Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan for our Future	)	GN Docket Nos. 09-47, 09-51, 09-137
Comments – NBP Public Notice #29	)	
	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Leslie Harris
Ari Schwartz
Alissa Cooper
Erica Newland
Heather West
Andrew McDiarmid
Jonathan Dunn

Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, DC 20006
(202) 637-9800

January 22, 2010

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
A National Broadband Plan for our Future	)	GN Docket Nos. 09-47, 09-51, 09-137
Comments – NBP Public Notice #29	)	
	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commission's NBP Public Notice 29, regarding privacy concerns and expectations associated with broadband adoption and use. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet.

Summary

National broadband access will support innumerable innovative online applications and provide great societal benefit if privacy is addressed in meaningful ways from the beginning. Promoting privacy online will encourage more citizens to take advantage of the benefits that broadband Internet can deliver and therefore help to achieve "maximum utilization of broadband" and other goals cited in the Recovery Act.

In its report to Congress, the Commission can contribute to the development of privacy policy in the US by highlighting the role of consumer trust in promoting adoption of broadband-based applications. The National Broadband Plan should include a comprehensive set of recommendations for appropriate government bodies and companies detailing how these entities can protect consumer privacy online. CDT believes that fully protecting consumer privacy interests online requires a rigorous mix of self-regulation, enforcement of existing law, development of technical tools and standards, and enactment of new legislation. In these comments, we discuss six of the most important recommendations that we believe the Commission can make in its broadband report.

1) The National Broadband Plan should release an updated version of Fair Information Practice Principles (FIPs) to guide privacy practices by the federal government and industry: Through the National Broadband Plan, the Commission can play an important role in defining and clarifying the meaning and substance of consumer privacy. We urge the Commission to endorse a modern, comprehensive set of FIPs and to recommend these principles to policymakers as the best available basis for federal legislation, agency rules, and self-regulatory guidelines.

2) The National Broadband Plan should recommend enactment of a federal baseline consumer privacy law: Despite how critical privacy protections are to the continued health of the Internet, the United States lacks a comprehensive consumer privacy law. Instead, American consumers currently face a confusing patchwork of privacy standards that offer only weak protections for much personal information collected by businesses and that leave some information unprotected in surprising ways. The National Broadband Plan should call on Congress to enact general privacy legislation. Simple, flexible legislation would protect consumers from inappropriate collection and use of their personal information while enabling legitimate business use to promote economic and social value. In principle, such legislation would codify the fundamentals of FIPs. While self-regulation would likely still be necessary to address certain areas not covered by a baseline privacy law, self-regulation cannot suffice on its own.

3) The National Broadband Plan should recommend updates to the Privacy Act of 1974: The Privacy Act of 1974 is the primary law regulating federal agencies' collection, maintenance, use, and dissemination of personal information. The Privacy Act is woefully outdated and must be updated to ensure its relevance into the future. The Act's limitations are particularly apparent with regard to government use of commercially-compiled personal information.[1] The FCC should recommend that Congress update the Privacy Act to provide more robust privacy protections for American citizens, integrating protections for new technological paradigms and transactional data.

4) The National Broadband Plan should promote the incorporation of Privacy by Design principles into both innovation and business and government practices: The "foundational principles" of Privacy by Design should be implemented to guide innovation in a manner that is consistent with FIPs.[2] Privacy by Design offers a roadmap for integrating privacy considerations into business models, product development cycle, and new technologies. The FCC should recommend that Congress and the FTC act to encourage business practices that are consistent with Privacy by Design and that the National Institute of Standards and Technology (NIST) deliver Privacy by Design standards for government agencies.

5) The National Broadband Plan should encourage a marketplace of privacy protective, user-centric decentralized identity providers: Decentralized identity management will be a key building block for new broadband applications, allowing users to share information using trusted providers and enabling new, innovative online applications. The keys to creating trusted relationships online are creating meaningful privacy and security and enabling user control within the identity management system. CDT recommends that trusted frameworks mediate the policies and practices of identity management providers. To avoid the creation of a massive and potentially vulnerable centralized repository of highly sensitive personal information on almost every American,

---

[1] *Privacy: The Use of Commercial Information Resellers by Federal Agencies. Hearing Before the Subcomm. on Information Policy, Census, and National Archives of the House Comm. on Energy and Commerce*, 110th Cong., 2nd Sess. (March 11, 2008) (statement of Ari Schwartz, Deputy Director, Center for Democracy & Technology); *available at* http://www.cdt.org/files/pdfs/20080311schwartz.pdf

[2] Anne Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August, 2009)*, available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

it is essential that identity management systems have a federated, or decentralized, structure.

6) The National Broadband Plan should encourage innovation and consumer protection in third-party applications: The past two years have seen the introduction and rapid adoption of a new model for broadband-enabled services: companies are increasingly opening their platforms to the public, allowing every-man innovators, advertisers, and even competitor companies to contribute applications that enhance the original platform in previously unimaginable ways. While these third-party applications have seen a boom in innovation, they have also attracted developers whose goal is to prey on weak security and privacy regimes. Creation of a trustworthy marketplace for third-party applications is not impossible. In fact, platform providers can go a long way in offering privacy and security protective regimes for consumers without fear of liability. CDT notes that existing limitations on liability for content provided by others and limitations on liability for voluntary filtering of content provided by others are specifically intended to encourage responsible innovation by providers of forums for third-party content. With the threat of liability removed, providers can launch more open and innovative platforms with less risk, while marketplace pressures to cultivate consumer goodwill are likely sufficient to encourage responsible vetting of applications. The FCC can play an important role in encouraging platform providers to build protections into their platforms while keeping them open, beginning with self-regulatory, information sharing and law enforcement reporting projects.

Introduction

National broadband access will support innumerable innovative online applications and provide great societal benefit if privacy is addressed in meaningful ways from the beginning. We thank the Commission for bringing attention to and addressing the privacy concerns of these new, broadband-enabled technologies.

These technologies include e-Government, smart grid technologies, and electronic health records. The applications and services enabled by these technologies depend on the widespread availability of affordable broadband and will drive demand for broadband services. However, these applications also pose risks to consumer privacy because they involve the collection and exchange of sensitive personal information. In some implementations they will require the development of more robust identification and authentication services to enable the exchange and management of user data. Therefore, consumer acceptance – and hence to some extent the future of broadband use – depend on the degree to which consumer privacy is protected. To increase consumer trust and truly achieve the potential of broadband, these applications require a robust and comprehensive privacy protection framework.

In CDT's June 2009 comments in response to the Commission's Notice of Inquiry ("NOI"), FCC 09-31, regarding the development of a national broadband plan for the United States,[3] we urged that a national broadband plan include recommendations for a number of policy initiatives and reforms that could help spur the Internet's continued

[3] *See Comments of the Center for Democracy & Technology In the Matter of A National Broadband Plan for our Future* (June 2009), *available at* http://www.cdt.org/files/pdfs/20090608_broadband_comments.pdf.

growth. For example, while protecting privacy is a valuable goal in its own right, promoting privacy online will also help foster growing broadband usage and demand by encouraging more citizens to take advantage of the benefits that broadband Internet can deliver. Protecting privacy therefore can help to achieve "maximum utilization of broadband" and advance consumer welfare and the other goals cited in the Recovery Act. While many of the policies that can help ensure online privacy are outside the Commission's normal jurisdiction, the National Broadband Plan offers the Commission the opportunity to recommend that Congress and other entities take action on this front.

Privacy is an essential building block of trust in the digital age. Privacy protections help to secure our communications and sensitive data, providing a foundation for e-commerce and the full realization of the potential benefits of the networked world. Privacy and the ability to remain anonymous are also fundamental to free expression, which has flourished nowhere more vibrantly than on the broadband Internet. For the broadband Internet to continue to thrive, consumers need to be assured that their communications and transactions will be secure, confidential, and anonymous.

In recent years, however, and at an accelerating pace, technology and market forces have created fundamental challenges to online privacy. More data is collected about individuals and retained for longer periods than ever before. Massive increases in data storage and processing power have sown the seeds for diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online activities. Study after study has shown that consumers do not understand how their data is used under these new models – and when they find out, it is cause for great concern.[4] Privacy worries continue to inhibit some consumers from engaging in even more established business models such as online shopping.[5] Privacy need not be a roadblock to broadband adoption. If privacy and security can be built into the infrastructure, the payback in user trust would far exceed the investment. Only with strong privacy protections will consumers be willing to take advantage of the full spectrum of services and opportunities that broadband Internet can offer.

The National Broadband Plan should include a comprehensive set of recommendations setting out the roles and responsibilities for government and industry to protect consumer privacy online and ensure that consumers are able to take advantage of the service that broadband offers – without having to relinquish their reasonable expectations of privacy. In these comments, we present six of the most important recommendations that we believe the Commission can include in its broadband report.

---

[4] *See, e.g.*, Alan F. Westin, *How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings,* Mar. 2008 (in which the majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, *Use of Cloud Computing Services,* (Sept. 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[5] *See* John B. Horrigan, *Online Shopping* (Feb. 2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf.

I. The National Broadband Plan should release an updated version of Fair Information Practice Principles (FIPs) to guide privacy practices by the federal government and industry.

A. An updated set of FIPS

Ensuring trust on the broadband Internet depends on the establishment of a guiding framework that recognizes the rights of consumers and the responsibilities of entities that collect, use, and share data about consumers. That framework already exists in the form of the FIPs that serve as the basis of existing privacy law and practice in the US. The first set of FIPs was released in 1973 by the Health Education and Welfare Department. Since that time, various versions of the FIPs have been used by federal agencies internally and externally; each agency adopts and abides by its own set of FIP principles. These sets of FIPs range in quality from the weak version adopted by the FTC in 2000[6] – which focus exclusively on notice, choice, access, and security – to the robust set adopted by DHS in 2008.

The set of FIPs adopted by DHS in 2008 provides a modern and comprehensive framework for articulating privacy expectations and privacy protections. CDT together with other groups has provided an overview of the FIPs in a separate filing,[7] but we offer the following set, based on the 2008 DHS FIPs, for reference within these comments:[8]

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of information.*
- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*
- **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*

---

[6] In 2000, the FTC issued a set of FIP principles that is far more limited than the most modern, comprehensive set used in the federal government. That year, the FTC issued a report to Congress outlining four core principles of privacy protection: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, and (4) Integrity/Security. The FTC's FIPs have, in practice, only yielded a focus on notice, consent, and security and have been insufficient to promote the types of privacy protections needed in the growing online ecosystem. This condensed set of FIPs has been largely criticized as a watered down version of previous principles. These principles focus narrowly on Web site privacy policies in practice, resulting in today's stagnant notice-and-consent framework.

[7] *See* Joint Comments of the Center for Democracy & Technology et. al, *In the Matter of a National Broadband Plan for our Future, NBP Public Notice #29* (January 22, 2010).

[8] *See* U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf ("DHS FIPs").

- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as is necessary to fulfill a specified purpose.*

- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*

- **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.*

- **Security.** *Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

- **Accountability and Auditing.** *Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

We urge the Commission to incorporate these or a similarly robust set of FIPs into its privacy recommendations in the broadband plan.

B. The National Broadband Plan should redefine "user control"

In recent years, through the cases it has brought and the reports and guidelines it has issued, the FTC has played an important role in promoting good privacy practices online. Although its authority has been limited in many respects, the FTC has forced a discussion of online privacy practices that was not happening elsewhere, most recently with its set of privacy roundtables. [9]

In pursuing online privacy protections, the FTC should be encouraged to broaden its conception of user control from click-of-the-button "consent" to a set of consumer rights and company responsibilities that together fortify and protect the decisions that consumers make online. The current notice and consent paradigm, which has been built around the limited set of FIPs that the FTC issued in 2000 and that governs how businesses handle online privacy issues, at best only gives consumers control over their data at the point of collection.[10] Long after data is collected, it lives in a Wild West of shared and sold personal profiles and databases that give consumers no control over how their identities will be tracked and used. As FTC Commissioner Pamela Jones Harbour has said, "Once data is shared, it cannot simply be recalled or deleted – which magnifies the cumulative consequences for consumers, whether they realize it or not."[11]

---

[9] *See* FTC – Exploring Privacy, A Roundtable Series, *available* at http://www.ftc.gov/bcp/workshops/privacyroundtables/. *Last Accessed January 22, 2010.*

[10] *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), *available at www.ftc.gov/reports/privacy2000/privacy2000.pdf ("Fair Information Practices in the Electronic Marketplace").*

[11] *See* Concurring Statement of Commissioner Pamela Jones Harbour, *Regarding Staff Report, Self-Regulatory Principles for Online Behavioral Advertising*, *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf.

An analysis of the FTC's 2009 settlement with Sears Holding Corp. highlights the need to move beyond today's simple notice and consent regime both within the FTC and more broadly. Between 2007 and 2008, Sears encouraged users to download tracking software on their computers.[12] This software monitored consumers' activities for clues about both online and offline behavior, peering into secure online sessions and culling information from consumers' email subjects and recipients, online bank statements, drug prescription records, video rental records, and similar histories and accounts. Although Sears offered customers a $10 coupon to download the software, the FTC nonetheless brought a complaint, concluding that consumers are harmed by privacy invasions in and of themselves. Companies must be certain that consumers clearly understand when they are selling their privacy.

The Sears case is an important example of the type of risk posed by future broadband applications. Despite the monumental privacy invasion involved in the Sears case, we would not be surprised to see the same practices used in the future by companies that track consumers just as insidiously but provide marginally clearer notification of their practices. Indeed, a company in similar circumstances may be able to sell consumers' personal information to others without providing customers the ability to revoke that information from the buyer. In the present regulatory environment, such a company would merely need to be a little more upfront about its intentions than Sears was in this case. This type of practice represents a threat to consumers' ability to trust companies use of their information.

The FTC's complaint against Sears focused on the fact that the extensive tracking undertaken by the software was neither accurately represented nor adequately disclosed by language buried deep in the Privacy Statement and User License Agreement.[13] The complaint represents broader recognition that few consumers read or understand these kinds of disclosures about online data collection and use practices.[14] As David Vladeck, Director of the FTC Bureau of Consumer Protection, recently told the *New York Times*,

---

[12] Between 2007 and 2008, 15 of every 100 visitors to sears.com or kmart.com were presented with a pop-up window that offered the opportunity to "talk directly to a retailer" and become part of "a place where your voice is heard and your opinion matters, and what you want and need counts!" No mention was made that this "opportunity" also installed detailed tracking software on the user's computer. Customers who asked for more information were offered a $10 coupon in exchange for downloading – and keeping on their computer for at least one month – software from Sears or K-mart that would allow them to become "part of something new, something different[.]" This software monitored consumers' online activities, including email messages, online banking sessions, and other similar activities. Customers consented to the download and tracking by agreeing to a lengthy terms of service agreement that showed up at the end of a long registration process. The agreement was presented in a small "scroll box"; consumers could only see ten lines of the policy at a time and not until the 75th line could the user find any description of the invasive tracking. *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.

[13] *See id.*

[14] U.S. District Court Judge Sterling Johnson Jr. recently ruled that simply posting a link to onerous terms and conditions on a website is not binding for the consumer. His reasoning? The evidence that any consumers actually read these policies is scant. *See* Wendy Davis, *Court Rules Overstock Can't Enforce 'Browsewrap' Agreement*, MediaPost Blogs (Sept. 14, 2009), *available at* http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=113404 (last visited Nov. 3, 2009). Further, in a large-scale study of consumer attitudes toward behavioral advertising, 62% of respondents believed that "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission." *See* Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

"the empirical evidence we're seeing is that disclosures on their own don't work, particularly disclosures that are long, they're written by lawyers, and they're written largely as a defense to liability cases. Maybe we're moving into a post-disclosure environment."[15]

The FTC should be encouraged to continue to promote industry best practices in this "post-disclosure environment" through the adoption of a comprehensive set of FIPs. The FTC's 2000 FIPs are insufficient in the present environment, one that sees consumer information collected and used in increasingly insidious ways. The Sears case also further exemplifies why the National Broadband Plan should endorse a new set of FIPs for all federal agencies, one based on those released by DHS. Future guidelines and principles on privacy-related topics, including those issued by the FTC, should be built around these FIPs.

For a set of recommendations and analyses detailing how the FTC's role in the online consumer protection space can be refocused and expanded, see CDT's November 6 comments to the FTC in Appendix A.

C. The National Broadband Plan should encourage establishment of benchmarks and metrics for evaluating company privacy practices.

One of the biggest challenges in establishing a framework for protecting consumer privacy is creating benchmarks and metrics for measuring whether privacy protections are in fact improving.

In particular, there has been too much focus on compliance efforts and not enough time spent attempting to find actual performance measures. For example, in the past, the FTC has evaluated success by counting the number of privacy policies online and the comprehensiveness of these policies[16] – but long privacy policies are not equivalent to better privacy protections. One obvious interim step is to measure the quality of compliance (that is, measuring whether policies actually protect privacy rather than simply attempting to indemnify a company with bad practices), however, even that type of measure does not really examine whether privacy is better protected.

The FTC's annual report on the number of identity thefts is one example of a useful metric, and we believe that with detailed research regulators can construct more ways to measure how well industries are protecting user privacy. Benchmarks are necessary for accountability and performance metrics are the best tools we have to see if efforts in this space are indeed succeeding. This same discussion is occurring within the federal government, as government agencies seeks to marry security and privacy measures.[17]

---

[15] *See An Interview with David Vladeck of the F.T.C.*, NYTIMES.COM, Aug. 5, 2009, *available at* http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (last visited Nov. 5, 2009) (Vladeck also remarked that given the "disclosures" complexity, "I'm not sure that [so-called] consent really reflects a volitional, knowing act.").

[16] *See* Fair Information Practices in the Electronic Marketplace.

[17] *See, e.g.*, *Protecting Personal Information: Is the Federal Government Doing Enough?: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 110th Cong., 1st Sess. (June 18, 2008) (statement of Ari Schwartz, Vice President, Center for Democracy & Technology).

The FTC should also be encouraged to conduct a roundtable and produce a report on this specific topic of developing performance standards on privacy.

II. The National Broadband Plan should recommend the enactment of a federal baseline consumer privacy law

Despite the unprecedented challenges to privacy in the modern environment, the United States still has no comprehensive law that spells out consumers' privacy rights in the commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage. For example, while there is a strong privacy law for cable viewing records, no law protects online purchasing data, and while the Commission's CPNI rules offer protections for location information collected by carriers, no comparable rules exist for the same information collected by other service providers. Consumers and companies alike deserve consumer privacy legislation that clarifies the general rules for all parties. The National Broadband Plan should recommend that Congress pass general consumer privacy legislation that codifies a full set of FIPs. Such legislation should include broad FTC rulemaking authority under Section 5 of the FTC Act that will enable the FTC to act with greater flexibility and within a more reasonable timeframe than it can today under its Magnuson-Moss rulemaking authority. Consumer privacy legislation should clarify how it applies to industries whose activities fall outside the FTC's scope. The FTC should not, however, be the only enforcement body for privacy. State attorneys general have an important role to play in policing consumer privacy violations.[18] A limited privacy right of action with a cap on damages would also be helpful for enforcement purposes. The FCC should recommend in the National Broadband Plan that Congress pass consumer privacy legislation that provides for both of these enforcement mechanisms.

A. Self-regulation cannot substitute for legislation

Industry members have long pointed to self-regulatory efforts as proof that baseline, federal privacy legislation would be duplicative and calamitous for innovation. In the past, the FTC too has suggested that self-regulatory regimes might play an important part in protecting consumer privacy. But FTC commissioners have also recognized that "self-regulation cannot exist in a vacuum."[19] Indeed, after the Google/DoubleClick merger FTC Chairman Jon Leibowitz warned: "Ultimately, if the online industry does not adequately address consumer privacy through self-regulatory approaches, it may well risk a far greater response from government."[20]

---

[18] The FTC can, however, influence the way state law enforcement handles privacy invasions. For example, the principles outlined by the FTC in its battles against spyware have helped to direct state law enforcers who have already begun to take on spyware cases. The spyware space is fraught with gray areas and the FTC's guiding principles provide a simple, understandable baseline for current and future law enforcers as they wade into spyware issues with which they may be unfamiliar. In this way, the leadership of the FTC has been a vital component in expanding the nationwide pool of law enforcement resources dedicated to combating spyware.

[19] Concurring Statement of Commissioner Pamela Jones Harbour, *Regarding Staff Report, Self-Regulatory Principles for Online Behavioral Advertising*, *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf.

[20] Concurring Statement of Commissioner Jon Leibowitz, *Google/DoubleClick*, *available at* http://www.ftc.gov/os/caselist/0710170/071220leib.pdf.

CDT believes that a fair review of current business practices with regard to the use of personal and sensitive information of individuals (see Appendix A, section II.C.) will reveal that the time for "a far greater response from government" is now: self-regulation works most effectively when consumer privacy legislation and effective enforcement exist to provide it with a meaningful backbone.[21] Fully protecting consumer privacy interests online requires a rigorous mix of self-regulation, enforcement of existing law, development of technical tools and standards, and enactment of new legislation.

III. The National Broadband Plan should recommend updates to the Privacy Act of 1974

A. The need for better rules for use of data by government agencies

The Privacy Act of 1974 is the single, major law that determines the way that the government collects, handles, maintains, protects, uses, shares, and destroys personal information held by federal agencies. The current rules on government access and use of data do not adequately govern transactional data or other modern data held by government agencies and are not sufficient to ensure that this data cannot be abused.

1. The base of the law is still sound

The Privacy Act of 1974 was passed as the result of a government-wide push toward the development of policies and practices to protect the information of citizens and other individuals. While the underlying framework is still sound, the thirty-five year-old wording of the Act renders it ill-equipped to meet many of the privacy challenges posed by modern information technology. In particular, transactional data is not addressed by the Act, which was passed to address relatively simple database technologies and data stored in filecabinets.

Despite the excellent basis and framework for the law, loopholes were identified as soon as 1977, when the Privacy Protection Study Commission found that advances in technology threatened to outpace the Privacy Act. Recent advances in information technology render the limitations of the Privacy Act even more significant. Transactional data poses special problems for the Privacy Act as the cost of data storage technologies drops and data mining technologies evolve. These kinds of small, repeated data points were not imagined by the drafters of the Privacy Act, nor were the data mining technologies that piece information together to make guesses about individuals.

2. Updating the Privacy Act to reflect updated technologies

The Privacy Act was designed to accommodate agency-held flat files, but computing has moved towards forms of networked centralization and relational databases beyond the Privacy Act's reach. In addition, the Privacy Act's drafters did not contemplate the industry that has arisen around collecting and sharing information with the government. Even the E-Government Act of 2002 failed to close the gulf between the letter of the

[21] Ira Rubenstein documents this issue in detail in his draft paper Privacy, Self-Regulation, and Statutory Safe Harbors (November 2009), *available at* http://www.law.nyu.edu/ecm_dlv3/groups/public/@nyu_law_website__centers__information_law_institute/documents/documents/ecm_pro_063814.pdf.

Privacy Act and modern technologies. To adequately protect privacy in this digital age, Congress and the Executive Branch will need to work together to close the long-recognized gaps in existing laws and policies. The FCC should recommend that laws regulating government protection of user data, including transactional data, be updated to address new technologies and techniques. At the same time, both Congress and the Executive branch must foster the leadership and insist upon the measurement capabilities needed to ensure that existing and new laws and policies are implemented uniformly and diligently.

Building on the recent work of the US Information Security and Privacy Advisory Board[22] and the Government Accountability Office,[23] CDT brought together a working group of public interest organizations, government representatives, and members of the private sector to draft the E-Privacy Act Amendments of 2009.[24] We opened this policy-drafting process to the public through a wiki that allowed the public to edit the draft. This process, as well as our working group, created a set of updates that address many of the shortcomings of the Privacy Act as laid out by the PPSC, GAO, and ISPAB.

Simple definition updates are key to any update of the Privacy Act. The technologies in use today are so different than those in use 35 years ago that the switch that turns the law on – the definition of a "system of records" – cannot address some of the most common database techniques in use today. We recommend a set of updates to definitions in order to clarify what the Privacy Act governs. In addition, the Privacy Act must be clarified to include all personal information used by agencies, rather than only information collected or held by agencies. In an age of data resellers, the definitions must be expanded to fit the practices of agencies.

Amendments to the Privacy Act and the E-Government Act's privacy provisions are urgently needed in order to improve privacy notices and create a Privacy.gov website to centralize information about privacy practices. This would also allow citizens to access the complete privacy notices of government agencies, notices that are currently fragmented across many editions of the Federal Register and are almost impossible to understand. We have also proposed that Routine Uses be redesigned to reflect the intentions of legislation and clarify what and how agencies are allowed to share information.

Most of all, privacy leadership within the federal government must be created. A Chief Privacy Officer should be created for the Federal government and every federal agency (including the FCC), in order to coordinate and organize privacy policy for the government and coordinate privacy officers at federal agencies. Privacy guidance must be regularly updated and must address new technologies.

---

[22] *See* NIST ISPAB Report, *Toward a 21st Century Framework for Federal Government Privacy Policy* (May 2009), *available at* http://www.cdt.org/privacy/20090529_ispab_rpt.pdf.

[23] *See* United States Government Accountability Office, PRIVACY: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information (June 18, 2008), *available at* http://www.gao.gov/products/GAO-08-795T.

[24] *See* E-Privacy Act Amendments Wiki, *available at* www.eprivacyact.org.

We call on the Commission to urge Congress to update the Privacy Act of 1974 and bring the federal government's privacy framework into the 21st century.

IV. The National Broadband Plan should promote the incorporation of Privacy by Design principles into both innovation and business and government practices

A. Background

In previous sections of these comments, we emphasized how adherence to a full set of FIPs can yield strong privacy protections for Internet users. In this section, we discuss how the principles of Privacy by Design – the incorporation of privacy into the very fabric of new technologies and the policies that govern them —– can be used to guide the implementation of these FIPs. Below, we first describe the general relationship between Privacy by Design and Fair Information Practice principles. We then discuss how the federal government can promote Privacy by Design. Appendix B includes an analysis of how adherence to the Data Minimization FIP and the collection and use of sensitive data can be guided by Privacy by Design principles.

B. Privacy by Design – a set of guiding principles for implementing FIPs

Privacy by Design, a concept prominently championed by Ontario's Information and Privacy Commissioner Anne Cavoukian, offers a roadmap for integrating privacy considerations into business models, product development cycles, and new technologies.

As described by Cavoukian, "Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation." Privacy by Design presents a set of "foundational principles" that can help companies innovate in ways that are consistent with FIPs. These seven principles are listed in abbreviated form below:[25]

- **Proactive, not Reactive; Preventative, not Remedial.** *The Privacy by Design approach … anticipates and prevents privacy invasive events before they happen. [It] does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.*
- **Privacy as the Default.** *If an individual does nothing, their privacy still remains intact.*
- **Privacy Embedded into Design**. *Privacy by Design … is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.*
- **Full Functionality – Positive-Sum, not Zero-Sum.** *Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.*

[25] Anne Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August, 2009), *available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

- **End-to-End Lifecycle Protection.** *Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish.*
- **Visibility and Transparency.** *Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.*
- **Respect for User Privacy.** *Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.*

These principles represent one set of tools that can help companies realize the implementation of a comprehensive set of FIPs; they suggest how some – though not all – of the privacy concerns raised *by* new technologies can be addressed *through* new technologies and solid business practices.

Cavoukian has published a Privacy by Design Diagnostic Tool Workbook that companies can use to determine whether and how they are complying with Privacy by Design principles.[26] Meanwhile, many companies, including IBM, Sun Microsystems, Hewlett-Packard, and Microsoft have already incorporated Privacy by Design into their product development processes and made strong statements about the important role that protecting privacy plays in their business models.[27]

Microsoft's implementation of its "Security Development Lifecycle" (SDL) for software development provides one example of how privacy can be built into the design process.[28] SDL aims to integrate privacy and security principles into the software development lifecycle, but each stage of Microsoft's five-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,"[29] a document that lays out guidelines that track some of Cavoukian's Privacy by Design principles End-to-End Lifecycle Protection, Privacy Embedded into Design,

---

[26] *See* Anne Caovukian, *Privacy Diagnostic Tool (PDT) Workbook* (August, 2001)*, Version 1.0, available at* www.ipc.on.ca/images/Resources/pdt.pdf.

[27] 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 (February 2009) at 5, *available at* http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en ("Microsoft Privacy Guidelines"); Hewlett-Packard Development Company, Protecting Privacy at HP: Giving Individuals More Control over their Information (August, 2007), *available at* http://h41111.www4.hp.com/globalcitizenship/uk/en/pdf/Privacy_casestudy_hires.pdf; Michelle Dennedy, Sun Privacy-enhancing Desktop Technologies (January 2009), *available at* http://www.privacybydesign.ca/speaker-dennedy.htm.

[28] See Microsoft Corporation, Microsoft Security Development Lifecycle - Process Guidance (2009), *available at* http://msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746bopq.aspx ("Microsoft SDL"). These guidelines are made available online in a form that tracks, but is abbreviated from, those used by Microsoft internally.

[29] See Microsoft Privacy Guidelines.

and Proactive, not Reactive Design. Microsoft's SDL and guidelines are not perfect.[30] But Microsoft's work in this space remains a positive example of how privacy impact can be evaluated during the planning stages of innovation, how this evaluation can be incorporated into product development, and how Privacy by Design can help ensure that FIPs such as Data Minimization, Individual Participation, and Security are heeded.

As the FCC seeks to promote implementation of a more robust set of FIPs that will benefit companies and consumers alike, we urge it to look to proactive approaches taken by companies, guidelines like Cavoukian's workbook, and documents such as CDT's Threshold Analysis, a framework developed with companies and advocates in our Internet Privacy Working Groups to help online advertisers evaluate their practices as a precursor to a full privacy impact assessment or fair information practices analysis.[31]

But Privacy by Design should not be seen as a replacement for much needed comprehensive, federal baseline consumer privacy legislation or a stronger regulatory approach to privacy. Foremost, Privacy by Design relies on an assumption of good actors who work with the understanding that protecting privacy is protecting business. It is clear that not all entities operating in the online marketplace prioritize privacy. Privacy by Design, while important, should be seen as one tool in a larger toolkit that includes regulatory approaches.

C. How the Government can encourage Privacy by Design

The federal government should commit itself to incorporating Privacy by Design into its operations and promoting Privacy Enhancing Technologies as part of its open government initiative as well as of part of day-to-day government operations. The federal government can have a considerable impact on the marketplace simply through leading by example. This simple form of leadership has already positively impacted the market by advancing privacy protections in the consumer space. For example, during the first weeks of the Obama administration, WhiteHouse.gov met with criticisms that cookies belonging to the White House's video provider YouTube were set as soon as a visitor accessed the landing page containing a video, in violation of WhiteHouse.gov's privacy policy and user expectations. The White House quickly responded and instituted a fix for its video cookie problem so that merely visiting a landing page containing a video does not automatically set a persistent cookie; the White House also worked with YouTube to develop a robust solution that protected user privacy while allowing the WhiteHouse.gov to use a state of the art video solution.[32] Within weeks, YouTube had made use of these "delayed cookies" available for any video on any site – bringing the privacy protective

---

[30]The guidelines, for example, do not fully implement a comprehensive set of FIPS into the design process; they rely on an outdated distinction between personally identifiable information and non-personally identifiable information that is too simplistic and should no longer be central to the privacy framework in this space, See Microsoft Privacy Guidelines.

For a discussion about how the identifiability of data should be reconceptualized, See Center for Democracy and Technology, Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, but Still Insufficient On Its Own to Protect Consumers (December, 2009) at 10-11, available at http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf ("CDT Behavioral Advertising").

[31] Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf ("Threshold Analysis").

[32] [32] *See* Alissa Cooper, *E-Gov 2.0 in Action* (Jan 22, 2009), *available at* http://blog.cdt.org/2009/01/22/e-gov-20-in-action.

innovation required by government web sites to every YouTube provider.[33] By insisting that the White House operate a Web site that promotes user privacy, the Obama administration influenced the provider and thereby brought a new Privacy Enhancing Technology to the marketplace. In turn, competing providers will innovate and highlight their privacy protective features.

The National Broadband Plan should call on the federal government to continue to incorporate the most modern and comprehensive sets of best practices into their policies, requiring that companies offer innovative new technologies to protect privacy in order to gain the government as a client. In 2009, along with the Electronic Frontier Foundation (EFF), CDT submitted comments to the Office of Management and Budget (OMB) detailing how the federal government should update its policy on tracking technologies used on government Web sites. We recommended a privacy protective policy that reflects the realities of agency culture, user expectations, and the needs of technological progress while continuing to respect FIPs. As it seeks to address the role that the federal government can play in promoting Privacy by Design, the National Broadband Plan should incorporate the principles and practices laid out in these comments.[34]

The National Broadband Plan should also call on Congress to pass a comprehensive update of the Privacy Act. This is an important part of creating a culture that builds privacy within the government. One important tool in helping agencies consider privacy early in progarm lifecycles and work to mitigate any risks to privacy is the Privacy Impact Assessment (PIA). PIAs are mandated by the E-Government Act of 2002 as analyses of the potential privacy impact of any new program or technology that an agency is developing. Agencies are expected to show that they have examined, mitigated, and justified any privacy risks assocaited with information. The PIA, when treated seriously, is a valuable tool for identifying and addressing privacy concerns associated with government records systems. While PIAs at some agencies, such as the Department of Homeland Security (DHS), have yielded comprehensive analyses of the potential impacts of new technologies or data collections, the GAO found that most agencies either provide summary one or two pages PIAs that contain limited information or do not provide PIAs at all.[35] Creating best practices for conducting PIAs and implementing privacy notices, and enforcing the requirement that all programs with information collections complete PIAs, would motivate agencies to address privacy and security concerns as programs are developed. This would promote key tenets of Privacy by Design within the federal government and would provide a positive model for industry practices. CDT has proposed further improvements to the privacy provisions of the E-Government Act as part of the E-Privacy Act Amendments, which also provide recommended updates to the Privacy Act.

---

[33] *See* Alissa Cooper, *WhiteHouse.Gov: Moving the Cookie Forward* (March 3, 2009), *available at* http://www.cdt.org/blogs/alissa-cooper/whitehousegov-moving-cookie-forward.

[34] *See* Center for Democracy & Technology, *Comments Regarding the Office of Management and Budget's Proposed Revisions of the Policy on Web Tracking Technologies for Federal Agencies* (August 2009) *available at* http://www.cdt.org/privacy/20090810_omb_cookies.pdf.

[35] *See* United States Government Accountability Office, *PRIVACY: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (May 2008), *available at* http://www.gao.gov/new.items/d08536.pdf.

Finally, the Broadband Plan should urge the US National Institute of Standards and Technology (NIST) to promote privacy protective standards for the federal government. NIST plays a key role in many areas of computer security and privacy. Most prominently, NIST has been the leading body to define encryption standards. NIST should work to implement the recommendations found in its Information Security and Privacy Board document "Toward a 21st Century Framework for Federal Government Privacy Policy." More generally, NIST should be encouraged to set standards for government implementation of Privacy by Design in much the same way it has set security standards.[36]

D. Promoting Privacy by Design by promoting technical standards

Technical standards and Internet standards bodies can have an influential impact on consumer privacy. For example, CDT has been working for years to incorporate some key principles for the protection of sensitive location information into technical standards, originally in the Internet Engineering Task Force's (IETF) Geopriv working group[37] and more recently within the World Wide Web Consortium (W3C) Geolocation working group. The W3C Geolocation group created the draft standard that Apple and other vendors of location-aware browsers are starting to use.[38]

Before that, CDT was involved in the development of the Platform for Privacy Preferences (P3P), a standard of the W3C, the main standard setting body for the Web. P3P was designed to provide machine-readable statements that can express the privacy practices of a Web site or a third party intermediary, such as a network advertiser or an analytics company. The theory was that such statements would provide a clear, standardized means of rendering potentially complex privacy policies into a format that could be automatically parsed and instantly acted upon. P3P has never been fully implemented as its creators had hoped, but its development and implementation have resulted in some key privacy protections and offer important lessons about the role that technical standards can play in protecting consumer privacy and the limitations of relying on these standards.[39] Those lessons are detailed in Appendix C.

Technical standards can harness the power of information technology to help implement individual FIP principles. They are perhaps the most obvious example of the third Privacy by Design principle: Privacy Embedded into Design. However, we hope to impress upon the Commission that the adoption of standards that enable better privacy protections will never be a panacea for privacy. Standards such as P3P are not meant to replace privacy legislation or regulation. Perhaps at some point, widespread and effective use of metadata tools, as one example, will justify a loosening of regulatory

---

[36] OMB has begun to require privacy procedures as part of the implementation of the Federal Information Security Management Act (FISMA). NIST, which already sets the security protocols and measurement for FISMA, has become more knowledgable about privacy and could expand FISMA implementation procedures to incorporate best practices for PIAs and more tenets of Privacy by Design.

[37] *See Geographic Location/Privacy (geopriv), available at* http://www.ietf.org/dyn/wg/charter/geopriv-charter.html.

[38] *See Geolocation API Specification, Editor's Draft* (Nov. 27, 2009) *available at* http://dev.w3.org/geo/api/spec-source.html.

[39] *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* [hereinafter "P3P Paper"].

requirements, but even after adoption is completely ubiquitous, we would need testing and data to prove that the technology was in fact effective. The development of Privacy Enhancing Technologies and the debates over regulation, in other words, should take place on largely separate tracks.

V. The National Broadband Plan should encourage a marketplace of privacy protective, user-centric decentralized identity providers

As broadband access and usage increases, new broadband applications will depend on the ability to manage and utilize identity online. The range of transactions and events that can be linked to individual identity continues to grow and Internet users' online identities are becoming increasingly intertwined with their offline identities – sometimes in unexpected or unknown ways. These developments have sparked a debate over how to balance the ideal of an anonymous Internet with the reality of an Internet on which we leave identifiable data trails and often are required to authenticate our online or offline identities. The quest for the right balance has become a central challenge of the digital age.

Identity management has been posed as one solution. Identity management encompasses all manner of systems that serve to identify individuals, prove identity, authenticate attributes, and control access to online systems and particular information. This field is developing quickly, and new solutions are being brought to the marketplace by many different parties. In cooperation with industry, academics, and public interest groups, CDT has developed a set of identity principles (see Appendix D) to address privacy concerns in identity management.

1. Centralized versus decentralized identity

Some have posited that consumers are best served by a centralized identity system, either through a card or centralized repository, that holds all data they generate online. Consumers would control the information in this repository and be able to sell it in exchange for broadband-enabled services. Internet users would also rely on this data vault to authenticate their identity for myriad purposes: filing taxes, booking airline tickets, and buying books. Some have even suggested that the government manage this repository of information.

The centralized repository raises many concerns. Developing a single database for all would create a massive and potentially vulnerable system of highly sensitive personal information on almost every American. There is not currently a legal or technical framework robust enough to ensure that the security and privacy of personal information stored in such a centralized, privatized, ID system is not abused by companies and government agencies. Such a centralized ID system could also be a "one stop shop" and treasure trove of valuable information for identity thieves, terrorists, and unscrupulous government employees.

A centralized repository or similar identity management system is not, however, the only alternative. Industry representatives, advocates, and government agencies have been working to develop a decentralized identity management system that can promote the penetration of broadband applications while protecting user privacy. Such a system would allow users to share information with trusted providers and would enable new,

innovative online applications. The key to creating trusted relationships online is creating meaningful privacy and security and enabling user control within the identity management system. CDT recommends that trust frameworks mediate the policies and practices of identity management providers. In order to create a healthy marketplace that allows consumer choice in identity management, the National Broadband Plan should acknowledge the privacy implications of identity management systems and recommend a set of principles for identity online.

CDT has published a list of identity principles that stress decentralization, diversity of services, proportionality of data collected, and the integration privacy and security by design.[40] Taken as a whole, these principles require a federated system of identity providers, each working with users and relying parties to ensure that privacy and security are respected and that all parties to the system are able to have their needs met.

New models for identity management separate the "identity service provider" from the "relying party" that needs some information about the user, allowing users to log in to thousands of websites using a single set of credentials. If carefully designed and implemented, such user centric, or federated, identity systems can give the user greater privacy protections and greater control over what information is provided in connection with any given transaction. They can also provide the relying party with greater assurance that the information provided is accurate, while lowering costs for systems that no longer have to implement their own identity management systems. A trust framework would connect the user, the identity provider, and the relying party, laying out a set of conditions that each party would be required to adhere to in order to maintain a trusted system.

Using only one or a very small handful of centralized identity solutions for multiple purposes leaves individuals with few choices and diminishes the ability of identity systems to protect privacy and security. Requiring individuals to use a single identifier or credential for multiple purposes creates a single target for privacy and security abuses by identity thieves, terrorists, government, business, and others.

Using a single identity for multiple purposes may, however, offer convenience and efficiency benefits. These benefits should be weighed against the risk of concentrating identity information in a single location or credential.

Rather than attempt to serve as a perfect single solution, enrollment and authentication options should function like keys on a key ring, with different identities for different purposes. They should allow individuals to choose the appropriate option to satisfy a specific need. On balance, it is not optimal to centralize identity information or use a single credential for a multitude of purposes. In cases where linking of identity systems and databases is deemed necessary, appropriate safeguards must be implemented to limit the associated privacy and security risks.

---

[40] *See* Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age, Draft for Comment* (December 2007) *available at* http://www.cdt.org/security/identity/20080108idprinciples.pdf.

2. Spectrum of credentialing

When individuals are asked to identify themselves, there are many ways to do so. For example, a user can identify him or herself as "anonymous," "someone with a specific fictitious name who has visited this site before," "someone who lives in California," or "the Jane Smith that was born in California 35 years ago and has a specific taxpayer identification number." These identity claims lie on a spectrum of identity credentialing ranging from lower to higher assurance and lower or higher risks to privacy and/or risks from data insecurity. An OMB memo in 2004 defined distinct "levels of assurance," making it clear that there is a spectrum of credentialing that is useful for government and commercial entities. Most importantly, it is clear that not every transaction requires the same amount or type of information.[41]

This spectrum of authentication credential options, ranging from anonymity to full identity, with pseudonymity as a key intermediate option, is important for both protection of privacy and security. In some case, only verification that the (unidentified) individual has specified attributes will be all that is needed by the relying party. Without the options provided by such a full spectrum of authentication solutions, it is likely that more information would be collected than is necessary and both privacy risks and data security risks would increase.

3. Creating trust frameworks

One way to establish responsible identity management systems is to create trust frameworks that outline the responsibilities and requirements for each player in an identity interaction and mediate the interactions in ways that ensure each party is fairly represented. CDT has published a whitepaper (Appendix E) that identifies important issues that must be resolved as these types of identity management programs are established.[42]

The development of trust frameworks for user centric identity provides a unique opportunity to design truly user-centric and privacy protective identity management regimes. Determining the obligations of each party interacting within the auspices of a trust framework will be the key aspect of creating such trust frameworks. Creating appropriate relationships between each of the parties in a user-centric federated identity system will in turn create stronger, more trusted relationships online.

Any such trust framework should:

- Impose and enforce some set of rules that increase trust in associated identification services, thereby enabling productive transactions between strangers;
- Allow flexible evolution of the relevant services and support an adequate

[41] *See* Office of Mgmt. & Budget, M-04-04, *Memorandum to the Heads of All Departments and Agencies: E-Authentication Guidance for Federal Agencies* (Dec. 16, 2003), *available at* http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.

[42] *See* Center for Democracy & Technology, *CDT Discusses Key Policies Issues Surrounding User Centric Identity Management* (November 6, 2009) *available at* http://www.cdt.org/policy/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management.

business model for participants;
- Be robust against fraud or manipulation, protect the privacy and security of user data, and provide appropriate avenues for dispute resolution, redress, and/or liability in the event of performance failure; and
- Be adequately open to new participants without eliminating minimum qualifications and rules.

The use of identity management by government and other online services will allow users to access services online that require personal or confidential information. It is important to ensure that the identity systems used by government will create trusted relationships online and allow users to control the information that is passed to the government. In addition, it is important to ensure that a centralized national database of identity information is not created and held by the government.

B. How do we ensure identity providers protect privacy?

While it is critical that government not discourage this nascent industry from growing by adopting overly intrusive regulations, identity providers must be covered under some type of private or public legal regime in order to ensure that they properly safeguard consumer privacy. CDT proposes two principal options for covering these entities. First, identity providers could required by a trust framework to offer a three-party contract that imposes restrictions on, and gives enforcement rights to, the identity provider, relying parties and users. Second, identity providers may already be covered under existing law, specifically the Fair Credit Reporting Act (FCRA). If both these options fail, however, there is a potential need for a new policy and/or law to govern these entities.

1. A contract regime

Developing a meaningful three-party contract between the user, identity provider and relying party could prove to be a particularly useful way to govern identity management systems and protect privacy. If properly implemented, the benefits of this approach include more direct enforcement (likely a mutually agreed upon dispute resolution process), greater flexibility, and less government regulation.

A user-centric identity transaction inherently involves three parties (with the exception of the case in which the user acts as its own identity provider) and all three parties have reasons to want to impose and enforce certain obligations on the other two parties. Thus, one way to address this need is to establish the terms and conditions of a three-party agreement that comes into effect as against all three parties when the user invokes the services of the identity provider, when the identity provider receives information from the user or submits information to a relying party in connection with such services, and when the relying party seeks and receives information from the identity provider or the user in connection with such a system.

In the past, rules for handling personally identifiable information provided to an online site would be established by the Terms of Service on the site. This type of notice regime has done little to ensure confidence or provide privacy to the user, especially in its relationship to an identity provider that controls data submitted to many other sites. What is needed, in effect, is a special purpose contract that applies across all three parties

and comes into effect, and becomes binding on the parties, when and insofar as they invoke the functionality of the identity service in question.

Such contractual terms and conditions can be spelled out in advance by the Trust Framework and imposed as a condition of using the trust framework's brand. It is key that the interests of each party should be represented as such contracts, conditions, and policies are developed. This approach could also give each of the three parties the ability to enforce the provisions of the agreement that are designed to protect their interests. These mandatory terms can incorporate requirements to use particular dispute resolution mechanisms in the even of a dispute, as well as appropriate limitations on liability and remedies in the event of a breach of the agreement.[43]

Of course, any identity provider could choose to unilaterally draft a set of terms and conditions that it asserts become applicable to users and relying parties that make use of its authentication services. But this could lead to the proliferation of many differing and even incompatible sets of terms and conditions – producing confusion in the marketplace and reducing the ability of the user centric identity system to induce trust. Moreover, the practical ability of enforcement of the agreement by any particular user or relying party would remain very much in doubt, as evidenced by the FTC cases that call into question terms buried in EULAs (see Appendix A).

The trust framework provider could and should, however, play a pivotal role in the process of developing terms and policies within the identity management system. The trust framework provider can impose a requirement, as a condition of participation in its branded network of identity providers, that all such providers offer and comply with three party contractual terms that meet some minimum set of requirements.

Under this approach, issues regarding the obligations to protect the privacy and security of personal information relating to the user, or obligations imposed on the user or relying party, would not be substantively covered as obligations running from the identity provider to the trust framework provider (and enforceable only by the trust framework provider, assuming it had the resources and capabilities and incentives to enforce). Rather, the contract between the trust framework provider and the identity provider would impose the condition that the identity provider enter into a specified minimum set of contractual obligations with both users and relying parties. That contract would give all three of these parties the right to enforce appropriate terms. The trust framework could withdraw certification of identity providers that repeatedly failed to honor their obligations, but enforcement would not be contingent on the institutional capabilities or inclinations of the centralized trust framework entity.

[43] CDT will be publishing a paper addressing this approach in more detail, especially what the specific terms and conditions of such a three party contract might be in order to ensure proper privacy protection and the particular role of the trust framework provider under this approach.

2. A FCRA regime

While it is far from clear, the FCRA may, in many instances, be read to cover identity providers, which would require them to comply with a pre-existing statutory regime and certain FIP principles that are already incorporated into the law.[44]

FCRA regulates consumer reporting agencies and the dissemination of information contained in consumer reports. The Act defines a "consumer report" as the communication of "any information" by a consumer reporting agency (CRA) that bears on a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" that is "used or expected to be used or collected in whole or in part" for the purpose of serving as a factor in establishing eligibility for credit, insurance, employment, or a range of other purposes defined in the statute.[45]

The "other purposes" authorized under the Act include disclosure when there is a legitimate business need in connection with a business transaction initiated by the consumer.[46] In its FCRA regulations, the FTC determined that "a party has a permissible purpose to obtain a consumer report on a consumer for use in connection with some action the consumer takes from which he or she might expect to receive a benefit that is not more specifically covered" as credit, insurance, or employment.[47]

The FTC regulations suggest a potentially broad understanding of what could constitute a permissible consumer purpose under the FCRA. For example, "a consumer report may be obtained on a consumer who applies to rent an apartment, offers to pay for goods with a check, applies for a checking account or similar service, seeks to be included in a computer dating service, or who has sought and received over-payments of government benefits that he has refused to return."[48] Significantly, these examples offer a detailed set of types of services that do not include credit, employment, or insurance. But all involve the use of a screening of background or reputation to deliver the service, which suggests identity providers could be covered under the FCRA as CRAs.

Depending on how identity providers develop, and what uses their services are put to, these entities may indeed be doing specialized types of background checks for online

---

[44] This is still very much an open question. There are also reasons to believe identity providers may not be covered under the FCRA, see, e.g., Ippolito v. WNS, Inc., 864 F.2d 440 (7th Cir. 1988) (reading the coverage of the FCRA relatively narrowly). In addition, when a consumer has provided all of the information directly to an entity that otherwise may be covered under the FCRA, it should not be considered a "consumer reporting agency." 15 U.S.C. § 1681a(d)(2) ("the term 'consumer report' does not include . . . any report containing information solely as to transactions or experiences between the consumer and the person making the report"). This is, of course, an important exception. A CDT paper analyzing coverage of identity providers under the FCRA in greater detail will be forthcoming.

[45] 15 U.S.C. § 1681a(d).

[46] 15 U.S.C. § 1681b(a)(F)(i).

[47] 16 C.F.R. Pt. 600, App. (Comment to Section 604(3)(E)). When the FCRA was amended in 1996 this section moved to Section 604(3)(E), but the general applicability of the FTC's commentary has not changed and it continues to be relied upon by the courts. *See, e.g.*, Wallace v. Finkel, No. 2:06CV05-SRW (WO), 2006 U.S. Dist. LEXIS 42271 (M.D. Ala. June 22, 2006).

[48] 16 C.F.R. Pt. 600, App. (Comment to Section 604(3)(E)).

consumers or government services that Congress had envisioned regulating when enacting the FCRA.

This uncertainty for identity providers leaves many open questions. Data brokers have often developed innovative means to avoid falling under the FCRA definitions when utilizing databases for identity verification purposes,[49] yet these companies have very little direct interaction with the public and therefore the amount of trust the general public has in them matters little to their success. It does not seem to be in the interest of a nascent industry that will have to interact directly with the public to push the limits of the law in the same way that data brokers have in the past.

User-centric identity providers have another option: they can develop practices through their trust frameworks that comply with the FCRA. Providers that offer services with consumers as the primary audience, or at least on equal footing to relying parties, will have little problem conforming to the FIPs laid out in the statute, which emphasize consumer notice, consent, access, correction, timeliness, and secondary use limitations. On the other hand, providers that place the consumers as a secondary audience behind the interests of the relying parties will have more difficulty complying with the statute.

There is no need to risk the threat of greater regulation when it is in providers' interest to utilize trust mechanisms that offer users the necessary control from the beginning, specifically when those mechanisms can be judged in compliance with current law.

3. Potential need for a new law

If neither a contract regime nor FCRA regime is able to provide consumers with adequate privacy protection here, Congress may need to address identity providers and related privacy concerns in a new law. New legislation governing this space should reinforce the FIP principles and possibly be part of a comprehensive consumer privacy law. The FCC should encourage Congress to look to the FCRA requirements as, at least, a good starting point for what would need to be covered in such a law.

For example, under the FCRA, CRAs must comply with requirements regarding (1) File Disclosure, (2) Access and Correction, (3) Timeliness, (4) Use Limitation, (5) Disclosures to Users, and (6) Disclosures to Data Furnishers. In addition, users of CRA data have a number of FIPs-related obligations, such as (1) Use Limitation, (2) Certification of Purpose, (3) Notification of Adverse Action, (4) Notification of an Address Discrepancy, (5) Proper Disposal of Records. There is also a range of other obligations for creditors, employers, investigative consumer report resellers and medical records.

Liability under the FCRA includes state or federal civil enforcement actions, as well as a private right of action.[50] Moreover, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution.[51]

---

[49] *See Exploring the Offline and Online Collection and Use of Consumer Information: Hearings Before the Subcomms. on Commerce, Trade and Consumer Protection and Communications, Technology and the Internet of the House Comm. on Energy and Commerce*, 111th Cong. (Nov. 19, 2009) (statement of Pam Dixon, Executive Director, World Privacy Forum), *available at* http://www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf.

[50] 15 U.S.C. §§ 1681n, 1681o, 1681s.

Ensuring proper protection for consumer privacy in the emerging identity provider industry would require similar FIPs-like obligations.

The National Broadband Plan should call on industry to move in the direction of building contractual frameworks to address privacy concerns in identity services and should stress that if these services cannot adequately protect privacy we must ensure that FCRA-like protections are granted for identity services where FCRA does not already apply.

VI. The National Broadband Plan should encourage innovation and consumer protection in third-party applications

The past two years have seen the introduction and rapid adoption of a new model for broadband-enabled services: companies are increasingly opening their platforms to the public, allowing every-man innovators, advertisers, and even competitor companies to contribute applications that enhance the original platform in previously unimaginable ways.

In inviting unknown third parties to develop extensions to their carefully developed platforms and well-honed brands, these platform providers have taken on an ambitious task: promoting a vibrant, open marketplace while striving to maintain a secure online environment and retaining consumer confidence in that environment. Efforts toward these desirable, but at times seemingly contradictory, goals have met with varying levels of success.

Companies that are considering opening their platforms must all confront a set of key questions: how involved will they be in vetting applications designed by third parties for their platforms? What types of guarantees – if any – do they want to make to consumers about the security of applications offered in their application "stores"? How can they protect users from applications that enable fraud, identity theft, privacy violations, and security breaches and thereby protect their brand? By making guarantees about these third party applications, are they opening themselves up to liability if seemingly innocent applications are in fact nefarious?

Some of the answers to these questions can be found in Section 230 of the Telecommunications Act of 1996. Since its inception, Section 230 has fostered the development of innovative Internet content, applications, and services, while at the same time removing disincentives for platform providers to voluntarily vet and filter material provided by third parties. The protections of Section 230 apply no less to open platforms.

In enacting Section 230, Congress articulated and pursued three legislative goals, two of which are directly relevant to the questions posed in the Notice.[52] First, Congress sought to foster, promote, and protect the continued rapid development of Internet content and services, "unfettered by Federal or State regulation."[53] Second, Congress sought to

---

[51] 15 U.S.C. § 1681q.

[52] For more on the goals underpinning Section 230, *see* Brief Amici Curiae of The Anti-Spyware Coalition et. al., *Zango, Inc. v. Kaspersky Lab, Inc.*, 2009 WL 1796746 (9th Cir. June 25, 2009).

[53] 47 USC § 230(b)(2).

remove barriers to voluntary "Good Samaritan" efforts by interactive computer services.[54] Taken together, these goals suggest precisely the "middle ground" between ensuring innovation and protecting consumers alluded to in the Notice.

Section 230(c)(1) fosters continued innovation by ensuring that Web sites and service providers can allow third parties to provide content without the fear of a constant stream of lawsuits trying to hold the service provider liable for content posted by others. Without the protections afforded by Section 230(c)(1), some of the most dynamic and popular video sharing, social network, blogging, and other user-generated content sites on the Internet could not flourish – and may not have even been created.

Whereas 230(c)(1) encourages unfettered innovation by enabling providers to allow third-party content with less risk, Section 230(c)(2) encourages *responsible* innovation by removing risk-based disincentives to self-regulate by filtering and vetting third-party content. Under this section, actions taken in good faith to filter content or protect users will not be a trigger for liability. By these provisions (and a third protecting creators and providers of user-empowering filtering tools), Congress created an environment where both rapid innovation and robust self-regulation co-exist.

Just as these provisions protect providers of platforms for third-party videos, so they protect providers of platforms for third-party broadband applications. Such platforms qualify for protection under Section 230's definition of "interactive computer service,"[55] And third-party application developers certainly qualify as "information content providers" under the law.[56] Indeed, courts have interpreted these terms broadly in applying Section 230's limitations on liability.[57] In other words, Section 230 creates an environment in which platform operators can vet third party applications for privacy and security risks without fear that any action taken to filter a platform's offerings would give rise to liability – either to an aggrieved application developer or to users for a rogue application that avoids the filter.

In light of the protections that platform providers are granted by Section 230, there is little reason for these companies not to adopt procedures for ensuring the security of the applications offered in their "app stores." Indeed, there already exists a spectrum of models that application providers can look to as they contemplate initiating vetting processes. Apple, for example, famously reviews submitted applications "in order to protect consumer privacy, safeguard children from inappropriate content, and avoid

---

[54] 47 USC § 230(b)(4).

[55] 47 USC § 230(f)(2).

[56] 47 USC § 230(f)(3).

[57] *See, e.g. Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003*) ("a service provider or user is immune from liability under § 230(c)(1) when a third person or entity that created or developed the information in question furnished it to the provider or user under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other 'interactive computer service."); *see also Zango, Inc. v. Kaspersky Lab, Inc.*, 2009 WL 1796746 (9th Cir. June 25, 2009) (holding that a software developer is protected by § 230 with respect claims by another software developer whose software was filtered by the former developer's anti-malware program).

applications that degrade the core experience of the iPhone."[58] Facebook does not require a review process before applications can be offered on its platform – it instead offers the "Facebook Verified App" badge to a subset of applications that "have passed a detailed Facebook review to confirm that the user experience they provide complies with Facebook policies."[59]

We call on the FCC to use the National Broadband Plan to encourage industry development of best practices for vetting processes. These best practices should be founded on a full set of FIPS with a special emphasis on the security and transparency principles. The need for special security checks should be clear; special attention should be paid to transparency to ensure that the vetting process does not stand in the way of innovation. Application providers must be clear about the criteria for successful applications and be transparent about their reasons for rejecting specific applications. We believe that by engaging in open and robust vetting processes, platform providers will earn users' trust and thereby promote, rather than infringe on, the ability of third-party applications to prosper.

Vetting processes, while important for exposing security holes and inappropriate collection of user data, are not a silver bullet. No process is going to be able to control how data is used after the point of collection or to ensure the quality and integrity of data that is collected. Companies that offer applications still must be held accountable to consumers, trade associations of which they are members, and the FTC for their data collection and use practices. Additionally, platform providers should be sharing information about companies that are in clear violation of basic privacy or security standards. The Broadband Plan should also encourage companies to engage law enforcement to pursue application makers that are committing fraud or identity theft, violating user privacy, or otherwise engaging in security breaches.

As platforms develop, greater involvement from government entities may be necessary. Continued monitoring and review of platforms and application makers will be an important means to measure consumer protection standards.

---

[58] *See Apple Answers the FCC's Questions* (July 31, 2009), *available at* http://www.apple.com/hotnews/apple-answers-fcc-questions/.

[59] *See What Are Verified Applications,* Facebook Help (Accessed January 22, 2010), *available at http://www.facebook.com/help/?page=876#/help/?faq=14858*.

* * *

This proceeding presents an opportunity to ensure that the dynamic growth and innovation seen on the Internet over the past 15 years can continue and that a framework of trust can be fortified as part of a thriving Internet. CDT looks forward to working with the Commission to refine the National Broadband Plan.

Respectfully submitted,

Leslie Harris

Ari Schwartz

Alissa Cooper

Erica Newland

Heather West

Andrew McDiarmid

Jonathan Dunn

Center for Democracy & Technology

1634 I Street, N.W., Suite 1100

Washington, DC 20006

(202) 637-9800'

January 22, 2010