KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

BEFORE THE DEPARTMENT OF COMMERCE

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

IN THE MATTER OF

INFORMATION PRIVACY AND INNOVATION IN THE INTERNET ECONOMY

DOCKET NO. 101214614–0614–01

RIN 0660–XA22

January 28, 2011

Introduction

The Center for Democracy & Technology (CDT) appreciates this opportunity to respond to the questions posed in the Internet Policy Task Force "Green Paper" on commercial data privacy. CDT applauds the Task Force's outstanding work on this report and believes it to be an important step toward a long overdue comprehensive privacy protection framework in this country. We are especially pleased to see that the administration is prepared to take on a leadership role on the issue of privacy, both domestically and internationally. It is noteworthy that the Task Force has recommended the adoption of the full range of Fair Information Practice Principles across all industries that collect and use consumer data. Fundamentally, CDT believes that this can only be accomplished through baseline privacy legislation, and we urge that approach as the appropriate means to implement a new privacy protection framework. We respectfully submit these comments to guide the Task Force's development of its final White Paper report.

Response to Questions Posed by the Task Force

(1) The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs).

(a) Should baseline commercial data privacy principles, such as the comprehensive FIPPs, be enacted by statute or through other formal means to address how current privacy law is enforced?

CDT has long argued and continues to believe that the only way to implement a commercial data privacy framework that fully and effectively incorporates all the Fair Information Practice Principles is through baseline privacy legislation.[1] While CDT supports the Department of Commerce approach of developing a multi-stakeholder process to help devise industry-specific implementations of privacy rules,[2] it will be difficult if not impossible to incentivize all industry players to agree and adhere to such rules unless legislation establishes a common floor of privacy protection. In the modern technology landscape, increasingly smaller, edge players such as mobile "apps" developers are gaining access to large amounts of sensitive consumer information.[3] Voluntary standards are unlikely to encompass all the new participants in the increasingly complex information ecosystem.[4] Furthermore, without baseline protections that apply to everyone, new uses of consumer information will start out with the current "no rules" default, and regulators and advocates will be forced to play catch up and try to retroactively append privacy protections to engrained business practices.[5]

Absent a legislated incentive to develop strong and privacy-protective rules, we do not believe companies will adopt an appropriate level of protection in a purely voluntary framework. Indeed, "voluntary and enforceable codes of conduct" is *the privacy protection framework that we have today,* which both the FTC and the Department of Commerce Task Force have found to be inadequate. Privacy policies and promises to adhere to industry codes already exist and are already subject to enforcement under Section 5 of the FTC Act or comparable state law.[6] As the Green Paper and the FTC privacy report describe in detail, this framework has failed consumers and businesses. And the situation is getting worse: Given trends in technology and business practices, one must conclude that consumers today have less control over a far greater range of their personal information than they did even just a couple of years ago.[7]

The failure of voluntary self-regulation has been bad for individuals, but it also poses risks for businesses as well. Individual and enterprise-level customers have been reluctant to adopt new cloud-based and location services (*see infra*, §10(a)), and consumers are demonstrating

---

[1] *See, e.g.,* Statement of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology, Before the Senate Commerce, Science & Transportation Committee, "Privacy Implications of Online Advertising" (July 9, 2008) *available at* http://www.cdt.org/files/pdfs/20080709harri.pdf.

[2] *See, e.g.,* Addendum to Testimony of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection on "The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation" (July 22, 2010) *available at* http://cdt.org/files/pdfs/Privacy bills comparison chart_CDT_0.pdf.

[3] Scott Turm and Yukari Iwatani Kane, *Your Apps Are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.htm.

[4] Even if the best industry participants were to agree to adhere to a strict privacy protective code and to exclude companies who do not meet the same standards, they may find their "voluntary" approach attacked by non-participants as an exclusionary tactic in violation of antitrust laws.

[5] *See, e.g.,* Turm, *supra* note 3; Ashley Yeager, *Researchers Find Phone Apps Sending Data Without Notification*, Office of News & Communications, Duke University, http://www.dukenews.duke.edu/2010/09/TaintDroid.html (last visited Jan. 27, 2011).

[6] *See* Act of March 21, 1938, ch. 49, § 3, 52 Stat. 111 (codified at 15 U.S.C. § 45(a)(1) (1994)); N.Y. GEN. BUS. L. §§ 349, 350 (Supp. 1999).

[7] *See, e.g.,* Emily Steel, *A Web Pioneer Profiles Users by Name*, THE WALL STREET JOURNAL, October 25, 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

increasing apprehensiveness about their privacy.[8] Moreover, while the United States is currently the unquestioned leader in providing cloud-based services, even companies willing to adopt the most stringent privacy policies find that overseas customers are skeptical of those assurances because of the lack of U.S. privacy laws to back them up.[9] Furthermore, without fundamental baseline protections, the United States loses credibility in its push for the harmonization of global privacy laws and for the easing of restrictions on cross-border data flows. If the United States cannot argue from a position of leadership on privacy, the global default rules will tend necessarily toward the more rigid European model. This is why several leading cloud computing companies such as Microsoft, Intel, and eBay explicitly endorsed the baseline privacy protection legislation introduced by Congressman Bobby Rush last year,[10] and why the call for a legislative solution had "broad support" from commenters to the Department of Commerce's Notice of Inquiry.[11]

It is difficult to envision any other mechanism (formal or informal) that could provide the same clarity and incentives as a baseline law. The Federal Trade Commission lacks standard Administrative Procedure Act rulemaking authority, and consumers and businesses cannot reasonably be expected to wait the several years that would be necessary to complete the alternative Magnusson-Moss process for rulemaking.[12] The rapid pace of technology innovation (and accompanying threats to privacy) requires a more immediate (but also more flexible) solution. That combination of responsiveness and flexibility can be found in the concept of baseline legislation implemented through industry "safe harbor" standards.

> *(b) How should baseline privacy principles be enforced? Should they be enforced by non-governmental entities in addition to being the basis for FTC enforcement action?*

While industry safe harbor systems should include an industry-based enforcement mechanism, the Federal Trade Commission should have robust enforcement authority under any privacy protection framework.

---

[8] *See, e.g.,* Edward C. Baig, *Internet users say, Don't track me*, USA TODAY, December 14, 2010, http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm; Scott Cleland, *Americans want online privacy –per new Zogby poll*, The Precursor Blog, June 8, 2010, http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll.

[9] Viviane Reding, *The Digital Forecast is Cloudy*, THE WALL STREET JOURNAL, January 25, 2011, http://online.wsj.com/article/SB10001424052748703555804576101591825228076.html.

[10] Letter from David A. Hoffman, Director of Security Policy and Global Privacy Officer, Intel Corporation, et. al., to The Honorable Bobby L. Rush, Chairman, Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, United States House of Representatives, et. al. (Oct. 4, 2010) *available at* http://blogs.intel.com/policy/HR 5770 Support Letter.pdf.

[11] Department of Commerce (Internet Policy Task Force), *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010) *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[12] *See* Magnuson-Moss Warranty Federal Trade Commission Improvement Act, Pub. L. 93-637 (1975) (codified as 15 U.S.C. § 2301).

In recent years, despite significant limitations in its authority absent a specific privacy law, the FTC's Consumer Protection Bureau has brought important privacy protection actions,[13] and consequently it has the experience and expertise needed to enforce new substantive privacy protections. However, the FTC currently lacks the ability to obtain statutory penalties for privacy violations brought under its Section 5 authority, and as a result, the FTC has in many cases been unable to hold companies fully accountable for their actions.[14] Any new privacy protection legal framework should give the FTC the ability to obtain penalties for violations of FIPPs-based rules, whether those rules are embodied directly in regulations or adopted by companies as part of a safe harbor or multi-stakeholder program.

In addition to the Federal Trade Commission, state Attorneys General should also be given the ability to enforce and obtain statutory penalties for violations of a FIPPS-based federal law. State enforcers have been on the vanguard in bringing privacy protection actions in recent years, and they must be part of any future privacy enforcement regime. For more discussion of the role states should play under a privacy protection framework, *see infra*, § 9(c).

If coregulatory safe harbor programs are a feature of a baseline law, those programs, in order to gain safe harbor status, must be subject to FTC review and approval to ensure that they include substantive privacy protections at least as strong as those required by the baseline law and must be backed up by a robust auditing and self-regulatory enforcement regime. CDT endorsed such a coregulatory approach in the BEST PRACTICES bill introduced in the last Congress.[15] However, delegating enforcement of safe harbor rules entirely to non-governmental bodies could debilitate any privacy protection framework and would fail to assuage the privacy concerns of foreign customers. Therefore, the FTC and state Attorneys General should always retain the authority to bring actions against companies who certify that they are in compliance with an approved code of conduct but in fact are not.

> *(c) As policymakers consider baseline commercial data privacy legislation, should they seek to grant the FTC the authority to issue more detailed rules? What criteria are useful for deciding which FIPPs require further specification through rulemaking under the Administrative Procedure Act?*

CDT has long advocated for the restoring APA rulemaking authority to the Federal Trade Commission,[16] and a grant of such authority should be part of any baseline privacy law. Both of the draft baseline privacy bills that were discussed during the last Congress included general grants to the Federal Trade Commission of rulemaking authority in order to implement the bills'

---

[13] *See* Complaint, In the Matter of Sears Holdings Management Corporation, No. C-4264 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf; Press Release, Federal Trade Commission, LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False (Mar. 9, 2010) *available at* http://www.ftc.gov/opa/2010/03/lifelock.shtm; Press Release, Federal Trade Commission, Online Data Broker Settles FTC Charges Privacy Pledges Were Deceptive (Sept. 22, 2010) *available at* http://www.ftc.gov/opa/2010/09/ussearch.shtm. *See also* Comments of the Center for Democracy & Technology, FTC Consumer Roundtable, November 6, 2009 *available at* http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.

[14] *See, e.g.,* Press Release, Federal Trade Commission, FTC Settles with Company that Failed to Tell Parents that Children's Information Would be Disclosed to Marketers (Nov. 30, 2010) *available at* http://www.ftc.gov/opa/2010/11/echometrix.shtm; Press Release, Federal Trade Commission, Advertising.com Settles FTC Adware Charges (Aug. 3, 2010) *available at* http://www.ftc.gov/opa/2005/08/spyblast.shtm.

[15] *See* Harris, *supra* notes 1 and 2.

[16] *See*, *e.g.,* Comments of the Center for Democracy, *supra* note 13.

protections.[17] Given the rapidly changing technological environment, the FTC should have the ability to issue regulations to adapt privacy protections to new challenges. If the FTC is not given the full set of tools to implement privacy protections, the United States may have difficulty developing international confidence in any new privacy protection framework.

However, there is a difference between *empowering* the FTC to issue regulations and *mandating* in the law that it issue such regulations immediately. Some of the Fair Information Practice Principles could benefit from prompt rulemaking to achieve standardization across industries. For example, Transparency is one area where it may make sense for legislation to direct the FTC to develop consistent short form notices or iconography to better inform consumers about companies' privacy practices. Similarly, persistent and uniform models for exercising individual choice could serve business and consumers as well.[18] For other FIPPs, it may be best to leave the decision as to whether to issue implementing regulations to the discretion of the FTC.

If a baseline privacy law incorporates safe harbor programs, the FTC may have less need to issue detailed regulations, as the expectation for coregulatory programs is that much of the "on-the-ground" rulemaking and implementation of privacy protections would take place within the safe harbor programs.[19] However, if the FTC deems that either cross-industry or industry-specific protections for consumers are inadequate, it should have the authority to issue new regulations to clarify the scope of law's protections.

(d) Should baseline commercial data privacy legislation include a private right of action?

Private lawsuits have played an essential role in the development of privacy protections in recent years. Private litigants brought actions against adware companies before either state or federal regulators could do so.[20] Recent class action suits against companies that surreptitiously use "local storage" files to track consumers who delete cookies have caused many companies to abandon such practices, again before regulators acted. Private suits were also the only actions taken against Facebook and Google over the privacy violations accompanying the release of their Beacon and Buzz products.[21] In a quickly innovating technological environment, overburdened regulators may not always be able to bring timely enforcement actions against emerging bad practices. Private lawsuits thus can serve a useful function as an element of enforcement.

Assuming a robust coregulatory structure that puts into place rigorous privacy protections for participants, it may be appropriate to grant compliant participants safe harbor from private

---

[17] BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009); Boucher-Stearns Privacy Bill Staff Discussion Draft, May 3, 2010 *available at* http://www.nciss.com/legislation/BoucherStearnsprivacydiscussiondraft.pdf.

[18] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 57-63 (Dec. 1, 2010) *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[19] Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY (forthcoming Winter 2011), 22-23 *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275.

[20] Wendy Davis, *Settlement Reached In Adware Suit*, Online Media Daily, March 16, 2006, http://www.mediapost.com/publications/index.cfm?fa=Articles.showArticle&art_aid=41054.

[21] *See* Caroline McCarthy, *Facebook Beacon has poked its last*, CNET NEWS, September 18, 2009, http://news.cnet.com/8301-13577_3-10357107-36.html; Mark Hackman, *Google Alerts Users of Google Buzz Settlement*, PCMAG, November 3, 2010, http://www.pcmag.com/article2/0,2817,2372027,00.asp.

lawsuits. This was the approach taken in the BEST PRACTICES bill introduced in the House of Representatives last year,[22] and it could provide a compelling reason for companies to develop and adopt meaningful privacy protection standards subject to the approval of the Federal Trade Commission. However, participants who fail to adhere to the safe harbor program's requirements and companies who do not join such a program should remain subject to private enforcement of privacy rights.

*(2) To meet the unique challenges of information intensive environments, FIPPs regarding **enhancing transparency**; encouraging greater detail in **purpose specification** and **use limitations**; and fostering the development of **evaluation** and **accountability** should receive high priority.*

> *(a) What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.*

So far, voluntary self-regulatory efforts by industry have not resulted in improved transparency for consumers. Incomprehensible and evasive privacy policies remain the norm.[23] Voluntary efforts to standardize privacy policies in a machine-readable format have also failed.[24] Industry coalition efforts such as the Online Privacy Alliance and the Network Advertising Initiative have failed to develop and generate consensus for consistent and understandable disclosures about consumer data collection and usage.[25]

More recently, the Digital Advertising Alliance has announced promising plans to introduce common iconography into online ads and to make available information about the sources of information behind those ads.[26] However, this self-regulatory effort has still not been publicly deployed on any wide scale after years of development, and not all the details about what information will be made available to consumers are known. Moreover, this transparency effort only pertains to online behavioral advertising. CDT is unaware of any comparable self-regulatory effort to improve transparency in any other industry.

Based on this experience, it appears that several things are needed to achieve better transparency. First is the adoption of baseline legislation expressly making comprehensible notice a requirement. (Policymakers should not forget that transparency is not a legal requirement now across all sectors, which is certainly one reason why there has not been more progress in achieving it.) Since such legislation could not possibly define exactly how to implement transparency, there would have to be industry-based efforts to provide those details. As we have expressed throughout these comments, such efforts should be subject to FTC safe harbor review and enforcement. And the FTC should have regulatory authority to fill any gaps where a sector has not developed its own standards or where cross-cutting issues require

---

[22] BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009).

[23] *See generally, e.g.,* CyLab Usable Privacy and Security (CUPS) Laboratory Website, http://cups.cs.cmu.edu/ (last visited Jan. 27, 2010).

[24] *See* Ari Schwartz, *Looking Back at P3P: Lessons for the Future* (Nov. 2009), *available at* http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

[25] *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439 (2011).

[26] *See* The Self-Regulatory Program for Behavioral Advertising Website, http:www/aboutads.info/ (last visited Jan. 27, 2010).

attention. The issue of transparency, like others related to privacy, can be effectively dealt with only by a combination of baseline legislated requirements, coregulatory industry standards, and FTC backstop enforcement and rulemaking.

(b) What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

We do not see PIAs mainly as a transparency mechanism. Instead, the main function of PIAs is to lead companies to proactively consider and address privacy risks in new products. PIAs can help to identify potential privacy problems in a product that is under development so that companies can fix those problems before the product is introduced to the market.[27] PIAs may have a secondary benefit in terms of transparency by helping all components involved with development and marketing of a new product or service to understand what data it will collect and how that data will be used, stored and disclosed, and that internal understanding may help in explaining the product to consumers when it is launched. However, PIAs should not be conceived as just another form of notice for consumers, but rather as a tool to help companies think about privacy during the product design and development processes.

(c) What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

There are at least three elements of a meaningful PIA in the commercial context.

First, PIA processes should begin at the start of the design cycle. The earlier problems are identified, the lower the cost of the solution.[28] Microsoft's work in this space serves as a positive example of how privacy impact can be evaluated during the planning stages of innovation and how this evaluation can be incorporated into product development.[29]

---

[27] For example, Google's Buzz Product Manager Todd Jackson spoke in the press about his team's failure to think in advance about the privacy problems that Buzz would cause. Jonathan Fildes, *Google admits Buzz social network testing flaws*, BBC NEWS, February 16, 2010, http://news.bbc.co.uk/2/hi/8517613.stm.

[28] Many companies, including IBM, Sun Microsystems, Hewlett-Packard and Microsoft have made strong commitments to conducting privacy impact assessments early in the product development processes. *See, e.g.,* 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* (Feb. 2009) at 5, *available at* http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83ECA18D1AD2FC1F; Hewlett-Packard Development *Company, Protecting Privacy at HP: Giving Individuals More Control over their Information* (Aug. 2007), *available at* http://h41111.www4.hp.com/globalcitizenship/uk/en/pdf/Privacy_casestudy_hires.pdf; Michelle Dennedy, *Sun Privacy enhancing Desktop Technologies* (Jan. 2009), *available a*t http://www.privacybydesign.ca/speaker-dennedy.htm.

[29] Microsoft's "Security Development Lifecycle" (SDL) for software development is one example of how privacy can be built into the design process. SDL aims to integrate privacy and security principles into the software development lifecycle, but each stage of Microsoft's 5-stage development lifecycle also includes privacy recommendations and requirements, which range from the procedural to the technical. Privacy impact ratings are given to each project and these ratings determine the design specifications needed for compliance. The SDL guidelines are supplemented by Microsoft's "Privacy Guidelines for Developing Software and Services," a document that lays out guidelines that track some of Cavoukian's Privacy by Design principles. Guidelines for Developing Software and Services (February 2009) at 5, *available at* http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83ECA18D1AD2FC1F&displaylang=en.
See also Microsoft Corporation, *Microsoft Security Development Lifecycle - Process Guidance* (2009), *available at* http://msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746bopq.aspx. These guidelines are made available online in a form that tracks, but is abbreviated from, those used by Microsoft internally.

Second, PIAs are most useful when they are detailed, frank, and focused. They should be drafted so as to assist engineers, management, and counsel to identify and address product weaknesses related to privacy. PIAs are not privacy policies, but instead honest, technical, detailed analyses.

For these reasons, CDT is hesitant to support the Task Force's suggestion that PIAs be made publicly available. We are concerned that public PIAs will be of diminished usefulness. Companies are less likely to be candid about product weaknesses in PIAs that they know will be made public — either because they are afraid of bringing on a lawsuit or enforcement action or because they are concerned that a detailed PIA would reveal proprietary information.

Third, PIAs should be designed to prompt consideration of FIPPs by engineers, management, and product counsel. In particular, PIAs should, at a very granular level, link the amount of data collected to the purpose for which data is being used. PIAs should also outline limitations on data use and transfer as well as protocols for storing, transferring, and deleting collected data.[30]

> *(d) What processes and information would be useful to assess whether PIAs are effective in helping companies to identify, evaluate, and address commercial data privacy issues?*

There is very fruitful research that could be done by academic researchers, think tanks and others on the PIA process to help industry improve its use of this tool, but CDT cautions against the government undertaking this assessment itself. Among other things, an assessment of the impact of PIAs would probably be most effective if conducted under terms of confidentiality, so that no company would face adverse consequences for participating in the assessment. Perhaps the government could fund such research. While PIAs can play a helpful, complimentary role within a robust privacy framework, we believe that limited government resources would be best spent on enforcement and on developing and evaluating industry-specific codes of conduct (presuming legislation is passed to generate the necessary incentives for industry participation).

> *(e) Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?*

As discussed *supra*, § 2(c), CDT believes that PIAs may be most useful when not public by default. Therefore, we do not believe there should be a requirement that PIAs be published in a standardized or machine-readable form.

> *(f) What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?*

There are some examples of companies making meaningful disclosures and explanations about consumer data usage outside of privacy policies. For example, the location-based service Loopt has done a good job of presenting basic information to consumers through the cell phone screen during the sign-up process. There have been some innovations in the applications space, as both Facebook and various mobile operating systems have implemented permissions models that describe to consumers the categories of functionality or data that an application will access before that application is installed. However, these models have their shortcomings as

[30] *See generally supra* note 28.

well. Additional data may be transferred to the applications or to other parties in ways that was not surfaced in the installation process.[31] Also, these permissions models do not disclose the purposes of data collection, or whether that data will then be transferred to other parties. Without meaningful disclosure of purpose specification, transparency as to data collection is of limited utility (*see infra*, § 2(i)-(n)). Other experiments have been undertaken to use symbols to express privacy policies, but these efforts have been unsuccessful to date.[32]

(g) What are the relative advantages and disadvantages of different transparency-enhancing techniques in an online world that typically involves multiple sources being presented through a single user interface?

Third-party data collection, usage, and transfers have always been the most vexing privacy concerns for advocates. Modern technologies that automate third-party monitoring by a wide array of third parties only exacerbate these concerns.[33] Transparency-enhancing techniques drawing multiple sources through a single user interface — such as is being developed in the behavioral advertising space by the Digital Advertising Alliance[34] — have the promise to empower consumers to set privacy preferences across a broader context of services. However, these interfaces can suffer from some notable flaws. They may be inconspicuous to a viewer or difficult to understand. Furthermore, if these disclosures are not comprehensive within their context, these interfaces might give consumers the false impression that they have addressed all relevant information practices. If an aggregating interface only identifies four of the eight third parties tracking a consumer or providing behavioral data for an advertisement, consumers may be deceived about the extent that are being tracked. To be effective, these interfaces must be easily accessible and comprehensive to their context.

Because of the sheer number of parties involved in much online and offline tracking (many of which do not have traditional consumer-facing sides), transparency about tracking must be supplemented by giving consumers the ability to make persistent and global choices about the use of their data. In the behavioral advertising context, this means that consumers should not be expected to locate and opt out of every conceivable ad network or tracking entity even if the identity of the parties that influence ad-serving decision is eventually disclosed to consumers though an aggregating interface. For this reason, CDT strongly supports the development of "Do Not Track" technologies to allow consumers to prevent all entities from conducting a particular type of tracking, as opting out on a piecemeal basis is becoming increasingly difficult in the modern ecosystem.

(h) Do these (dis)advantages change when one considers the increasing use of devices with more limited user interface options?

---

[31] *See Your Apps are Watching You*, *supra* note 3.

[32] Nearly ten years ago, TRUSTe called for industry groups, the government and other privacy advocates to establish a set of standard symbols that would define online privacy policies for consumers. Jennifer DiSabatino, "Truste proposes standard privacy symbols for Web sites," Computerworld (June 19, 2001) http://www.computerworld.com/s/article/61475/Truste_proposes_standard_privacy_symbols_for_Web_sites. Just last year, the Future of Privacy Forum created a symbol intended to lead consumers to more information about online advertising. Stephanie Clifford, A Little "i" to Teach About Online Privacy," New York Times (January 26, 2010), http://www.nytimes.com/2010/01/27/business/media/27adco.html, but so far the icon has not been widely deployed. See generally, J. Tsai et al, "Symbols of Privacy" (2006), http://cups.cs.cmu.edu/soups/2006/posters/tsai-poster_abstract.pdf.

[33] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, THE WALL STREET JOURNAL, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html; *supra* note 3.

[34] *See* The Self-Regulatory Program for Behavioral Advertising Website, *supra* note 26.

Transparency challenges are heightened in the mobile context. Small screens reduce opportunity for meaningful notice, and mobile operating systems regularly transmit unique identifiers far more persistent than traditional HTML cookies.[35] Providing detailed disclosures about the scope of information sharing and the number and identity of third parties receiving data will be extremely difficult. In the mobile space, consumers may be served less by just-in-time disclosure and more by the ability to make broad choices about the use of their data. "Do Not Track"-type technologies need to be explored, not just as the mobile browser level, but also at the mobile operating system level to allow consumers to make global and persistent choices about data transfers through all applications.

(i) Are purpose specifications a necessary or important method for protecting commercial privacy?

The Purpose Specification principle is an essential element of the FIPPs. The limitations outlined in other principles — such as Data Minimization[36] and Use Limitation[37] — only have meaning in the context of a statement about the purpose for which data was first collected. Absent enforceable purpose specifications (and use limitations), data collected for legitimate and transparent purposes – such as fraud prevention or order delivery – may be used in ways that would undermine consumer trust.

However, purpose specifications only promote privacy insofar as they are bounded within certain parameters. As the Green Paper states: "An entity that clearly states that it intends to do anything and everything with the data it collects . . . may not be providing adequate protection for consumer privacy." CDT emphatically agrees. Purpose specifications, whether presented in a privacy policy or in some form of enhanced notice, should take the form of narrowly scoped, clear, affirmative, and binding statements describing the purpose of data collection. Moreover, purpose specifications must be enforceable. Any new privacy protection framework should make clear that the adoption of a data collection or use practice not specifically described in a purpose specification will be considered a deceptive practice by the FTC.

(j) Currently, how common are purpose specification clauses in commercial privacy policies?

The typical privacy policy today includes elements of purpose specification with respect to "commonly accepted practices" such as order fulfillment, fraud prevention practices, or customer service. However, these policies often fail to "state specific reasons or objectives for collecting personal information" with respect to more controversial uses of data, such as consumer tracking and profiling.

---

[35] *See* Jennifer Valentino-DeVries, *Unique Phone ID Numbers Explained*, Digits Blog, December 19, 2010, http://blogs.wsj.com/digits/2010/12/19/unique-phone-id-numbers-explained/.

[36] "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)." *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, *supra* note 11 at 26-27. *See also* 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* (Dec. 2008) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[37] *Id.*

The privacy policy for the website Buy.com serves as a useful example. Certain elements of the privacy policy accord with the purpose specification principle. For example, the policy reads: "we use a third party to help us provide customer service. In order to help you most effectively, we provide them with your order information." However, the privacy policy also includes the following sentence in its policy overview: "Except as limited below, we reserve the right to use or disclose your personally identifiable information for business reasons in whatever manner desired."[38]

Such broadly scoped statements subvert the principle of purpose specification, and a new privacy protection framework should prevent such companies from insulating themselves from legal liability by issuing such vague and sweeping statements.[39]

(k) Do industry best practices concerning purpose specification and use limitations exist? If not, how could their development be encouraged?

CDT is not aware of any currently implemented best practice principles concerning purpose specification. To the contrary, our review of industry privacy policies leads us to the conclusion that the Buy.com privacy policy referenced *supra* § 2(j), represents the norm, not the exception. Without a requirement that companies explain what they are doing with consumer data, companies will (understandably, from a risk management perspective) continue to devise privacy policies that serve only to avoid making definitive accountable statements about data usage in order to evade Section 5 liability.

(l) What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

CDT believes that a substantive legal requirement to state clear, specific purposes for using personal information is the most logical approach to this dilemma. Clearly, under the existing privacy framework, such incentives do not exist. While government pressure may help at the margins, it is difficult to see how the bully pulpit without other incentives will lead *all* industry players to adopt a robust and voluntary code of true purpose specification.

Alternatively, CDT believes that the FTC could interpret its Section 5 unfairness authority to require that companies declare the specific purpose for which personal information is collected.[40] However, as they to date have failed to do so, we believe the FTC is unlikely to do so in the near future. Moreover, we believe a legislative solution that allows for precise industry-specific implementation of the Fair Information Practices under a coregulatory, FTC-approved safe harbor structure or through administrative rulemaking is a preferable approach.

(m) How should purpose specifications be implemented and enforced?

Implementation

The multi-stakeholder generated codes of conduct outlined in the Green Paper should include clear requirements and standards for statements of purpose specification. Because these codes

[38] *See* Buy.com Privacy Policy, July 30, 2009, *available at* http://www.buy.com/corp/privacy_policy_complete.asp (last visited Jan. 27, 2011).

[39] CDT believes that they may constitute a deceptive practice under the current privacy framework as well.

[40] *See* Comments of the Center for Democracy & Technology, *supra* note 13.

of conduct would be industry-specific, each code could include industry-appropriate purpose specification requirements. For example, a code of conduct for ISPs should require that ISPs be very specific about their uses of data gleaned through Deep Packet Inspection, while codes of conduct for entities that collect users' email addresses should require clarity about how the email address will be used and whether it will be transferred.

Enforcement

As discussed *supra*, § 1, CDT believes that in any new privacy framework, a failure to clearly state specific purposes for using personal information should be illegal and subject to enforcement by the FTC and state Attorneys General, as well as any coregulatory safe harbor program. The inclusion of language that is excessively broad or generalized should similarly be forbidden and subject to enforcement.

> *(n) How can purpose specifications and use limitations be changed to meet changing circumstances?*

The Green Paper articulates a concern that purpose specification requirements that are too prescriptive could prevent innovation. However, companies can always change their privacy policies going forward, creating new rules for data that will be collected *after* the date that the new privacy policy is posted. Such changes should not require new and affirmative "opt-in" consent from consumers. However, companies should post new privacy policies in advance of those policies going into effect, to allow consumers and advocates the opportunity to review and assess changes to those policies, and to let users make informed decisions about whether to continue using those companies' services.[41]

With respect to which practices are permitted within the parameters of a pre-existing privacy policy, it is important to not forget the purpose behind requiring purpose specifications. Purpose specifications are designed to limit data retention and to limit use. Too much flexibility can leave the purpose specification FIPP without any meaning.

Consider the following example: In Spring 2010, the online music service Pandora started partnering with Facebook's new "Instant Personalization" program. Pandora used customers' email addresses to connect their Pandora profiles to their Facebook profiles (and share their music preferences with their Facebook friends), without first obtaining permission. This data use practice was criticized by many privacy advocates and consumers: it was not a use that consumers had expected when they signed up for the music service and it had not been described in the privacy policy that was in place when they signed up for the service.[42] The data use practice seemed to contradict the purpose specifications in the privacy policy, but it appears that Pandora read its purpose specifications as being extraordinary broadly scoped. Further, people were embarrassed that their music preferences were shared with their Facebook

[41] For example, Congressman Bobby Rush's Best Practices Act requires covered entities to post new privacy policies (that include material changes re collection, use, and disclosure of covered and sensitive information) 30 days in advance before collecting information pursuant to those policies. §105(b) BEST PRACTICES Act, H.R. 5777, 111th Cong. (2009). CDT supports this approach.

[42] Troy Wolverton, *New Facebook Changes Threaten Privacy*, MERCURYNEWS.com, May 4, 2010, http://www.mercurynews.com/news/ci_14985800. Nick O'Neill, *Facebook Must Make "Instant Personalization" Opt-In Immediately*, All Facebook, May 8, 2010, http://www.allfacebook.com/2010/05/facebook-must-make-instant-personalization-opt-in-immediately.

friends.[43] A few months after the partnership with Facebook began, Pandora responded to this criticism with a great tool to put its users in charge of their privacy. Beginning in August, when Pandora users returned to the site, they were shown a box that asks them whether they want their profile to be "public" or "private." Users had to pick one or the other. The box also contained links to give users the chance to learn more about how sharing works.[44]

This case study offers two lessons. First it serves as a reminder that, absent meaningful user consent, companies should not be allowed to materially change how they use the data they collected under a different privacy policy; this amounts to changing the rules in the middle of the game, is unfair to consumers, can undermine trust in the system, and can cause embarrassment, or worse. Second, obtaining meaningful consent, in response to a clear and understandable notification, is not difficult. Pandora's example should serve as a model for companies who seek to repurpose previously collected data for unexpected uses.

> *(o) Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations? What steps should be taken if inconsistencies are found?*

At a fundamental level, each individual organization is responsible for complying with the Fair Information Practice Principles. For this reason, CDT has long advocated that companies adopt Privacy by Design principles, create PIAs, and employ chief privacy officers as elements of an internal accountability structure that will inculcate a culture of privacy throughout the entire company.[45]

If a company is a participant in a coregulatory safe harbor program that exempts it from elements of a baseline privacy law (such as a private right of action, *see supra*, § 1(d)), that company should be required to affirmatively demonstrate its adherence to the safe harbor program's requirements on a regular basis as part of a robust auditing process. However, we do not believe that companies should have an affirmative obligation to notify or certify to the Federal Trade Commission or other government regulators that they are in compliance with safe harbor requirements or underlying law. Instead, the FTC and state Attorneys General should have the authority to investigate suspected illegal practices, at which point the question of compliance or not can be determined in the context of specific facts.[46]

> *(p) Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?*

As a general rule, consumers do not have the ability to track the use of their personal information, which is why a new privacy protection framework must require companies to make clear, precise and accountable statements to consumers about how they use data. Once a consumer gives information to a third party, there are few intrinsic limitations on what that party

---

[43] Caitlin McDevitt, *Facebook Opens Pandora's Box, Reveals My Embarrassing Playlist*, FacebookStatus Blog, April 23, 2010, http://www.thebigmoney.com/blogs/facebook-status/2010/04/23/facebook-opens-pandora-s-box-reveals-my-embarrassing-playlist.

[44] CDT worked closely with Pandora to come up with this solution. *See* Justin Brookman, *Closing Pandora's Box*, CDT Blog, August 4, 2010, http://www.cdt.org/blogs/justin-brookman/closing-pandora%E2%80%99s-box.

[45] For more on Privacy by Design, *see* Comments of the Center for Democracy & Technology, FTC Consumer Roundtable, December 21, 2009 *available at* http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf.

[46] CDT has long argued that both the federal government and the states should be more vigilant. *See* Comments of the Center for Democracy & Technology, *supra* note 11

can do with the data, or ways to track its usage. While CDT has advocated for consumers to have the ability to bind data permissions to information (effectively consumer-side privacy policies or terms of use) in both the standards community,[47] and more recently with regard to "Do Not Track" browser headers,[48] adoption and acknowledgement have lagged. Currently for consumers, there are few options to track what happens to their data.

Ironically, one of the reasons that online behavioral advertising has driven much of the current privacy debate is that technologists and activists actually have the ability to forensically determine in some cases how consumer data is being transferred, by studying the code on various webpages that redirect to other third-party content and code.[49] However, in most other contexts, such as with cloud computing, social networking, and notably the offline environment, consumer data goes into a black box, and consumers and advocates have no means to evaluate how companies use, trade, or sell individualized data. Absent meaningful purpose specification, consumers cannot make informed decisions about the privacy implications of the data-driven services they use.

(q) Are technologies available to help companies monitor their data use, to support internal accountability measures?

Unlike with consumers, companies do currently have the ability (if not always the will) to assess and control how they are using consumer data. If there is a market for robust and systemic internal monitoring to track usage of consumer data, those technologies and internal processed will be built and developed.

At the moment, however, the current privacy framework does not provide adequate incentives to companies to monitor their use and transfers of consumer data. Last year, a Wall Street Journal story detailed how several mainstream websites included a surprising number of third-party invisible "web bugs" on their sites that allowed a wide range of targeting companies to place unique tracking cookies on users' computers. Congressmen Ed Markey and Joe Barton issued letters to many of these companies asking, *inter alia*, whether the companies knew to which third parties they were transferring consumer information. Many answered "no."[50] However, unless the companies had promised otherwise, they had no clear obligation to prevent those transfers or even disclose them to consumers under existing law. A requirement that companies tell consumers about how their data is being shared, however, would strongly incentivize companies to implement procedures to track how they share consumer data.

(r) How should performance against stated policies and practices be assessed?

---

[47] *See, e.g.,* Alissa Cooper, John B. Morris, and Erica Newland, *Privacy Rulesets: A User-Empowering Approach to Privacy on the Web*, W3C Workshop on Privacy for Advanced Web APIs, July 2010, *available at* ww.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html; John Morris, Alissa Cooper, and Erica Newland, *Binding Privacy Rules to Data: Empowering Users on the Web*, W3C Workshop on Privacy for Advanced Web APIs, July 2010, *available at* http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-13.pdf.

[48] Erica Newland, *"Do Not Track" Solves Only Part of the Problem*, CDT Blog, http://www.cdt.org/blogs/erica-newland/%E2%80%9Cdo-not-track%E2%80%9D-solves-only-part-problem (last visited Jan. 27, 2011).

[49] *See supra* note 13; Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, *Flash Cookies and Privacy* (August, 2009) *available at* http://ssrn.com/abstract=1446862.

[50] *See, e.g.,* Press Release, Congressman Ed Markey, Markey, Barton Release Responses form Web Sites on their Tracking of Consumer Behavior, October 8, 2010 *available at* http://markey.house.gov/index.php?option=content&task=view&id=4103&Itemid=125.

In order to be accredited by the FTC for safe harbor status, a self-regulatory program must require that industry participants demonstrate compliance with a code of conduct as part of a regular auditing process. If the FTC has reason to believe that a particular safe harbor program does not have in place rigorous auditing and enforcement mechanisms, it should investigate the safe harbor program and, where appropriate, revoke the program's safe harbor status.

> *(s) What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?*

The U.S. needs a legal framework that establishes a requirement that privacy be protected; the internal mechanisms will develop in response to generate compliance. Though regulators can encourage privacy by design, government should not necessarily specify the process or particular technology to safeguard consumers' privacy interests. Law should provide the mandate, companies should establish the means.

(3) Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support;(b) stepped up FTC enforcement and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

The Internet Policy Task Force has not asked any questions about this recommendation.

(4) Using existing resources, the Commerce Department should establish a Privacy Policy Office (PPO) to serve as a center of commercial data privacy expertise. The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concern with the Executive Office of the President as the Administration's lead on international outreach on commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO have any enforcement authority.

> *(a) Should be the FTC be given rulemaking authority triggered by the failure of a multi-stakeholder process to produce a voluntary enforceable code within a specified period of time?*

While we support the coregulatory model, we believe that the best approach for consumers and businesses would be for Congress to grant the FTC rulemaking authority to implement the Fair Information Practice Principles without the need for a triggering event, for two reasons. First, as new business models and threats to privacy emerge, there may be urgent issues that require quick response. Second, even where multi-stakeholder processes are convened and are successful, there may be cross-cutting issues where uniformity is needed but is not afforded by otherwise successful industry codes.

In addition, there are existing self-regulatory systems for only some of the privacy issues facing consumers today. Many of those established efforts focus on online behavioral advertising,

which is just one relatively narrow piece of the privacy puzzle. As the Green Paper notes, there are no parallel self-regulatory initiatives to address the wide range of other privacy concerns, such as cloud computing, social networking, data brokers, or any offline data collection, usage, and transfers.[51] It is not clear that it would be desirable to put all those issues on hold to await the formation and success or failure of coregulatory efforts. The FTC should have the discretion to act where it appears that no coregulatory process is likely to convene or likely to produce results in a reasonable timeframe.

(b) How can the Commerce Department best encourage the discussion and development of technologies such as "Do Not Track"?

In 2007, CDT along with a number of other consumer advocates first suggested the idea of "Do Not Track" as a means to offer users persistent and global options for avoiding third-party tracking.[52] The idea lay dormant for three years until last summer, when Chairman Leibowitz of the FTC expressed support for the concept at a Senate Commerce Committee hearing on privacy.[53] The FTC's support for "Do Not Track" has produced remarkable results in a few short months, as both Microsoft[54] and Mozilla[55] have announced their intent to develop browser features that would allow consumers to prevent third-party tracking. In at least this area, the bully pulpit has shown impressive results. To keep the momentum going, CDT urges the Department of Commerce in its final White Paper and through other means (including through the PPO) to similarly encourage browser vendors to develop "Do Not Track" mechanisms. The Department of Commerce should also encourage other industries, such as the makers of mobile operating systems, to explore similar "Do Not Track" tools to allow users to set persistent and global choices to opt out of third-party tracking.

CDT believes that "Do Not Track" technology could be included as one piece of baseline privacy legislation, though we would be hesitant about statutory language that mandates specific technical solutions.[56] However, a "Do Not Track" law cannot substitute for a baseline privacy protection framework. "Do Not Track" does not address a wide range of other privacy concerns, such as cloud computing, social networking, and offline data sharing. With or without "Do Not Track," we need a comprehensive approach to baseline privacy legislation.

(c) Under what circumstances should the PPO recommend to the Administration that new policies are needed to address failure by multi-stakeholder process to produce an approved code of conduct?

As stated earlier, *supra* § 1, CDT believes that legislation should be adopted to establish baseline privacy rules and to create the framework for the multi-stakeholder processes and that the Federal Trade Commission should be granted the discretion to issue regulations implementing such a baseline privacy protection law without any triggering events. The need for

---

[51] *See supra* note 11.

[52] Center for Democracy & Technology, *Consumer Rights and Projections in the Behavioral Advertising Sector*, October 31, 2007 *available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

[53] Juliana Gruenwald, *FTC Weights 'Do Not Track' List*, NationalJournal, July 27, 2010, http://techdailydose.nationaljournal.com/2010/07/ftc-weighs-do-not-track-list.php.

[54] Jordan Robertson, *Microsoft unveils 'do not track' IE feature*, MSNBC.Com, December 7, 2010, http://www.msnbc.msn.com/id/40554324/ns/technology_and_science-security/.

[55] Julia Angwin, *Web Tool On Firefox To Deter Tracking*, THE WALL STREET JOURNAL, January 24, 2011, http://online.wsj.com/article/SB10001424052748704213404576100441609997236.html.

[56] *See "Do Not Track" Solves Only Part of the Problem*, *supra* note 48.

such legislation is already established by the failure of self-regulatory efforts to date, and, while we support the creation of a PPO, we are quite certain that a PPO without enforcement powers would be no more effective in encouraging better self-regulation than an FTC without enforcement powers has been in all its efforts to encourage effective self-regulation over the past decade. Without a statute establishing baseline rules, companies will not be sufficiently motivated to engage in the multi-stakeholder process.

(d) How can cooperation be fostered between the National Association of Attorneys General, or similar entities, and the PPO?

State consumer protection authorities should certainly be included in any multi-stakeholder process, as states have often been on the leading edge of privacy enforcement. For example, states have taken the lead on investigating and bringing actions against companies that deceptively transfer financial account information to third-party subscription services (commonly referred to as "post-transaction marketing").[57] CDT recently held a convening of stakeholders to create a set of best practices for companies wishing to engage in legitimate subscription marketing, and we received extremely useful input from some of the state offices investigating the issue.[58] The Task Force should similarly seek to bring state enforcers to the table in developing industry-specific implementations of a privacy protection framework.

(5) The FTC should remain the lead consumer privacy enforcement agency for the U.S. Government.

(a) Do FIPPs require further regulatory elaboration to enforce, or are they sufficient on their own?

FIPPs will require elaboration through industry standards, regulation, and enforcement action. As described in more detail, *supra*, § 1, the Federal Trade Commission should be given the authority to issue regulations to adapt a privacy protection framework to account for new innovations in technology and data usage. Industry self-regulatory and coregulatory efforts should also iterate to respond to the privacy issues associated with changing business models and practices, and the FTC, as it monitors such industry programs, should be prepared to withdraw its approval of any one that does not keep pace with evolving privacy risks.

(b) What should be the scope of FTC rulemaking authority?

As described in more detail, *supra* § 1, the Federal Trade Commission should have the discretion to issue the regulations it deems necessary to implement a baseline privacy protection framework.

(c) Should FIPPs be considered an independent basis for FTC enforcement, or should FTC privacy investigation still be conducted under Federal Trade Commission Act Section 5 "unfair and deceptive" jurisdiction, buttressed by the explicit articulation of the FIPPs?

---

[57] *See* Tanzia Vega, *Online Marketer Settles With New York for $5.2 Million*, THE NEW YORK TIMES, September 21, 2010, http://www.nytimes.com/2010/09/22/business/22cuomo.html; Press Release, Office of the New York Attorney General, Cuomo Obtains $10 Million in Settlements with Companies That Tricked Consumers Into Signing Up for Discount Clubs with Hidden Fees, *available at* http://www.ag.ny.gov/media_center/2010/aug/aug18a_10.html.

[58] Center for Democracy & Technology, *Online Subscription Upselling Working Group Best Practices Working Draft*, December 13, 2010 *available at* http://www.cdt.org/files/pdfs/20102113_upselling_best_practices.pdf.

While CDT believes that the FTC already has authority under Section 5 to articulate the full FIPPs and treat any FIPPs violation as an unfair and deceptive trade practice, it has not done so yet and it is unlikely to take that approach any time soon. Assuming that legislation is adopted establishing the full FIPPs as a baseline of privacy protection, consideration would have to be given to structuring FTC enforcement of those principles, taking into account the strengths and limits of the FTC's current authorities.

One approach would be to codify the FIPPs into law, and then deem violations of those principles as an unfair and deceptive act or practice in violation of a trade regulation under Section 18(a)(1)(B) of the FTC Act. This was the approach taken by the BEST PRACTICES bill introduced in the House last year, and would subject violations of FIPPs principles to the FTC's limited statutory penalty authority.[59] Whether through this mechanism or another, the key point is to ensure that privacy legislation enables the FTC and state regulators to obtain penalties for violations of the FIPPs.

(d) Should non-governmental entities supplement enforcement of voluntary codes?

As discussed in more detail, *supra*, § 1, in order to obtain safe harbor status as part of a baseline legislative framework, any coregulatory program must be required to issue and require compliance with FIPPs-based protections as strong or stronger than the letter of the law and couple this with robust auditing, compliance and enforcement. However, the FTC and state Attorneys General should always possess the ability to bring enforcement actions against companies out of compliance with the standards of a safe harbor program.

Consumer advocacy groups and other non-governmental entities should have a role in both forms of enforcement. (Non-governmental entities are already able to file complaints at the FTC, and that should remain an important source of input to the Commission's enforcement process.) The voluntary codes are to be adopted through a multi-stakeholder process that should, in order to be credible, include consumer advocates, and the more effective self-regulatory bodies may include consumer advocates in their enforcement mechanisms. Indeed, the FTC, in assessing the adequacy of a coregulatory standard for safe harbor status may consider whether the code's enforcement process includes representation by consumer advocates. A major issue, unfortunately, will be the limited resources of consumer advocacy groups.

(e) At what point in the development of a voluntary, enforceable code of conduct should the FTC review it for approval? Potential options include providing an ex ante *"seal of approval," delaying approval until the code is in use for a specific amount of time, and delaying approval until the enforcement action is taken against the code.*

Provided that the FTC has the ultimate authority to accept or reject codes of conduct, CDT could support a range of approaches as to how that authority is exercised. The interest of providing certainty to companies may weigh in favor of *ex ante* approval. We believe that it would be helpful for the FTC to be able to track the progress of multi-stakeholder convenings as they develop codes; we also assume that the FTC would have the inherent authority to indicate where a code fell short, in order to allow improvements before final approval. Overall, CDT recommends that under a framework that requires FTC approval of safe harbor programs, the FTC should be given maximum flexibility to determine and revise over time its process for

[59] *See* H.R. 5777, *supra* note 17.

assessing and approving codes of conduct, as well as for revoking such approval where appropriate.

> *(f) What steps or conditions are necessary to make a company's commitment to follow a code enforceable?*

Absent a law, a company should make a clear, public statement that they are in compliance with a particular code of conduct in order to clearly demonstrate public accountability under Section 5 of the FTC Act. Indeed, merely being a participant in a program that explicitly requires certain behavior and then failing to adhere to that could be considered a deceptive or unfair business practice under Section 5 of the FTC Act or state law. However, this fact demonstrates a weakness in a purely "voluntary and enforceable" approach: the dearth of strong and privacy protective voluntary codes of conduct can perhaps be explained by the fact that stated or implied adherence to such a code would subject a company to Section 5 (or other, such as unjust enrichment or state law) liability for failing to fulfill those obligations. For this and other reasons, a baseline privacy law is needed to encourage industry to adopt strong and accountable codes.

(6) The U.S. government should continue to work toward increased cooperation among privacy enforcement authorities around the world and develop a framework for mutual recognition of other countries' data privacy frameworks. The United States should also continue to support the APEC Data Privacy Pathfinder project as a model for the kinds of principles that could be adopted by groups of countries with common values but sometimes diverging privacy legal frameworks.

The Internet Policy Task Force has not asked any questions about this recommendation.

(7) Consideration should be given to a comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols, and allows States to build upon the framework in limited ways. Such a framework should track the effective protections that have emerged from State security breach notification laws and policies.

> *What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?*

All but a few states have enacted data breach notification laws, so as a practical matter companies today do notify affected individuals in the event of a data breach.[60] From a consumer perspective, even a good federal breach notification requirement does not by itself offer much tangible progress over the status quo, since notification is already effectively the law of the land. And if a federal framework – likely in the form of a data breach notification law — were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security.

However, as the Department pointed out in its Green Paper, the current patchwork of

[60] There are federal breach notification rules that apply to entities that are covered by HIPPA and vendors of personal health records. See American Recovery and Reinvestment Act (ARRA), Pub.L. 111-5, Sec. 13402; American Recovery and Reinvestment Act (ARRA), Pub.L. 111-5, Sec. 13407.

notification standards can prove a challenge from an industry compliance perspective. In the interest of removing unnecessary compliance barriers, CDT supports the concept of a nationwide data breach notification standard, so long as that standard is at least as effective as the laws already in place at the state level. The price for strong preemption must be strong substantive protections. CDT believes that for a federal law to be as effective as the strongest state laws, the following elements would be necessary:

Appropriately-scoped preemption: CDT has reservations about preempting state data security laws covering topics other than notification. The information security provisions of the Gramm-Leach-Bliley Act (GLB) preempted inconsistent state laws, but otherwise allowed for state-level experimentation on the difficult question of how to ensure sufficient attention and precautions with respect to data security. Any federal data breach notification regime should preserve a state's ability to come up with an idea that is truly a fresh approach. California's breach notification law, the first in the nation, was a classic example of this. Had GLB broadly preempted state data security laws, it would not have been possible.

A "notify unless" notification trigger: A notification trigger should permit notification to be avoided only when there is an affirmative determination that there exists no serious risk that personal information could be misused. In other works, the standard should be that, in the event of a breach, a company must notify *unless* such an affirmative determination can be made. A finding that appropriate technical safeguards prevent unauthorized access to the data should qualify as an affirmative determination that there is no significant risk is misuse.

A "notify unless" trigger creates strong incentives for a company suffering a breach to get to the bottom of what happened –because if it can determine there is no real risk, it will not have to notify its customers.[61] A trigger that requires notification only in the event of an affirmative finding of risk would create the opposite incentive — a company might not want to investigate too closely, because finding evidence of risk would trigger the obligation to notify.

A "safe harbor" for companies that appropriately safeguard the data they hold will both incentivize companies to adopt better data security practices and help prevent needless consumer notification. It is important to note, however, that safeguards should not excuse notification when the circumstances of the breach suggest that those safeguards are unlikely to be effective. For example, a breach involving encrypted data should generally be exempt from notification, but not when it appears that the encryption keys may have been breached as well.

Outside scrutiny: Adopting a "notify unless" notification trigger is crucial. However, in the absence of any outside scrutiny of risk determinations, a company could have an incentive to err consistently on the side of finding little or no risk. Even if the affected individuals were eventually to become victims of identity theft, it would be difficult ever to trace those crimes back to the specific breach, since nobody other than the company and the identity thieves would be aware that the breach even occurred. In short, with nobody in a position to question dubious risk assessments, there could be a temptation to under-notify.

CDT believes this problem could be greatly mitigated by requiring a company, when it determines a breach poses insufficient risk to warrant notification, to notify the FTC or other appropriate regulator and provide some explanation as to why the company believes there is no

[61] HR 2221, introduced in 2009, had such a "notify unless" formulation.

significant risk. No formal process for FTC review or approval of a company's determination would necessarily be required. Simply knowing that a brief explanation would need to be filed with the FTC, and that the FTC might respond if it spotted a pattern of behavior or otherwise became suspicious, may be all it would take to ensure that companies remain diligent in their risk determinations and weigh the inevitable judgment calls in an even-handed manner. CDT therefore recommends that any data breach law require that breaches judged to be non-risky still necessitate a submission of a brief written explanation to a regulatory body such as the FTC.

No harm standard: Debates about security breach notification requirements often center around whether or not notification should be required in the absence of a determined "harm" to the consumer, such as identity theft.

CDT cautions against a federal framework that would limit notification to cases where particular harms or risks of particular harms can be identified. In 2005, attorneys general from 45 states, the District of Columbia, and Puerto Rico signed a letter to the U.S. Congress, which at the time was considering a harm standard. As the letter stated:

> Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud.[62]

The "notify unless" formulation that CDT suggests excuses notification when there is no real risk of misuse, but does not require any showing that harm has occurred or is likely to occur. Nor does it require any analysis of what specific harms could occur; it would not say, for example, that notification depends on whether there is a risk of a particular harm such as identity theft or of a type of harm such as financial cost.

Avoiding specificity with respect to possible harms is consistent with the 2005 Interagency Guidance on breach notification put out by financial regulators (OICC, the Fed, FDIC, OTS), which called for notification if a financial institution determines that "misuse of information about a customer has occurred or is reasonably possible."[63] It also is consistent with OMB's 2007 memorandum on data breach notification by federal agencies. OMB directed agencies to assess the likely risk of harm, but stated that "[a]gencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice." It went on to cross-reference language from the Privacy Act requiring agencies to protect against data security threats "which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[64] Thus conceived, notification does not turn on whether the possible impact to an individual can be expressed in financial terms or criminal terms.

The federal breach notification requirement recently enacted by Congress that applies to personal health records is not triggered by the potential for harm. Notification is required if

---

[62] Letter from the National Association of Attorneys General to Honorable Bill Frist et. al (Nov. 7, 2005) *available at* http://www.cdt.org/security/State_AGs_2005_Letter_to_Congress_on_Breach_Notification.pdf.

[63] 70 Fed. Reg. 15743 and 15752 (Mar. 29, 2005).

[64] Office of Management and Budget, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Memorandum for the Heads of Executive Departments and Agencies (May 22, 2007) at 13 & n.39 *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

personal information is actually acquired by an unauthorized person or entity.[65] The FTC, which is charged with enforcing the notification requirement, explicitly rejected calls to adopt a harm standard.[66] Similarly, a harm standard for breach notification by HIPAA covered entities was adopted by the Department of Health & Human Services (HHS) in an interim final rule,[67] but this action was criticized by members of the House Energy & Commerce Committee and is currently under reconsideration by HHS.[68]

Some companies may claim that a more narrowly focused harm standard ensures that consumers are not overwhelmed by unnecessary notices. However this argument incorrectly presupposes that the only purpose of breach notification is informing individuals of the steps they can take to protect themselves from specific threats such as identity theft. While this is in fact one purpose behind breach notification standards, it ignores the larger goal of the policy: reducing the number of data breaches by incentivizing companies to improve their data security practices. Indeed, a 2007 study of the impact of state-implemented breach laws conducted by the Samuelson Law, Technology, & Public Policy Clinic at the University of California, Berkeley found that "regardless of the risk of identity theft and alleged individual apathy towards notices, the simple fact of having to publicly notify causes organizations to implement stronger security standards that protect personal information."[69]

Exceptions for data held in a personal capacity: CDT would suggest including in any data breach law or rule a *de minimis* exception for persons that own or possess data in connection with purely personal, family, or noncommercial activities. Arguably, if an individual uses his or her computer for online shopping and also keeps personal data on it concerning, say, his or her elderly parents, the person could qualify as a person engaged in interstate commerce who possesses personal data, and thus might be covered under certain data breach notification standards. Given the small quantity of data such a person has, however, it would make little sense to require a formal written security plan.

(8) A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather act in concert with these protections.

Are there lessons from sector-specific commercial data privacy laws — their development, their contents, or their enforcement — that could iforms U.S. commercial data privacy policy?

CDT strongly supports the Department's recommendation that a baseline commercial privacy law not preempt the strong sectoral laws and policies already in place. As we detailed in our response to the Department's privacy Notice of Inquiry, while consumer data will not receive the

[65] 74 Fed. Reg. 42966 (August 25, 2009).

[66] *Id.*

[67] 74 Fed. Reg. 42744-45 (August 24, 2009).

[68] Howard Anderson, *Final Breach Notification Rule on Hold*, Healthcare Info Security, July 30, 2010, http://www.healthcareinfosecurity.com/articles.php?art_id=2801&rf=2010-08-10-eh.

[69] Samuelson Law, Technology, & Public Policy Clinic, *Security Breach Notification Laws: Views from Chief Security Officers*, University of California-Berkeley School of Law (2007). The study found: "Breach notification laws have significantly contributed to heightened awareness of the importance of information security throughout all levels of a business organization and to development of a level of cooperation among different departments within an organization that resulted from the need to monitor data access for the purposes of detecting, investigating, and reporting breaches. [Chief Security Officers] reported that breach notification duties empowered them to implement new access controls, auditing measures, and encryption. Aside from the organization's own efforts at complying with notification laws, reports of breaches at other organizations help information officers maintain that sense of awareness."

protection it needs absent a general privacy law, existing sectoral laws have an important role to play in any new US privacy framework.[70] Sectoral 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.

More than a decade's experience with privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA) offers some useful lessons for developing U.S. commercial data privacy policy. First, relying on notice and consent alone is ineffective for protecting privacy. In 2001, HIPAA required health care providers to obtain patient consent to disclose health information for treatment, payment and many routine business functions. In 2002, HIPAA was revised to exempt these uses of information because the consent requirement proved an overwhelming burden on businesses and patients alike — for very little privacy gain. Modern health privacy efforts are focused on developing a comprehensive framework of privacy and security protections. Consent is an important element of this framework, but the framework gives appropriate weight to each of the full set of Fair Information Practice Principles.[71] For this reason, CDT supports a baseline privacy protection framework that exempts certain commonly-accepted data sharing and usage practices (such as using a third-party shipping company for order fulfillment) from consent requirements.[72]

Experience with HIPAA has also demonstrated the need for consistent enforcement and ongoing regulatory guidance. The Dept. of Health and Human Services (HHS), charged with enforcing HIPAA privacy complaints, has been historically reluctant to issue meaningful penalties for gross and chronic noncompliance with the law, leading to less patient trust in the health care system and continued violations of privacy rules.[73] HHS has issued some guidance for health care entities on how to comply with HIPAA privacy and security requirements, but there remains widespread confusion regarding how HIPAA applies to services and tools that are evolving due to technology — such as personal health records, which are only partially covered under HIPAA.[74] Privacy and security frameworks must be periodically reevaluated to match consumer expectations and business practices as technology and other forces change the marketplace.

(9) Any new Federal privacy framework should seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns that arise from emerging technologies, should those developments create the need for additional protection under Federal law.

> (*a) Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matters, leaving*

[70] Comments of the Center for Democracy & Technology, NTIA Notice of Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy, November 19, 2010 *available at* http://www.cdt.org/files/pdfs/CDT%20Comments%20to%20NTIA%20Copyright%20Task%20Force.pdf.

[71] *See* Deven McGraw, *Rethinking the Role of Consent in Protecting Health Information Privacy*, January 26, 2009 *available at* http://cdt.org/paper/rethinking-role-consent-protecting-health-information-privacy.

[72] *See* H.R. 5777, *supra* note 17.

[73] Deven McGraw and Harley Geiger, *HHS Holds Keys to Next Generation of Health Information Privacy*, iHealthBeat, September 24, 2009, http://www.ihealthbeat.org/Perspectives/2009/HHS-Holds-Keys-to-Next-Generation-of-Health-Privacy.aspx.

[74] Center for Democracy & Technology, *Building a Strong Privacy and Security Policy Framework for Personal Health Records*, 7 (2010) *available at* http://cdt.org/paper/building-strong-privacy-and-security-policy-framework-personal-health-records.

States free to regulate new concerns that arise from emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

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. The Department should look to the states as one source of new ideas and approaches to privacy protection. Hence, 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.

The positive impact of narrowly-tailored preemption is well-documented. For example, data breach notification laws are one of many important new ideas that have emerged from the states, and they would not have emerged had the information security provisions of a (sectoral) federal privacy law, the Gramm-Leach-Bliley Act (GLB), had broad preemption.[75] The information security provisions of 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.[76] Similar laws have so far been adopted by 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands.[77] 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 the Department 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.

(b) How could a preemption provision ensure that Federal law is no less protective than existing State laws? What are the useful criteria for comparatively assessing how protective different laws are?

It is essential that a preemption provision is appropriately narrowly tailored to reach only those state laws that expressly cover the same set of covered entities, while allowing states to specify additional protections on sensitive areas such as health and financial information.

CDT believes that the language in the privacy legislation that Congressman Bobby Rush introduced in the 111th Congress meets these criteria.[78] CDT recommends that a preemption provision of national FIPPs-based commercial data privacy policy track the preemption provision

[75] See Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 507, 113 Stat. 1338 (1999) (codified as 15 U.S.C. § 6807).
[76] *See* CAL. CIV. CODE § 1798.82(a).
[77] *See* National Conference of State Legislatures, State Security Breach Notification Laws (Apr. 12, 2010), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx.
[78] *See* H.R. 5777, *supra* note 18.

in Rush's bill.[79]

(c) To what extent should State Attorneys General be empowered to enforce national FIPPs-based commercial data privacy legislation?

State Attorneys General have been always essential consumer protection enforcers, and CDT strongly urges that state Attorneys General be given the authority to enforce baseline privacy law. CDT has previously endorsed the approach of the BEST PRACTICES bill, which granted the states the ability to enforce the bill's provisions and to obtain statutory penalties for violations.[80] In the rapidly changing online environment, sometimes state Attorney General offices are best equipped to bring quick, targeted consumer protection actions against emerging illegal practices. For example, state Attorneys General brought the first regulatory actions against adware companies when annoying "pop up" ad programs were becoming a major nuisance.[81] In 2009, the State of New York brought an enforcement action against a company for "astroturfing" (companies falsely posing as satisfied customers on internet message boards and other fora) well before the FTC issued its Endorsement Guidelines and began enforcing them.[82] The Federal Trade Commission is tasked with a wide range of responsibilities of which privacy protection is only one, and the Division of Privacy and Identity Protection has only a limited number of attorneys with a number of substantive duties, of which enforcement is only one. As long as states are enforcing one common standard, additional deputies to stop violations of privacy protection rules can only be positive.

(d) Should national FIPPs-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

CDT urges that it would be unwise to advocate for the general preemption of state or federal UDAP statutes as part of a baseline privacy law. For decades, statutes modeled on Section 5 of the FTC Act have been the staple tool for state Attorneys General to bring consumer protection actions on behalf of their citizens. These statutes have been interpreted to apply to a wide range of illegitimate activities, many of which have nothing to do with privacy. Certainly, a privacy law should not affect the enforcement of UDAP statutes in non-privacy related cases. However, regardless of whether consumer privacy legislation is passed, business practices that were previously deceptive or unfair to consumers would still be within the scope of behaviors that law should seek to prevent. Rather than try to sort out whether a particular deceptive or unfair practice falls within or without the umbrella of privacy protections, regulators should have the authority to act against a deceptive or unfair practice *qua* a deceptive or unfair practice. A narrow preemption provision for activities explicitly condoned by the FTC in a regulation or as part of a coregulatory safe harbor program may be appropriate, but it should be carefully crafted to be narrow in scope and to preempt UDAP laws generally.

---

[79] *Id.*

[80] *See* H.R. 5777, *supra* note 18; *see also* Harris, *supra* note 1.

[81] *See, e.g.,* Matt Hines, *Intermix hit with spyware suit*, CNET NEWS, April 28, 2005, http://news.cnet.com/Intermix-hit-with-spyware-suit/2100-7348_3-5688609.html; Joris Evers, *Washington state sues over spyware*, CNET NEWS, January 25, 2006, http://news.cnet.com/Washington-state-sues-over-spyware/2100-7348_3-6031108.html.

[82] Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.0 (2009) *available at* http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf; Press Release, Federal Trade Commission, Public Relations Firm to Settle FTC Charges that It Advertised Clients' Gaming Apps Through Misleading Online Endorsements (Aug. 26, 2010) *available at* http://www.ftc.gov/opa/2010/08/reverb.shtm.

(10) The Administration should review the Electronic Communications Privacy Act (ECPA), with a view to addressing privacy protection in cloud computing and location-based services. A goal of this effort should be to ensure that, as technology and market conditions change, ECPA continues to appropriately protect individuals' expectations of privacy and effectively punish unlawful access to and disclosure of consumer data.

CDT welcomes NTIA's recommendation that the Administration review and update the Electronic Communications Privacy Act. As convener of the Digital Due Process (DDP) coalition,[83] CDT continues to push for updates to ECPA. Because of technological advances, ECPA today is a patchwork of confusing standards that have been interpreted inconsistently by the courts. ECPA can no longer be applied in a clear and consistent way, and, consequently, the vast amount of personal information generated by today's digital communication services may no longer be adequately protected. Concern about the privacy afforded personal and business information can hold back adoption of emerging technologies, discouraging innovation. ECPA's complexity also imposes substantial costs on service providers seeking to review and comply with the data requests from law enforcement. ECPA must be flexible enough to allow law enforcement agencies and services providers to work effectively together, while at the same time ensuring that citizens can be confident that their expectations of privacy will be enforced and that businesses and innovators can rely on clear legal protections for their own and their customers' data.

Cloud computing and location-based cell tracking, in particular, challenge the existing statutory framework. Over the last few months, two federal appeals court decisions have concluded that ECPA has not kept up with advances in those two areas. In December, the Sixth Circuit ruled that the government must have a warrant before it can access the contents of email messages stored in the cloud.[84] The court stated that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[85] As a result, "to the extent that [ECPA] purports to permit the government to obtain such emails warrantlessly, [ECPA] is unconstitutional."[86] In September, the Third Circuit ruled that ECPA also allows magistrate judges discretion to require warrants from the government when it requests location information from a user's cell service.[87] These cases confirm the need for reform, and demonstrate once more that Congress should act to update the law, both to protect personal privacy and to ensure that businesses are not subject to the uncertainties associated with the slow, drawn-out process of developing law through the court system.

> *(a) The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that link any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.*

---

[83] DDP is a broad coalition of technology and communications companies, trade associations, advocacy groups, and think tanks, as well as academics and individual lawyers. For more information, *see* Digital Due Process, http://www.digitaldueprocess.org/ (last visited January 25, 2011).

[84] *United States v. Warshak*, 2010 U.S. App. LEXIS 25415 (6th Cir. Dec. 14, 2010).

[85] *Id.* at *35.

[86] *Id.* at *43.

[87] *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

The issue of privacy is critically important to both individuals and businesses that use cloud computing for commercial purposes,[88] and surveys have repeatedly demonstrated this fact. Despite the potential benefits in terms of productivity, cost, and flexibility,[89] a recent global ITGI survey states that only 60% of IT administrators are currently willing to use cloud computing in their enterprises, and less than 45% would do so for mission-critical applications.[90] The top concern preventing those administrators from adopting cloud services was data privacy, and the second most-commonly-named concern was security.[91] An annual CIO Magazine survey of American IT decision-makers finds that the top two concerns with cloud computing adoption are security and "loss of data control," and that the percentage of decision-makers with those concerns is increasing over time.[92] A recent survey from KPMG of Dutch businesses finds a large number of participants interested in moving to the cloud over the long term,[93] but again notes that less than 45% plan to move critical business functions there anytime soon,[94] mostly because of security and privacy concerns.[95] A Yankee Group survey of American businesses finds that 67% of those that currently use cloud computing use a private cloud operated for them alone,[96] despite that model's inability to fully realize the flexibility and cost savings of cloud computing. Again, they do so because of security and privacy concerns.

On the consumer side, a Pew survey looking at cloud computing growth on the consumer side found that more than two-thirds of individual Internet users were using some form of cloud computing service two years ago.[97] That study also found that 64% of American Internet users are concerned about cloud computing companies turning over their files to law enforcement.[98] A

---

[88] The cloud-computing providers themselves recognize this. *See, e.g.*, SALESFORCE.COM, SECURE, PRIVATE, AND TRUSTWORTHY: ENTERPRISE CLOUD COMPUTING WITH FORCE.COM 1 (2010), at http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf ("Polls and industry analysts consistently cite security and privacy concerns as the most significant barriers to the mainstream adoption of cloud computing, especially among enterprise customers."); MICROSOFT TRUSTWORTHY COMPUTING, PRIVACY IN THE CLOUD COMPUTING ERA: A MICROSOFT PERSPECTIVE 2 (2009), at http://download.microsoft.com/download/3/9/1/3912E37E-5D7A-4775-B677-B7C2BAF10807/cloud_privacy_wp_102809.pdf ("Consumers and businesses are willing to use online computing only if they trust that their data will remain private and secure.").

[89] KPMG, FROM HYPE TO FUTURE: KPMG'S 2010 CLOUD COMPUTING SURVEY 33 (2010), *available at* http://www.kpmg.com/AR/es/IssuesAndInsights/ArticlesPublications/KPMGInternacional/Documents/Cloud_Computing_Survey_2010.pdf (indicating in the figure the several advantages businesses have experienced from cloud computing adoption).

[90] IT GOVERNANCE INSTITUTE, GLOBAL STATUS REPORT ON THE GOVERNANCE OF ENTERPRISE IT 37 fig. 34 (GEIT) 2011 (January 2011), *available at* http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf.

[91] *Id.* at 38 fig. 35. 49.6% of respondents indicated that concerns about data privacy were preventing them from adopting cloud computing. 47.2% of respondents indicated security concerns, 41.7% indicated reliability concerns, and 34.6% indicated legacy investment issues.

[92] *See* CIO, *Cloud Computing Survey*, June 2009, at 1 fig. 1 *linked at* http://www.cio.com/article/498671/Cloud_Computing_Survey_Adoption_Prospects_Are_Hazy (click on link saying "Find the complete survey results here" and register to download). In 2009, 51% listed security as a concern, and 37% listed loss of control over data. In 2008, those numbers were, respectively, 45% and 26%.

[93] *See* KPMG, *supra* note 89, at the figure on p. 19 (indicating a long-term interest in cloud computing from more than 75% of firms).

[94] *Id.* at 35 (indicating in the figure that 62% of businesses have no near-term plans to move critical functions over to the cloud).

[95] *Id.* at 28 (indicating in the figure the major concerns that businesses have with cloud computing, with 76% of potential adopters concerned about security and 50% about privacy).

[96] *See* The Yankee Group, *Cloud Computing FastView Insights*, July 27, 2010, at http://www.yankeegroup.com/research/downloads/cloudComputingDatasheet.pdf.

[97] Pew Internet & American Life Project, *Use of Cloud Computing Applications and Services*, Sep. 12, 2008, at 4, *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.

[98] *Id.* at 7.

recent Zogby poll found that 88% of Americans believe consumers should enjoy similar legal privacy protections online as they have offline, while only 4% do not.[99] Moreover, cloud computing experts warn that potential business and consumer clients are seeking data storage centers outside the U.S. due to concerns that our laws give the government access to huge quantities of information with little judicial oversight.[100] If this trend continues, American workers may miss out on the jobs that would accompany the growth of this industry.

> *(b) The Task Force also seeks input on whether the current legal protections for transactional information and location information raise questions about what privacy expectations are reasonable and whether additional protections should be mandated by law. The Task Force also invites comments that discuss whether privacy protections for access to location information need clarification in order to facilitate the development, deployment and widespread adoption of new location-based services.*

Location-based services are another promising opportunity for U.S. companies. A 2010 study predicts that revenues from mobile location-based services will grow to more than $12.7 billion by 2014.[101] However, courts conflict on what level of legal protection is appropriate to protect this information from law enforcement access.[102] Researchers suggest that uncertainty about the privacy afforded location information against both commercial and governmental access can hold back consumer use of this technology.[103] Both anecdotally[104] and statistically,[105] privacy concerns with location-based services remain widespread. As CDT has previously noted,[106] additional statutory protection for both governmental and commercial access to location information is necessary to bring these tools into the mainstream and to ensure that citizens' reasonable expectations of privacy are protected.

---

[99] Zogby International, Results from June 4-7 Nationwide Poll (June 7, 2010), http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. According to the survey, the large majority (79%) believes law enforcement should have to get a warrant, like the one they have to get to wiretap phone conversations, to track where a user goes on the Internet, while 12% do not.

[100] Jeffery Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computing Paradigm*, MARKETSPACE, Mar. 20, 2009, at 38, available at http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf.

[101] Robin Wauters, *Mobile Location-Based Services Could Rake in $12.7 Billion by 2014: Report*, TECHCRUNCH, Feb. 23, 2010, http://techcrunch.com/2010/02/23/location-based-services-revenue (discussing study by Juniper Research).

[102] For a listing of the numerous cases espousing conflicting standards for disclosing to law enforcement either historical or prospective cell site data information, see *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Comm. on the Judiciary and Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. Exh. B (2010) (statement of Stephen Wm. Smith, United States Magistrate Judge), *available at* http://judiciary.house.gov/hearings/pdf/Smith100624.pdf.

[103] Tsai, et al., *Location-Sharing Technologies: Privacy Risks and Controls*, Carnegie Mellon University (Feb. 2010), p. 18, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[104] Claire Cain Miller & Jenna Wortham, *Technology Aside, Most People Still Decline to Be Located*, N.Y. TIMES, Aug. 29, 2010, at B1, *available at* http://www.nytimes.com/2010/08/30/technology/30location.html.

[105] A recent Webroot survey of 1500 social network users found that "55% of respondents said they worry over loss of privacy incurred from using geolocation data." Posting of Josh Halliday to The Guardian's Technology Blog (July 12, 2010 7:00 BST), at http://www.guardian.co.uk/technology/blog/2010/jul/12/geolocation-foursquare-gowalla-privacy-concerns (citing Webroot survey).

[106] *See The Privacy Implications of Location-Based Services: Hearing Before the H. Comm. on Energy and Commerce Subcomm. on Commerce, Trade, and Consumer Protection and Subcomm. on Communications, Technology, and the Internet*, 111th Cong. (2010) (statement of John B. Morris, General Counsel and Director of CDT's Internet Standards, Technology, and Policy Project), *available at* http://www.cdt.org/files/pdfs/CDT-MorrisLocationTestimony.pdf.