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of Inquiry ("NOI") as well as present a ninth topic – the impact on economic growth and innovation of unclear and outdated rules for access to consumer data by the US government.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.