Moreover, the sectoral approach can cause an uneven application of rules. When the same information is gathered and used in provisioning similar services, but the privacy obligations that apply to individuals' information are different based on how specific sectoral laws define "covered entities," consumers can be harmed. For example, the Communications Act's definition of "telecommunications carrier" was adopted almost 15 years ago – long before the explosive growth in Internet-related communication applications, services, and tools. Requiring that only certain competitors comply with the Act's and the FCC's robust privacy requirements, while allowing others to avoid them altogether, distorts competition. The resulting cost advantage could translate to a lower price that would drive consumers to these companies. Yet these same consumers would likely mistakenly believe that the same privacy protections they have available to them when their information is held by a "telecommunications carrier" would

continue.

To avoid this harm to competition and consumers, the privacy protections afforded to the collection and use of data deemed sensitive in a specific sector should be required of all parties collecting or using that sensitive data, regardless of nominal sector. The notion of a "covered entity" based on traditional industry silos is outdated and has the end result of regulating the same service in different ways. These differences and the consequent inconsistency in privacy protections are generally unknown to consumers.

While the sectoral laws in the United States have responded to specific areas of concern, effective self-regulatory programs have developed in other areas and complement those laws. Examples of such programs include the BBB Advertising Review Services,[4] the CTIA Best Practices and Guidelines for Location-Based Services,[5] and the recently released Self-Regulatory Principles for Online Behavioral Advertising.[6] These self-regulatory programs promote innovation while maintaining privacy protections as a mainstay of new services or technologies. Self-regulatory programs leverage the particular expertise of industry players that understand the way in which consumer information is collected and used and what controls can best afford consumer privacy protection while allowing market and technical innovations to continue. Self-regulation also offers greater flexibility for industry to respond effectively to new privacy

---

[4] BBB Advertising Review Services, http://www.bbb.org/us/Advertising-Review-Services (last visited June 11, 2010).

[5] CTIA Best Practices and Guidelines for Location-Based Services, http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf (April 2, 2008).

[6] American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising*, http://www.iab.net/media/file/ven-principles-07-01-09.pdf (July 2009).

concerns, helping consumers avoid emerging threats.

### C. State Laws

Privacy laws and regulations that establish controls around the collection, use, or protection of customer information exist in nearly every state. State legislatures have forged state-specific data breach notification laws and have been active in areas including data security, data retention and destruction, use and display of social security numbers, and privacy-protective marketing practices. Not surprisingly, the legal requirements of the many state-specific laws vary. For example, while state laws requiring consumer notification in instances where sensitive data has been breached are largely consistent in their desired outcomes, detailed requirements, such as the trigger for notification, the timing of notification, the content of notification, the manner of notification, and the regulatory entities that must be notified, often differ.

Businesses like Verizon that have a wide geographical footprint must ensure they comply with *all* applicable state requirements simultaneously. Businesses approach the multiplicity of state privacy laws by choosing the most restrictive requirements across the board, implementing different rules for different states, or using some combination of these approaches. Regardless of the approach selected, these variations raise businesses' costs and increase the difficulty of compliance without necessarily improving customers' privacy protections.

In addition to compliance, businesses must closely follow and participate in, to the extent possible, the legislative processes around state privacy laws in all of the jurisdictions where they do business. State legislatures have been actively modifying existing privacy laws and developing new laws. Over 100 state data-security and privacy

laws have been enacted in the past five years. When state legislative sessions are in progress, it is not unusual for Verizon to be monitoring or engaged in discussion on twenty different privacy-related bills. When new legislation becomes law in a given state, businesses must conduct a comprehensive reevaluation of their privacy policies and practices. Such significant inefficiencies would be averted by the harmonization of state privacy laws.

## II. The Department Should Promote Innovation and Consumer Education.

The Department should support the development of privacy-enhancing technologies and processes that further consumer understanding and engagement in decisions about the use of their personally identifiable information. For instance, identity services are being developed that enable online authentications and help consumers manage their privacy and information use and sharing preferences. As the FCC recognized in its National Broadband Plan, trusted "identity providers" could help consumers manage their data in a way that maximizes the privacy and security of the information. Through the development of appropriate safe harbor provisions, services that maintain identity management and authentication components could be acknowledged as trusted intermediaries. Such services would safeguard information by following strict guidelines, audit mechanisms, and reporting obligations to help consumers manage their online identities across Websites and application providers to better utilize new technologies and services they choose. And consumers would benefit from the innovations that businesses can provide on top of the identity and profile data that consumers are willing to share.

The Department should also encourage businesses to consider privacy principles

and appropriate consumer privacy controls as they design and develop products and services, rather than retro-fit protections after problems have arisen and consumer privacy has been compromised. Verizon strives to build privacy controls into new products and services within the development process so that controls are as effective and comprehensive as possible.

## CONCLUSION

Verizon supports the Department's goals as it examines the impact of the current privacy framework on Internet commerce and innovation. In light of the compliance complexities required of businesses from the myriad international, federal, and state privacy requirements, and the need for greater consumer understanding of privacy protections and controls, the Department should promote a unified approach to privacy that recognizes and incorporates the flexibility offered by self-regulatory programs. The Department should play a leadership role in the international environment to ensure that U.S. privacy positions are represented as new approaches to privacy are considered in other parts of the world. Finally, the Department should emphasize the importance of consumer outreach and education and foster better understanding of general consumer privacy programs and controls.

Respectfully submitted,

Karen Zacharia
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3158

Attorneys for Verizon

John T. Scott, III
Verizon Wireless
1300 I Street, N.W.
Suite 400-West
Washington, DC 20005
202.589.3760

Attorneys for Verizon Wireless

Michael E. Glover
*Of Counsel*

June 14, 2010

Russell W. Schrader
Associate General Counsel
Global Enterprise Risk

June 14, 2010

***By Electronic Delivery***

National Telecommunications Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Re: Information Privacy and Innovation in the Internet Economy

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa Inc. ("Visa") in response to the Department of Commerce ("Commerce") Internet Policy Task Force's Notice of Inquiry ("Notice") relating to privacy and the Internet economy, published in the Federal Register on May 10, 2010. Visa operates the Visa payment card network, which is the largest consumer payment system and the leading consumer e-commerce payment system in the world. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud. We appreciate the opportunity to comment on this important matter.

**Commerce Should Play a Leading Role in the Global Privacy Debate**

Commerce should play a leading role in representing the interests of U.S. businesses in domestic and international discussions to ensure that individual privacy interests are respected within the world's information-driven economy. Over the years, a number of federal agencies have represented the U.S. in global privacy discussions. Commerce, however, has significant policy responsibility for growth and innovation in the U.S. economy. Specifically, Commerce's mandate is to advance economic growth and jobs and opportunities for the American people. As the U.S. and global economies grow far more dependent on information, any new limitations on how businesses may handle information can have a significant impact on economic growth. As a result, Commerce should be a leading voice representing U.S. interests in global privacy discussions.

Visa
P.O. Box 8999
San Francisco, CA 94128
U.S.A.

t. 650-432-1167
f 650-432-2145
rschrade@visa.com

Moreover, Commerce should continue to support global policy frameworks that assure that information flows throughout the world without impediments, but with oversight and governance. Current global privacy frameworks that are being discussed, such as the APEC Privacy Framework and the OECD Privacy Guidelines, will evolve over time. It is important that the U.S. government be a part of the process and actively contribute to this evolving area. In addition, these frameworks work best when there are common objectives for data protection. In this regard, Commerce should lead a process involving international industry stakeholders to develop these common objectives.

With respect to the Internet specifically, Commerce should help provide the U.S. government's vision for an innovative but safe Internet that bolsters our information-driven economy. Innovation comes from understanding data, including personal information, and using that understanding to improve business processes. Business processes are diverse, ranging from logistics to risk management and fraud prevention to business continuity. The benefits of improved business processes are unquestioned. Nonetheless, innovative uses of information must be compatible with responsible and answerable personal information management. The U.S. should be a leader in finding innovative ways to protect privacy and enhance data security while encouraging the free flow of information in a globally connected economy.

**Commerce Should be Cautious of Overly Broad Regulation**

Commerce and the U.S. government should be particularly cognizant of the balance that must be struck between innovation and regulation. In this regard, overly broad regulation tends to stifle innovation, and, with respect to privacy, tends to do so without actually protecting consumer privacy interests in a substantive manner.

Moreover, if U.S. companies are subjected to an overly broad privacy regime, they will likely be put at a competitive disadvantage with respect to their global competitors. For example, inconsistent and often contradictory limitations on cross-border data transfers of personal information can place companies at an immediate disadvantage. These limitations prevent businesses from providing the products and services that their customers demand and from managing their global operations in an efficient and cost effective manner. Global data flows have become a common and essential component of our daily lives and restrictive cross-border data transfer limitations create artificial barriers to trade without enhancing privacy protection for consumers.

The U.S. should avoid the pitfalls that we have seen with other data protection laws that put procedural requirements ahead of strategic management and protection of information. Large multi-national businesses rely on global data flows in order to comply with legal and regulatory obligations such as risk control and fraud prevention. For many global financial businesses, moving and centralizing data around the world is critical to effectively identifying, assessing, monitoring and managing risk. Moreover, global data flows are essential to preventing fraud,

money laundering and terrorist financing. In fact, existing U.S. privacy laws include exceptions to limitations on sharing personal information because they recognize the critical need to ensure data flows for precisely these purposes.

As a leader in information security standards and a provider of important anti-fraud tools, Visa relies on cross-border data flows. For example, Visa deploys cutting-edge technologies to monitor payment card transaction on a global basis—24/7/365—in order to spot fraud the moment it occurs and stop it. Our sophisticated neural networks flag unusual spending patterns that enable financial institutions to block authorizations for payment card transactions where fraud is suspected. These important fraud prevention tools, however, cannot be utilized on a global basis without cross-border data flows. Similarly, other businesses must be able to manage their global operations effectively and transfer both personal information, such as customer and employee data, as well as general business information, such as technical data, to their operations around the world in order to prevent fraud and ensure that consumer information is protected. Rules that limit businesses ability to effectively and efficiently prevent fraud or manage their business will stifle innovation, hurt U.S. business and will not lead to greater protection of consumers.

**Other Privacy Considerations**

In considering privacy and the Internet, there are a number of important considerations that should be weighed in developing a vision for an innovative but safe Internet and information-driven economy.

- Any new privacy framework or protection should preempt state laws and, in so doing, create a uniform national standard. If any changes are adopted, those changes should provide for a single national standard will provide all American consumers with the same protections no matter where they may reside. In addition, a single national standard will provide covered businesses with just one standard with which they must comply. If a federal a law is adopted that does not preempt state laws, the result will be inconsistent or conflicting standards. Moreover, businesses would have to adopt complex compliance plans based on where they operate or where their customers reside.

- In addition, any new privacy framework or protection should preserve the values that are derived from regulating privacy with an understanding of the industry to which that framework or protection will apply. Where there are strong sectoral regulators, those regulators should be responsible for oversight for the particular industry. For example, financial institutions, including banks, credit unions and broker-dealers, are subject to examination and oversight by various federal financial regulatory agencies.

The privacy issues that the U.S. Government is considering are complex. Moreover, working through these privacy issues across business models, technologies and industries will be both

time consuming and difficult. Nonetheless, the process is worth the effort and difficulty. Ultimately, consumers drive a significant portion of the U.S. economy. Visa works everyday to protect the trust of the consumers who carry Visa-branded payment cards, including through robust privacy and information security programs and practices. Visa would value the opportunity to work with Commerce to foster greater consumer trust in the use of their data, while also fostering innovation in both technology and business models that has made the U.S. economy the envy of the world.

* * * *

Visa appreciates the opportunity to comment on this important matter. If you have any questions concerning these comments or if we can otherwise be of assistance in connection with this matter, please do not hesitate to contact me at (650) 432-1167.

Sincerely,

Russell Schrader
Associate General Counsel and Chief Privacy Officer
Visa Inc.

**Response to the Notice of Inquiry on Information Privacy and Innovation in the Internet Economy by the US Department of Commerce**

The Department of Commerce's Internet Policy Task Force is conducting a review of the nexus between privacy policy and innovation in the Internet Economy. This document answers two questions posted in the Notice of Inquiry, based on 13 years of experience at the World Wide Web Consortium (W3C) related to privacy on the Web.



## I. Introduction

W3C is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. Led by Web inventor Tim Berners-Lee and CEO Jeffrey Jaffe, W3C's mission is to lead the Web to its full potential.

W3C efforts related to privacy on the Web began in 1997, when development started on the widely known Platform for Privacy Preferences (P3P), published as a Web Standard in 2002.

The W3C staff have been part of the broader privacy conversation throughout the last decade, and have participated in many different research projects on Privacy in the United States and in Europe, including the Transparent Accountable Datamining Initiative, Policy Aware Web, Theory and Practice of Accountable Systems, PRIME and PrimeLife. One important vehicle for making connections from research work to other work is the W3C Policy Languages Interest Group (PLING), which also helps to bridge communities fragmented around policy languages and access control. Findings from the research influenced the work carried out in other W3C Working Groups, but not to the extend we had hoped for.

The role of the standards W3C builds is increasingly broad: W3C is no longer tied to the document mindset of the early Web; instead, we build the standardized underpinnings for what looks increasingly like a Web operating system: General purpose data formats, general purpose communications frameworks, general purpose APIs that make device features accessible to the Web that had previously been outside the sandbox.

As we build and design advanced APIs that permit access to risky features, topics like the transparency of the data collection itself, limiting the scope of user errors, or the user's ability to recover from erroneously granted consent take center stage. These factors at times influence the design of APIs (does the user pass a selection of cards from his address book to a web site, or

does he grant the web site access to the address book). At other times, all we might be able to do in specifications is to sketch basic requirements, as the distinction between a privacy friendly and a dangerous implementation may be entirely dependent on the details of user interfaces and interactions, beyond the scope of what can be reasonably specified.

**II. Notice, choice, use-based models & accountability systems**

The Notice of Inquiry puts forward questions about **use-based privacy protection models** (including accountability systems) to overcome limitations of the **notice & choice model**.

Answer

**II.a Existing technologies**

For the comparison of these two models, it is useful identify the following phases in the "life-cycle" of personal information:

- collection
- primary use ("the primary reason personal data was requested")
- secondary ("opportunistic") use
- deletion

Notice & choice approaches involve the collection step. Use-based approaches limit primary and opportunistic uses of personal data by emphasizing technologies and promises that address the "back end" of commercial or benevolent endeavors.

While P3P was initially designed to help the notice & choice model by giving clear information to the user, it was later used to enable back end systems and middleware to help manage the promises made to consumers or business partners. This can be seen as a first attempt to provide technical support for use-based approaches. Since 2002, this notion has been pursued again and again in research:

- In the PRIME project, the notion of Sticky Policy appeared and was shown to work.
- In the TAMI project, researchers showed that manual and automatic re-use of personal information can be efficiently monitored and audited to determine whether such uses were reasonable and within the pre-defined boundaries.
- In the PrimeLife project, participants explored the efficient downstream data usage control if personal data is handed on to third parties.

The technologies discussed above primarily address privacy needs under the assumption that all parties are acting in good faith. Even without considering enforcement in the presence of

malicious actors, the technologies are often seen as complex, costly and expensive to implement. Data models have to be adapted, new business processes have to be designed, staff has to be trained. An investment of such order of magnitude is a challenge and has to be backed by potential benefits.

But while implementing these technologies may be expensive, that cost must be weighed against the cost (both risks and actual implementation cost) of doing nothing. A fair observation of the last ten years suggests that doing nothing has often won in this weighing. Doing nothing costs nothing to implement, has only a moderate impact on driving customers away, and does not constrain further opportunistic use by freely given commitments. The risk of non-compliance with regulations is often mitigated by weak enforcement of that regulation: Even given the strong European regulation implemented by data commissioners, the German statistics show 2.2 inspectors per 100.000 companies which results in an average control every 39,000 years. Given this low risk, investment in data usage control is improbable or will be cosmetic at best. We will see more incomprehensible statements on notice & choice augmented by further complicated statements on use-based permissions.

The scale of the Web is such that only scalable solutions that involve all the participating actors (commerce, consumers, and intermediaries) will work. This will need to be supported by the underlying technology.

Unless some economic incentives are given by the legal framework to invite companies to use the existing technology for privacy aware data management, intelligent data warehouses, and data mining technologies that take into account privacy, substantive change in current business practices is unlikely.

The current economic and legal environment has not provided incentives that would lead to the deployment of privacy enhancing, use-based technologies. As both the technological and legal framework is developed further, further research into the economics of personal information online will be crucial to achieve meaningful privacy. **Therefore, we encourage the DoC to push for further interdisciplinary research on Internet, economy and its relation to privacy in order to find means to encourage deployment of privacy enhancing technologies and have a greater buy-in from the commercial world.**

**II.b Challenges to technology enhanced notice, choice and use-based limitations**

If controlled by technology, use-based privacy restriction may hinder creative opportunistic re-use of data collections. Many of the inventions on the Internet of the past ten years were made based on creative re-use of existing information. A system — legal or technological — that constrains that creative re-use tends to put brakes on innovation. The challenge, therefore, is to balance privacy values and allowance for data re-use in a fair and reasonable way. In using personal data, how does society promote creativity while remaining responsive to privacy rights and expectations? Neither method, nor content of such reconciliation of interests are on the

horizon. More creativity and research is needed to find new approaches that respect the human right of privacy without blocking to road to more innovation based on data re-use and personalization. While basic rules for privacy may cut off the most blatant abuses, we have to remain careful not to stifle innovation.

**III. Usability and code as a new focus of action in the area of privacy**

What is the state of development of technologies and business methods aimed at: (1) Improving companies' ability to monitor and audit their compliance with their privacy policy and expressed user preferences; (2) using text analysis or similar technologies to provide privacy notices; and (3) enabling anonymized browsing, communication and authentication? Please describe any other ongoing efforts to develop privacy-enhancing technologies or processes of which the Commerce Department should be aware.

Answer

**III.a Investment into user interface research is needed**

Research and development of privacy enhanced data management technology is well under way. But progress in deployed technology is slow. The policy languages used so far are still too complex for mainstream consumption. They must be simplified to enable adoption. Given the complexity of the notion of Privacy, simple technology is hard. Therefore, more research is needed.

The theoretical background for descriptive policy languages and associated technologies is by now well-established. We are seeing new ideas emerge, such as splitting data base tables to control the access to knowledge. This can, e.g., be used in cloud scenarios to control privacy and secrecy. The foundations are in place (but not deployed yet) for the privacy-friendly exchange of data, tied to purposes, annotated with notification obligations, and access to one's data. Subject access API standardization may become a hot topic in the future.

Legal requirements on privacy-friendly behavior are high in some parts of the world, and expectations are close behind. But technology does not let us meet those expectations fully, especially within the European context. The nature of requirements tends to make already-complex privacy-enhancing technology even more complicated. Businesses do not want that complexity. They fear that privacy-enhancing technology might in fact drive away customers, instead of building their trust and attracting them.

"Identity" on the Internet and on the Web has been the subject of constant research and development for years. Solving the identity problem on the Web is seen as a major condition for new innovative services. The Internet identity system that takes off promises to bring profits magnified by the economic network effects for those who have pioneered it. Therefore, we observe fierce competition around the notion of identity, with numerous competing technologies

and companies aiming at wide deployment. Complex privacy-enhancing technologies will decrease the chances of wide deployment, and are therefore not found in widely-deployed identity systems.

Users might complain loudly at times, but ultimately use even privacy-unfriendly systems that enable desirable services. As long as there is no "giant oil spill," why should one really opt-out of disruptively useful innovations? There remains, thus, public unease without a compelling technological alternative.

Some services, such as social networking, rely on the users' sharing of personal data and profiles for their business models. Not surprisingly, privacy controls that once existed have eroded over the years. Where such steps crossed out of the public's comfort zone, the outcry was strong enough that "doing nothing" about privacy isn't an option any more. However, the actions taken in response show the tremendous difficulties to create useful user interfaces to privacy controls. Put to the point, privacy user interactions are currently developed through trial and error, where errors are detected through public outcry. How can businesses be encouraged to make a sustained investment into privacy technologies and research?

Experience with P3P and its deployment demonstrates some of the obstacles: P3P was a short and simple specification. Nevertheless, businesses were often reluctant to make simple, machine-readable declarations about their data usage. Mostly they preferred vague statements in human readable privacy policies written by lawyers for some perceived additional liability protection. The lesson is that fear of liability may well drive businesses away from the sort of clear and succinct statements that would convey a clear message to the user, whether or not those messages are mediated through a user agent that evaluates a machine-readable privacy policy. Regulation has to take into account the tension between usable privacy experiences on the one hand, and the fear of legal liability on the other hand.

Another element of the P3P experience may shed light on why PETs have not reached a significant market deployment. Considerable investment into the deployment of the P3P led to some modest success on the server side — data suggest that at one time, 28% of the top 1000 sites were using P3P. But P3P relies on efforts from both content providers (who put machine-readable statements on their site) and browsers (which mediate the user's experience based on some processing of privacy policies, e.g. by matching them to preferences). In the case of P3P, major browser vendors did not adopt the technology. Apart from the privacy bird plugin (first AT&T research, then Carnegie Mellon), there was only rudimentary support for P3P in user agents. Browsers mainly combined the compact policy format with a rudimentary user interface, thus increased the fuzziness of the privacy statement resulting in an increase of fear of liability. The resulting privacy messages were barely understandable for the average user.

The incentives for browser implementers are complex: beyond just implementing a policy protocol, they need to work out a meaningful user interaction with the policy, and they have an

interest in popular online services being usable and simple when accessed through their software. User interactions that were tried include:

- writing preferences and warning users when those aren't met – but users won't write preferences
- informing users of a human-readable form of the privacy policy – but users won't read policies
- making canned sets of preferences available for users to choose from – but users won't change defaults

At the same time, implementers will face the pressure to not make interactions appear "scary", even if they involve personal data. As a result, we see a landscape in which client implementations have turned away from implementing policy protocols. Instead, they focus on blacklisting known criminal players, and punting privacy decisions to individual web sites. There has been little further investment in the design of privacy policy related user interfaces in client software.

Sustainable online commerce requires sustained trust by users in their online experiences. A key piece of trust online is confidence that privacy expectations are met. Even when the provider acts in good faith, a consumer who does not understand the provider's effort, will not gain more trust, and might very well walk away. User trust requires user understanding. Privacy-related interactions need to be simple and understandable to everyday users. Unfortunately, today's interfaces tend to display large complex statements or technical jargon that nobody understands, if they say anything about privacy at all. Such incomprehensible messages neither improve privacy, nor increase the trust and confidence required for online transactions.

At this point, research into privacy user interfaces and experiences lags far behind user needs. Research investment is needed into simple, understandable user interfaces and experiences. While research in complex cryptographic primitives can lead to powerful technological enablers, development and deployment of simple user experiences are crucial in order to achieve practical privacy. We have revolutionized interfaces on mobile devices that can change direction if flipped, glow if poked, and so on, but that cannot answer important questions like "who knows where I am?" or "how do I limit who knows where I am?" Once more, what economic incentives would improve this situation and drive innovation? More research investment is urgently needed to develop *simple and helpful* user interfaces and experiences for privacy management.

**III.c. Regulation should allow for incremental improvements**

From the research projects done for the European Commission, we know how hard it can be to make software that is able to fulfill certain requirements established by law and regulation. The laws were not made with the available technology -- and the evolution of its use in the future --

in mind, but rather in the spirit of describing a desirable end state, based on a given time's culture of technology use. The expectation is that technology will ultimately fall in place. This approach is described with the phrase of technology neutral regulation. While technology neutrality is an important principle, having requirements in law and regulation that are very difficult to achieve with technology today (or that become obsolete in the future) will undermine small, incremental improvements toward better privacy protection, as these won't improve compliance. It would be worthwhile to try an interdisciplinary approach and to confront lawmakers and regulators with technologists to determine what is easily achievable and sufficiently simple to be put into the market. A measure, to be effective, has to be able to address the Web's massive scale. Only simple but intelligent rules and technologies — taking into account the human part of the system — can cope with this requirement.

---

*For questions about W3C or the answers here, please contact Rigo Wenning (rigo@w3.org)*

Walmart
Save money. Live better.

702 SW 8th Street
Bentonville, AR 72716
Phone 123.456.7890
Fax 123.456.7892
www.walmart.com

June 14, 2010

National Telecommunications Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Wal-mart Stores Inc. (Walmart) appreciates the opportunity to respond to the Department of Commerce National Telecommunications and Information Administration's Notice of Inquiry (NOI), "Information Privacy and Innovation in the Internet Economy." Walmart thanks the Department for examining this important issue.

In order to provide context, we first describe Walmart's engagement in this area. We then break our remarks into the following topics:

- The value of a principles-based approach to privacy;
- Key privacy principles and the continued value of notice and choice;
- Other relevant principles and comments on a use-based approach; and
- Jurisdictional and enforcement issues.

## Walmart's Role and Privacy Perspective

As the largest retailer and private employer in the U.S., with approximately 1.4 million employees and 140 million customers coming through U.S. stores every week, Walmart considers an array of privacy issues on a daily basis. Walmart approaches privacy from a very broad perspective. Walmart operations cover almost every conceivable privacy topic, channel, and geographical region. Walmart operations include:

- Operating as a "brick and mortar" retailer, with over 3500 outlets domestically.
- Operating as a leading online merchant through walmart.com. According to Hitwise, a service that measures online usage, Walmart.com is among the top five most visited ecommerce websites in 2009.

- Operating over 600 Sam's Clubs domestically, which offer a membership model for its customers.
- Conducting extensive global retail operations throughout the world, including Europe, Canada, Asia, and Central and South America.
- Communicating with our customers across multiple channels, e.g. via email, postal mail, mobile devices, websites, and our stores.
- Collecting and merging data through numerous sources, including customers themselves, third party sources, and technology such as websites.
- Providing a wide variety of products and services. Some of these are more regulated regarding privacy or personal data than others. Examples include health services (some of which are covered by HIPAA and some of which are not like personal health records); financial products and services governed by the Gramm-Leach-Bliley Act; sales of hunting and fishing licenses; and sales of over-the-counter products containing pseudoephedrine.
- Serving in a leadership role in technology, online or offline. Some of these technologies have privacy implications, including online advertising, Radio Frequency Identification (RFID), or mobile devices.

In sum, Walmart has a deep engagement with consumers in a variety of contexts. We have made it our business to understand what customers want. Consequently, we respectfully submit that Walmart has a strong understanding of not only the dynamics of compliance with myriad privacy requirements, but also what we see as the underlying goals of what privacy rules seek to accomplish for consumers.

Principles-Based Approach

As an initial matter, we note that the scope of the NOI focuses on the Internet, although many questions in the NOI have a wider application. We welcome this wider scope. Since the emergence of online behavioral advertising as a topic of legislative and regulatory interest, we have been concerned that policymakers evaluating privacy issues may narrow their focus to the practices and concerns relating to Internet practices. This can lead to less upfront involvement of other sectors that face similar privacy issues. However, inevitably, and correctly, other practices become part of the debate. It does not serve consumers or businesses well when these issues are bolted on late or later in the process. This can lead to inconsistent or skewed regulatory schemes that may fit poorly or be ineffective. For the vast majority of U.S. businesses, this could be cumbersome at best and unworkable at worst, and also likely will not address the underlying issues for consumers. It is thus imperative that, as privacy frameworks are developed, policy-makers take the time to

understand the impact to consumers and companies that have online as well as offline relationships.

In considering how to examine privacy effectively, Walmart favors a principles-based approach. We think this is the best way for privacy to work for companies and consumers. It also provides the right foundation to discuss global privacy issues with stakeholders in other countries. Having a set of framework principles in place that can be applied in many different contexts would provide an effective, consistent approach to privacy. A privacy regime based on a well-conceived set of principles could be applied to every new technology, every new marketing channel, and every new use of consumer information. Such a framework would impose coherent and predictable standards that are easily understood by both consumers and businesses. We believe that the more coherent the guidance, the better the customer communications and business compliance will be.

A principles-based approach to privacy is certainly not new. Indeed, it is how existing models are framed, including the FTC's Fair Information Practice Principles, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the APEC Privacy Framework. Focusing on core privacy principles would facilitate the creation of predictable standards, and help avoid repeatedly dedicating time and energy to the creation of ad hoc requirements to address emerging technologies or business activities. While it may be possible to devise customized requirements to address privacy issues on an individualized, technology-specific basis, we question the efficiency – and, more importantly, the outcome – of such an approach. Not only does it create difficulties for companies attempting to develop an overarching approach to privacy, it also puts consumers in the position of having to navigate a confusing maze of unpredictable standards.

As an example of a principle-based approach, last summer we updated our customer privacy policy for Walmart domestic operations. The updated policy is based on the Fair Information Practice Principles and developing industry standards and global guidelines. Our goal was to make the policy transparent, to meet best practices, and to be integrated across all business units and product offerings. This initiative gave us further insights into how to focus on underlying privacy principles and then to operationalize them.

Key Privacy Principles

We believe certain core principles round out a privacy framework. One way to think about privacy principles is from the consumer's point of view. There appears to be four distinct principles that inherently involve direct interaction between a consumer and a business. These principles are notice, choice, access/correction, and accountability. Other

privacy principles typically involve internal data practices. Each of these principles is discussed below.

Consumer Notice and Choice

As part of a principles-based approach, we would like to turn to the key aspects of notice and choice that were raised in the NOI. We understand that a growing topic in the public policy debate is whether a traditional privacy approach, including consumer notice and choice, is still valid as technology, business practices, and consumer expectations evolve. We do believe that notice and choice still have a central place. This is not to say that there are no other protections to consider as a framework is developed. But we should not lose sight of a key way that consumers interact with businesses. We believe that notice and choice are key elements of a principles-based approach that need to be flexibly applied among various technologies and to meet consumer needs. We offer the following examples to show the value of notice and choice.

As one example, Walmart has begun pilot programs with mobile messaging. These messages can alert customers that pharmacy prescriptions are ready for pick-up, or about special offers in a store. Notice and choice are essential to make mobile interactions work. Indeed, direct marketing efforts, and the laws and industry practices that bound them, operate on a notice and choice model. We are not aware of another model that could work well for direct marketing.

Another example concerns our experiences with the use of Electronic Product Code (EPC) technology. At the simplest level, EPC is the next generation bar code. Currently, EPC is primarily used to track certain case and pallets in the supply chain. When EPC may be offered on individual products on the sales floor, future potential consumer benefits are real and direct. Examples include receipt-less returns; product authenticity and traceability; and food and product safety. Even though EPC tags used in retail contain no personal data, we are building in privacy protections.[1] As a cornerstone of EPC development, Walmart is

[1] Walmart also follows industry standards and policy-maker guidance with regard to its EPC usage. Walmart follows the Guidelines on EPC for Consumer Products issued by GS1 EPCglobal, the standard-setting body for EPC, in 2003 with final adoption in 2005. We also adhere to the EU Commission Recommendation published in May 2009 regarding the implementation of privacy and data protection principles for applications supported by radio-frequency identification. This includes use of a Privacy Impact Assessment (PIA) tool.

designing its use to enable choice. The goal is to provide EPC tags that are readily removable from the product or packaging, such as by placement on the price tag, or that can be deactivated if embedded for those who are concerned. We believe that choice is the right model for this technology. Some, perhaps most, consumers will appreciate its benefits. Some will not. But ultimately consumers should be able to choose which they prefer.

There are certainly challenges to notice and choice. For notice, it can be difficult to establish when to provide it and what is the right content. We should be careful to avoid prescribing notice with only certain channels in mind. For example, notice requirements that essentially require serving a pop-up on a website, or that require a template based on mail notices, may not work in other environments. The more specific the requirement, the less likely it will work in different contexts or technologies, and the strictures may also not serve the intended purpose. As another example, in terms of timing, it may only be feasible to provide notice close in time but not before data collection (think of security cameras in stores). Perhaps a better terminology is openness. This would demonstrate a company's commitment to providing basic and also complete information about data practices. It could encompass such items as immediate notice, layered notice, and also availability of the full policy based on a consumer's interest. Effective notice should cover both how consumers will know technology or certain business activities are in operation – and also how they can understand what the technologies or practices mean. Fundamentally, however, consumers should have access to information about business practices.

Regarding choice, the most basic challenge is being clear about when choice should apply. Clearly choice is appropriate for direct marketing. In our discussion of EPC, we have also provided an example related to removing or disabling a technology. But in what other circumstances should choice apply – e.g. data sharing, social media, geolocation – and what is the underlying principle? Unless choice is to be removed from a privacy framework – which seems unlikely given its centrality to direct marketing and customer relations – there must be clarity about when it applies. Otherwise there will be a murky standard that will be hard to explain and offer to customers and harder to implement.

Other Principles and a Use-Based Approach

In addition to notice and choice, other privacy principles include access/correction, accountability, and data management. As we understand and apply an access principle, consumers should be able to find out what information companies maintain about them, and request correction of the information. If the access requests are administratively burdensome, and involve non-sensitive data, the company should be able to respond by describing the types of data it typically maintains. If a consumer requests corrections,

companies should make the changes or explain to the consumer why a correction could not be made. Companies can impose reasonable authentication and other mechanisms to support access and correction requests.

Companies also should be accountable for compliance with privacy principles. Besides internal governance structures, accountability also includes how companies offer consumers a redress mechanism for their questions or concerns. Retailers deal with consumer questions and requests on a daily basis and have been doing so for years. It is part of the business-consumer relationship to respond to consumer wants and needs. We make it a priority to respond fully and timely to the customer inquiries we receive about privacy.

Other privacy principles tend to relate to internal data management. These principles could be encompassed under an umbrella principle related to information management or responsible uses. As examples, these include data integrity, security, disposition, and data uses. We agree that terminology relating to primary and secondary purposes has outlived its usefulness, and in fact probably never reflected business realities. The fact is that information is often collected for multiple purposes or uses. Certain groups, like the Centre for Information Policy and the Business Forum for Consumer Privacy, have done excellent work examining and describing common legitimate business purposes. This work is especially helpful as policy-makers consider how to frame principles across different business models. For instance, notice and choice may be more relevant for companies with direct B-C relationships, whereas a used-based model may be more effective for companies e.g. that perform data brokerage activities.

We offer a couple of caveats regarding a use-based framework. First, as discussed above, careful consideration needs to be given to how to incorporate notice and choice principles. Second, how to implement a use-based model needs consideration. We sometimes hear the FCRA raised as a workable model for used-based principles. The FCRA may well be a good model for sensitive data that is used for high impact activities like offers of credit or employment. However, we question whether that sort of model is appropriate for non-sensitive contact information used for lower impact activities like data analytics or marketing. It may well set up a large compliance burden and costs that produce little or no value for consumers. Rather, a use-based model should set forth appropriate criteria to which companies can adhere without unnecessary complexity.

Jurisdiction and Enforcement

The Department raises a number of questions about the impact of privacy rules being set by a number of different jurisdictions – state, federal, global – and how they can be broad-based or sectoral. We believe that a framework that is principles-based can do a great

deal to harmonize these different rules. We may find that the differences are not as great as first believed. We do believe federal standards are more appropriate, especially in interstate commerce areas like website operations, and also enable clearer conversations with our global partners.

As policy-makers work through jurisdictional issues, we wish to draw attention to two areas. First, careful consideration needs to be given to accommodating existing laws, especially sectoral laws. It would be simpler, and certainly convenient, to provide that a framework sits on top of and does not impact these laws. However, this is easier said than done. It could lead to different and perhaps conflicting requirements applying to the same data, which would be problematic for business and consumers.

Second, consideration should be given to the best methods to enforce a privacy framework. A common recent trend, at least in part, is to propose FTC and state AG enforcement. We think that can be a workable model. However, an area of concern is potential penalties. One advantage to a principles-based approach is it allows policy-makers to focus on the outcomes or impacts that are important to consumers—this helps set the framework. Another advantage is that, as it provides insights into the outcomes or impacts to avoid or minimize, this should also help guide enforcement parameters. We think it may be inappropriate to apply a simple formula of a dollar penalty per violation in all circumstances. Such a regime may make sense, for instance, in a direct marketing situation, where illegal conduct directly touches consumers and the sanction serves to penalize improper profit. However, if a framework is intended to cover the broad range of privacy issues, like responsible data management and disposal, we wonder if this formula makes sense in all contexts. As an example, if paper is not properly shredded before it is recycled, or if access controls are not properly implemented initially, there may be a violation of company procedures but with low or minimal impact if corrected. A per violation penalty is hard to envision – how do you measure each violation – and appears to impose strict liability unrelated to consequence. Just like with other aspects of a privacy framework, enforcement and penalties need careful consideration as well.

## Conclusion

The Department's final question is how can it help address issues raised in the NOI. We believe that the Department can help by continuing this effort and remaining engaged in the privacy debate. This will help the U.S. framework as well as the dialogue within the global community. Walmart welcomes the Department's participation. Please feel free to contact Zoe Strickland, Vice-President, Chief Privacy Officer, at zoe.strickland@wal-mart.com with any questions or comments.

zixcorp

June 28, 2010

Via Email: privacy-noi-2010@ntia.doc.gov

Internet Policy Task Force
National Telecommunications and Information Administration
U.S. Department of Commerce
Room 4725
1401 Constitution Avenue, NW
Washington, DC 20230

Subject: Notice of Inquiry

Ladies and Gentlemen:

This letter responds to the request by the Department of Commerce's Internet Policy Task Force (Task Force) for public comment by Internet stakeholders on the impact of current privacy laws on the pace of innovation in the information economy and whether those laws serve consumer interests and fundamental democratic values.

## Who we are

Zix Corporation is the market leader of email encryption services. We provide secure email services to more than 1,200 hospitals and 1,300 financial institutions, including some of the nation's most influential companies. We also secure email for federal, state and local government organizations, including the United States Treasury Department and the Securities and Exchange Commission.

## The Role of Email in Internet Commerce

We agree with the Task Force's statement that "*Commerce today depends on online communication and the transmission of significant amounts of data*." Global business today is increasingly based on electronic commerce. Online communication and data transfers via the Internet enable commerce at a pace that is increasingly instantaneous and borderless. Much of the information being communicated over the Internet for business and personal use takes the form of electronic mail messages – "email."

Email is a principle consumer and business use of the Internet. According to Wall Street Research, the number of email users worldwide is expected to grow to 1.6 billion by 2011. In the United States, 91% of Internet users have sent or read email online and 56% of Internet users do so daily. Access to the Internet is nearly universal in the U.S., and it is increasingly available to consumers using mobile devices. Email is the main content type accessed by 44% of mobile Internet subscribers via their smart phones.

Email is extraordinarily simple to use, ubiquitous and flexible. There are a variety of email applications for desktop, laptop and mobile devices. Email can be retrieved via an internet browser using a shared computer. Email facilitates the rapid exchange of all types of information in real

time among multiple participants. It also serves as a file transport tool, allowing senders to attach a variety of document formats, images and other files. For all these reasons email has become an integral part of electronic commerce. Email is the primary method that businesses and individuals use to exchange information.

## Need for Consumer Confidence in Internet Data Privacy

We agree with the Task Force's statement that "*Internet commerce is dependent on consumer participation, consumers must be able to trust that their personal information is protected online and securely maintained.*" Moreover, that statement is equally true whether the information is "at rest" on an enterprise's server or "in transit" over the Internet. For electronic commerce to continue to flourish, consumers must have confidence that confidential information they send, receive and store online will remain secure and private.

When consumers purchase goods or services online, their transactions are frequently confirmed and detailed in email receipts. Consumers provide email addresses to subscribe to information delivered periodically by email. Becoming a participant in social media sites or other online communities requires the individual to provide a valid email address and private messages from other users of those sites may be transmitted via email.

Despite their including confidential content, emails in transit are often stored on multiple servers, and the content may be "in the open" so that the message content can be intercepted and viewed by unauthorized persons and used in ways unintended by the sender and recipient. Email senders should, therefore, be encouraged to take steps to ensure that the content of email messages may be read only by the intended recipients.

One proven method of enhancing consumer privacy and confidence in e-commerce is through the use of encrypted email. As described below, new technologies make using encrypted email simple and efficient.

## Expectations of Privacy in Email Communications

We note the comment submitted by Robert Sprague, indicating that courts assume that a person loses a reasonable expectation of privacy in email messages once they are sent to and received by a third party (citing *Rehberg v. Paulk*, 598 F.3d 1268 (11th Cir. 2010)). We assert that conclusion should not be true for messages sent via encrypted email, where the sender has taken additional steps to protect the content of the email message and thereby continues to have a reasonable expectation of privacy.

Furthermore, we believe the vast majority o f U.S. consumers would be shocked to learn that their email communications are considered by some courts to be less private than a postcard sent via mail. Consumers in the U.S. have reasonable expectations of privacy in the content of their email messages similar to their privacy expectations in telephone communications. For example, the Electronic Communications Privacy Act and state wiretap laws create the expectation that the content of email communications is secure and private.

In the early days of email services, Internet Service Providers (ISPs) stored messages on their servers only until the user downloaded the message to a personal computer. Once

downloaded, the message was deleted from the server. Increasingly, however, email is being offered as a hosted service by ISPs and others. The content of emails can be stored by the provider indefinitely and accessed by the user remotely "in the cloud," rather than being downloaded and stored offline.

The fact that emails are increasingly accessed "in the cloud" should not diminish consumers' reasonable expectation of privacy in those communications. Consumers do not consider their stored emails to be publicly available or "in plain view" whether they are locally downloaded or they are stored on a server operated by an email services provider. They most likely do not expect their email provider to scan the content of their emails to glean insights for targeted behavioral marketing or other purposes not intended by either the sender or recipient.

We also note Mr. Sprague's observation that current privacy law does not necessarily protect information derived from the accumulation of data. "In other words, when individuals voluntarily relinquish their right to privacy over small, unique pieces of information, an analysis of accumulated data may generate a much fuller profile, which itself is not protected because the underlying data are not protected (citing *Solove, D.* 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy, *Stanford Law Review* 53: 1393-1462)." As we describe below, this is equally true with respect to information aggregated from the content of unsecured emails.

## The Scope of Private Data in Email

An email address is unique to the individual or organization that creates it. The discussion draft privacy legislation published on May 4, 2010 by Representative Rick Boucher, Chairman, and Cliff Stearns, Ranking Member, of the House Energy and Commerce Committee's Subcommittee on Communications, Technology, and the Internet, recognizes in section 2(5)(D) that an email address should be protected as "covered information" because it can uniquely indentify a sender.

The types of "private" information that may be contained in email goes beyond ordinary concepts of Personally Identifiable Information (PII) like a driver's license number or social security number. In nearly every e-commerce interaction, individuals provide an email address together with their name, address and often their credit card information.

Access to an email account permits one to know a considerable amount of private information about the email account holder. An individual's email address can become inexorably linked to private details of that individual's lifestyle and behavior. For example, emails may divulge what medications, products and services the individual purchased online; where and to whom those items were shipped; movies and music they downloaded; travel arrangements they made; books, magazines and newspapers they read; sexual orientation, and their membership in professional, political, religious, ethnic and social groups. An individual's email account is a portal into that person's lifestyle. The content of email, individually or in the aggregate, can expose fundamentally private information about the individual.

Contractual usage restrictions and privacy policies, particularly when they may be periodically revised in ways adverse to individual privacy, have not proven to be effective in protecting consumer's confidential information. Although it is possible for a consumer to "opt out"

by changing to an email provider whose policies are more protective of individual rights, it is impractical for consumers to routinely change email addresses because of the time and effort required to provide the new email address to all of their personal and business contacts, update their website subscriptions, etc. Moreover, the notion of "informed consent" presumes that consumers actually understand how data service providers utilize and re-purpose the personal data that they obtain in providing services, and the implications of how their personal data might be utilized.

Technological privacy solutions are far more effective in protecting individual rights than are policy-based usage limitations.

## New Privacy-Enhancing Technologies and Information Management Processes

### How Email Encryption Protects Privacy

Data encryption can make the contents of every email, both the message text and any attachments, virtually indecipherable to unauthorized individuals. Encryption uses a complex mathematical equation to convert the original email content into an information package that cannot be read until the intended recipient unlocks the message. Email is encrypted to meet standards set by The National Institute of Standards and Technology, which are deemed adequate to protect the content from malicious individuals. So, as a practical matter, if an unauthorized individual intercepts a copy of an encrypted email while it is moving across the internet or while it is stored in message archives, the unauthorized individual simply will not be able to read the message contents.

The U.S. government and state governments have acknowledged that encryption of email is an effective means of protecting confidential information. For example, a recent Massachusetts regulation requires for healthcare providers the "encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly."

### Automated Policy-Driven Email Encryption

A law or policy that relies on employees not to send sensitive information via "open" email is not practically effective to protect consumer privacy. Even if full compliance could be ensured within an enterprise's own workforce, external participants such as consultants may be tempted to ignore the policy in favor of the convenience and efficiency of email communication.

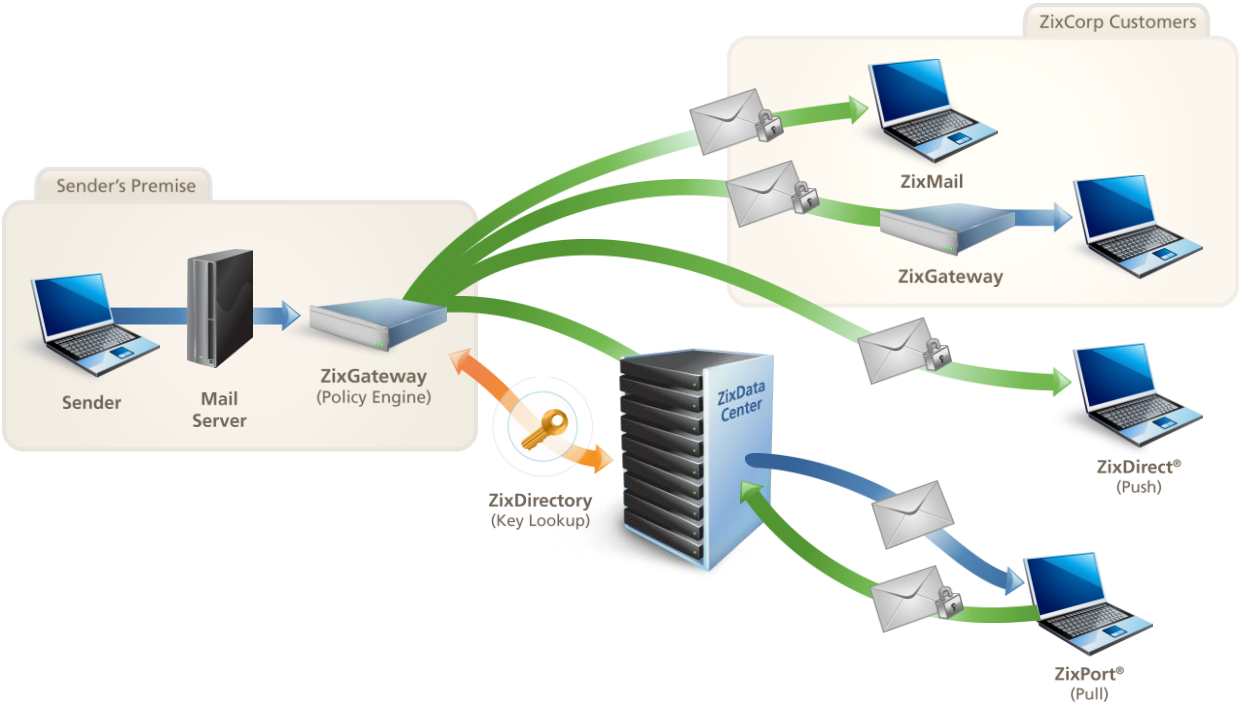
Automated, policy-driven email encryption offers a privacy solution that facilitates compliance with national and state privacy regulations as well as voluntary enterprise practices. An enterprise can adopt a "policy" that prescribes what email must be encrypted based on content, attachments, email address or other factors.

A compliance "lexicon" is developed that examines the message subject, text and non-binary attachments for content that policy dictates should be encrypted for confidentiality – including personal privacy concerns. An electronic appliance on the enterprise's email server inspects each outbound email and its attachments to see if the adopted policy and lexicon requires

that the message be encrypted. If the policy applies, the appliance automatically encrypts the message before sending it to the recipients.

At an enterprise that uses automated, policy-driven email encryption, the employees do not have to make judgment calls about whether content is private. The employees don't need to remember to secure sensitive email content. Confidential messages are automatically encrypted. Similarly, when encrypted messages are delivered to the appliance, it automatically decrypts inbound messages and delivers them to enterprise recipients in the clear. In that way, the encryption of private information is "transparent" to the enterprise users behind the firewall. Intended recipients may not even realize that the information was automatically protected from malicious eyes as it traveled across the internet.

For example, our *ZixGateway*SM users experience simple, automatic and totally transparent email encryption when exchanging secure information with other *ZixGateway* customers. Consumers and other recipients receive via the *Best Method of Delivery*SM either an encrypted *ZixDirect*® email or an open email directing them to retrieve an encrypted *ZixPort*® message from our secure *ZixMessageCenter*SM.




**Automated Inspection of Inbound Email**

An electronic appliance can scan incoming email to identify message content and attachments that should have been encrypted by external senders for privacy law or policy compliance, but that were not encrypted and potentially expose private information to a data breach. By identifying these policy lapses, an organization using automated inspection of inbound email can address the attendant privacy and security issues with the external senders.

An electronic appliance uses the enterprise's compliance lexicon to examine the inbound messages in the same way an appliance is used for policy-driven encrypted outbound email. If unprotected private information is detected, the appliance notifies the appropriate internal compliance and data security managers and provides reports logging the details of inbound vulnerabilities, so managers can take appropriate action with senders of unprotected email. For example, our *ZixGateway* Inbound service can help an enterprise ensure that its business associates are taking appropriate steps to protect private information.

**Secure Messaging Directory in the Cloud**

Conventional email encryption solutions can be difficult to implement and maintain because they require the sender to manage encryption keys for each recipient organization or user. By enabling a shared directory "in the cloud" senders don't have to create and manage encryption keys for each individual or organization with which they communicate. For example, our *ZixDirectory*™ connects more than 21 million members to enable secure communication among communities of interest, including healthcare, financial services and government. Users can transparently send and receive encrypted emails without having to manage public encryption keys or exchange certificates. By providing customers with an automated directory service in the cloud, solutions such as *ZixDirectory* greatly reduce the typical cost and complexity associated with email encryption solutions.

## Conclusion

Electronic commerce relies greatly on email. Email is a principle consumer and business use of the Internet. Email is frequently used to transmit details of online memberships, subscriptions and transactions. The content of email can expose fundamentally private information about consumers, including purchases and website memberships. Consumers must be able to trust that their personal information associated with their email address, as well as personal information transmitted via email, remains secure. Automated encryption of email provides an effective, simple means of protecting personal information and enhancing consumer privacy. The use of automated email encryption technology should be encouraged by governments to enable electronic commerce while simultaneously protecting consumer privacy.

Respectfully submitted,

James F. Brashear
General Counsel
Zix Corporation