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

Statement of **Justin Brookman**
Director, Consumer Privacy
Center for Democracy & Technology

Before the Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on
"Balancing Privacy and Innovation: Does the President's Proposal Tip the Scales?"

March 29, 2012

Chairman Bono Mack, Ranking Member Butterfield, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Chairman's continuing leadership in exploring privacy issues and potential solutions.

CDT is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. We believe that privacy and innovation — when properly balanced — are mutually beneficial. We view the Administration's proposal for transparent, multistakeholder collaborations to translate the Fair Information Practices (FIPPs) into voluntary, enforceable codes of conduct as a modest but important step forward toward protecting user rights and building the consumer trust necessary to encourage continued innovation. Ultimately, however, we agree with the Administration and the Federal Trade Commission that flexible, comprehensive legislation will be necessary to fully achieve these goals.

My testimony begins with a brief overview of the privacy threats faced by modern consumers, analyzes the relationship between privacy and innovation, and finally discusses the Administration's proposal and the need for a privacy framework to support the rapid innovation propelling our economy forward today.

1. Privacy in the information age

Privacy is an essential building block of trust in the digital age. However, in recent years, technological developments and market forces have created fundamental challenges to our assumptions about privacy. Massive increases in data storage and processing power have enabled diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online — and offline — activities. While these new services and applications are often of great value to consumers, they also present new risks to consumer privacy. Americans turn to search engines to answer sensitive questions about their health. They use smart phone applications to pinpoint their location and obtain directions to a lawyer's or therapist's office. They shop, leaving digital traces of the book stores they browse, credit card numbers, and home and email addresses with "salesclerks" they never meet.

Loss of Control

A crucial first step to protecting privacy is empowering consumers to make meaningful decisions for themselves. Meaningful decisions presuppose both that choices are available and that consumers understand enough about the services they use (and, even more obscurely, the online data trade these services participate in).

It is well-established that consumers today simply aren't provided with enough insight to make informed choices, even when such choices are available. For example, a 2009 study conducted by researchers at UC Berkeley and the University of Pennsylvania's Annenberg School of Communication found that sixty-two percent of respondents incorrectly believe 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."[1]

Given the considerable length and complexity of most privacy policies, it is no surprise that consumers do not understand their purpose. Researchers at Carnegie-Mellon University have shown that for a consumer to reach a basic understanding of how his or her information is being collected and used, he or she would have to spend between 181 and 304 hours each year reading Web site privacy policies. Nationally, this sums to between 39.9 and 67.1 billion hours per year spent reading privacy policies, for an estimated annual national economic cost of between 559 billion and 1.1 trillion dollars. [2]

This state of affairs is made worse still by the fact that the few controls we do have are often overcome. Over the past few years, we've seen "flash cookies" override choices made by users who choice to disable cookies to avoid tracking.[3] More recently, we read about Google's inadvertent tracking of users on Apple's Safari browser, despite privacy features in the browser that should be trusted to prevent such tracking.[4] Mobile applications routinely take more

---

[1] Turow, et. al, *Americans Reject Tailored Advertising and Three Activities that Enable It*, September 29, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[2] Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[3] *See, e.g.,* Ayenson, et. al., *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning*, July 29, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390.

[4] Julia Angwin and Jennifer Valentino-Devries, *Google's iPhone Tracking, The Wall Street Journal*, February 17, 2012, http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

consumer data than they need,[5] including in many cases entire address books.[6] And major services have violated their own privacy policies, leaving users unsure of what to expect.[7]

This lack of meaningful understanding and choice is just the threshold problem. A lack of privacy assurances creates an array of undesirable results, from palpable physical and financial losses (in the cases of stalking[8] and identity theft[9]), to global distrust of American products and services.[10]

Why Privacy Matters

As the President wrote in his forward to the Department of Commerce's privacy report:

> *Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails . . . . Citizens who feel protected from misuse of their personal information feel free to engage in commerce, to participate in the political process, or to seek needed health care.*[11]

The enjoyment of privacy enables the exercise of our right to liberty. The FTC recently endorsed the idea that privacy harms extend beyond literal physical and financial harms.[12]

---

[5] Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

[6] Cesar Torres, *Path addresses privacy controversy, but social apps remain a risk to users*, ARSTECHNICA, February 12, 2012, http://arstechnica.com/gadgets/news/2012/02/path-addresses-privacy-controversy-but-social-apps-remain-a-risk-to-users.ars.

[7] *See, e.g., In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.; *In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order) *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf.

[8] *See, e.g.,* Kate Ashford, *Online Privacy Predators*, Women's Health, December 20, 2010, http://www.womenshealthmag.com/life/cyber-crime.

[9] Identity theft and other scams cost Americans $1.52 billion last year. Ian Simpson, *ID theft, fraud cost Americans $1.52B last year*, MSNBC, February 28, 2012, http://www.msnbc.msn.com/id/46562746/ns/business-consumer_news/t/id-theft-fraud-cost-americans-b-last-year/.

[10] *See, e.g.,* Jennifer Baker, *European distrust of US data security creates market for local cloud service*, COMPUTERWORLD, December 2, 2011, http://www.computerworld.com/s/article/9222361/European_distrust_of_US_data_security_creates_market_for_local_cloud_service.

[11] *See generally Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, February, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (letter from President Obama).

[12] The recent *News of the World* hacking incident provides a useful case study about why an expansive definition of "harm" is necessary to evaluate privacy concerns. In this example, reporters from a British tabloid used readily-available technological means to obtain the private voicemails of dozens of high-profile celebrities. The tidbits gleaned from these voicemails became the basis for many of the paper's subsequent stories. Although the individuals whose privacy was breached cannot say they were "harmed" in a physical or economic sense, an ordinary person would certainly deem this unexpected access of their private communications to be improper, unwarranted, not consented to, and, hopefully, illegal. *See* Julia Day, August 6, 2006, *Phone Tap Investigation Widens*, http://www.guardian.co.uk/media/2006/aug/09/royalsandthemedia.themonarchy

These include "the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties."[13] The FTC's recent actions against Google Buzz and Facebook exemplify rectification of these harms.[14] These harms should resonate on both a personal and business level: unexpected uses of data damage our trust and impinge upon our desire to engage with innovation.

Increasingly, we live in a world where *everything we do is observable*. Pervasive closed-circuit television and drone surveillance, and the emergence of facial recognition, may soon allow companies to persistently track users across space and over time by their individual identities.[15] Indeed, even the privacy that we expect inside our house is threatened by technological developments. Researchers at the University of Washington have uncovered ways to determine what television shows are being watched inside a home by measuring the electromagnetic radiation emitted from the power lines publicly observable outside your house.[16]

There is an incredible amount that we as a society have to gain from innovative new technologies, but there is also an incredible amount that we have to lose. Without a framework in place to assure everyday consumers of the ability to limit the collection and retention of the minutiae of their lives by unknown third parties, any sense of a realm of personal privacy may completely evaporate. In short, we may lose:

- Our right to read newspapers unnoticed: to throw a quarter into the vending box and grab a copy, to privately choose which articles we read and which we don't, gradually slips away each time a local paper shutters its presses or halts print distribution.

- Our right not just go for a drive unnoticed, but to talk to friends unnoticed, to write letters unnoticed,[17] to read books unnoticed, to watch a TV show unnoticed, to buy a gift unnoticed — all of these rights are eroding as these activities move into the networked world and surveillance technologies become more sophisticated.

- Our right to walk down the street unnoticed, whether en route to a political rally or to a doctor's office, is eroding as facial recognition technology advances and becomes more widely deployed.[18]

---

[13] *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, 8.

[14] *Id.*

[15] *See* Harley Geiger, *The Drones are Coming*, CDT Blog, December 21, 2011, https://www.cdt.org/blogs/harley-geiger/2112drones-are-coming; Harley Geiger, *Facial Recognition and Privacy*, CDT Blog, December 6, 2011, https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/.

[16] Miro Enev, *et al*, Televisions, Video Privacy, and Powerline Electromagnetic Interference, *Working Paper*, http://abstract.cs.washington.edu/~miro/docs/ccs2011.pdf.

[17] USPS mail currently receives more privacy protections than does electronic mail. *See*, *Federal Statutes and Regulations Relation to the Privacy and Security of Mail*, http://about.usps.com/who-we-are/privacy-policy/intelligent-mail-privacy.htm#H7.

[18] *See* Harley Geiger, *Facial Recognition and Privacy*, CDT Blog, December 6, 2011, https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy/.

But to "opt out" of the data collection, correlation, and/or use that takes place when we go about the activities described above would be analogous to "opting out" of electricity a mere thirty years ago. To disconnect from the services that collect such personal, sensitive data would be to disconnect from society. Cutting off all data collection is not viable, but finding a middle-ground compromise that forestalls persistent monitoring is absolutely necessary to ensure consumer trust in the digital ecosystem.

Crucially, neither the loss of privacy nor the assumption of these harms is an inevitable cost of technological innovation. Instead, both have been the natural outgrowth of a policy framework that has turned a blind eye to the foundational benefits that privacy offers us as citizens of a democracy and as consumers in a strong capitalist society. Smartphones, for example, would be no less magical if applications did not have such pervasive access to all of our phone's files and functionality. In some instances, consumers could lose functionality if they were unwilling to share some personal data with services, but increasingly, many consumers would prefer a more privacy-protective, and less personalized, user experience.[19]

Certainly, many companies that access user data in unexpected ways do not intend to publicize or even share the data with others. However, that fact alone does not nullify a consumer's reasonable privacy concerns. Even when data is collected merely for limited purposes, consumers could reasonably worry that their data could later be used for new, unexpected and unwanted purposes,[20] accessed by a rogue employee,[21] breached by hackers,[22] unwittingly exposed to the world,[23] or accessed by the government without robust legal process.[24] And the knowledge that their behavior is being monitored and retained (and potentially shared, accessed, or lost) can have a very real chilling effect on free expression, as well as the adoption of new technologies and services.[25]

2. Trust and innovation are inseparable ideals

Technology and market forces have unleashed a wave of innovation rolling at a pace we have never seen. Today, consumers regularly turn to the Internet to build their social networks,[26]

---

[19] John C. Dvorak, *Pew Finds Searchers Attitudes Toward Privacy Are Changing*, March 16, 2012, PCMAG, http://www.pcmag.com/article2/0,2817,2401717,00.asp (finding "73% of search users supported a statement that they would not be okay with a search engine keeping track of their searches and using that information to personalize future search results because they feel it is an invasion of privacy").

[20] *New York Accuses Gratis Internet of Largest Deliberate Privacy Breach Ever*, March 24, 2006, CONSUMERAFFAIRS, http://www.consumeraffairs.com/news04/2006/03/ny_gratis.html.

[21] Adrian Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats*, September 14, 2010, GAWKER, http://gawker.com/5637234/.

[22] Liana B. Baker and Jim Finkle, *Sony PlayStation suffers massive breach*, April 26, 2011, REUTERS, http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[23] Declan McCullagh, *AOL's disturbing glimpse into users' lives*, August 7, 2006, CNET, http://news.cnet.com/2100-1030_3-6103098.html.

[24] David Kravets, *Yahoo, Feds Battle Over E-Mail Privacy*, April 14, 2010, WIRED, http://www.wired.com/threatlevel/2010/04/emailprivacy/.

[25] Emmett Higdon, *Privacy Concerns Threaten Emerging Interest in Banking on Social Sites*, Emmett Higdon's Blog, May 21, 2010, http://blogs.forrester.com/emmett_higdon/10-05-21-privacy_concerns_threaten_emerging_interest_banking_social_sites.

[26] For example, Facebook reported 845 million monthly active users as of December, 2011. Facebook Newsroom, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (*last visited* March 27, 2012).

keep in touch with loved ones,[27] engage in commerce,[28] and join political movements.[29] American companies play a leading role in this innovation, benefitting the economy and creating jobs,[30] and enriching our lives. This is innovation we should all embrace and encourage.

And the pace of this innovation is still accelerating. Exponential growth in data, computing power, and powerful analytic techniques are opening new markets and creating possibilities every day.[31]

While few consumers fully grasp the extent of this large and growing data trade, numerous independent studies show that practices such as deep packet inspection, online behavioral advertising, and the merger of online and offline consumer data into profiles undermine consumer trust, the fundamental building block of Internet use.[32] Privacy worries continue to inhibit some consumers from engaging in online shopping and banking, [33] and are a top reason consumers decline to adopt location-based services.[34] A poll conducted by Zogby International

---

[27] And find new ones: online dating has recently surged in popularity. *See, e.g.,* Abby Ellin, *The Recession. Isn't It Romantic?*, THE NEW YORK TIMES, February 11, 2009, http://www.nytimes.com/2009/02/12/fashion/12dating.html.

[28] Online retail sales in the United States total $145 billion annually. U.S. Census Bureau, *E-Stats*, May 26, 2011, http://www.census.gov/econ/estats/2009/2009reportfinal.pdf, at 1.

[29] Online political engagement is growing but stratified by income and education. *The Demographics of Online and Offline Political Participation*, Pew Internet, Sept. 1, 2009, www.pewinternet.org/Reports/2009/15--The-Internet-and-Civic-Engagement/3--The-Demographics-of-Online-and-Offline-Political-Participation/2--Online-Politics.aspx.

[30] *See, e.g.,* John Moore, *IT jobs thriving despite lackluster economy*, ABC NEWS, August 16, 2011, http://abcnews.go.com/Technology/jobs-thriving-lackluster-economy/story?id=14311664; John Furrier, *Big Data is Creating The Future — It's A $50 Billion Market*, FORBES, February 29, 2012, www.forbes.com/sites/siliconangle/2012/02/29/big-data-is-creating-the-future-its-a-50-billion-market/.

[31] For example, Apple reported that over 15 billion apps have been downloaded from its app store as of July 2011. Apple Press Release, *Apple's App Store Downloads Top 15 Billion*, July 7, 2011, http://www.apple.com/pr/library/2011/07/07Apples-App-Store-Downloads-Top-15-Billion.html

[32] *See e.g.,* Scott Cleland, Americans Want Online Privacy – Per New Zogby Poll, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll; Joseph Turow, 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), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. See also Alan F. Westin, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced, HARRISINTERACTIVE, April 10, 2008, http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-withWebsites-Customizing-C-2008-04.pdf (in which 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, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, 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).

[33] *See* John B. Horrigan, Online Shopping, PEW INTERNET & AMERICAN LIFE PROJECT, February 13, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf; Emmett Higdon, *Privacy Concerns Threaten Emerging Interest in Banking on Social Sites*, Emmett Higdon's Blog, May 21, 2010, http://blogs.forrester.com/emmett_higdon/10-05-21-privacy_concerns_threaten_emerging_interest_banking_social_sites..

[34] *See* Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, & Norman Sedeh, Location-Sharing Technologies: Privacy Risks and Controls, CYLAB USABLE PRIVACY & SECURITY LABORATORY 18 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

in June 2010 found that 88% of Americans are concerned about the security and privacy of their personal information on the internet.

This trust is the difference between innovation that delights us and innovation that deeply discomforts us. In short, trust underpins and fuels this innovation. If consumers are unable to trust this increasingly complex network of innovative services, innovation suffers.

Privacy is about securing user rights. But it is also about building trust in the marketplace in hopes of protecting and accelerating the innovation we see today. In short, innovation and privacy are not incompatible paths, but intertwined paths.

Increasingly, for many companies, the growth of cloud computing is bringing new urgency to the call for comprehensive privacy legislation.[35] As American companies continue to innovate and expand their markets overseas, they are finding that America's weak privacy framework is bad for business. Without adequate privacy protections in place, individuals, companies, and governments in other countries do not feel comfortable — or in many cases are legally restricted from — taking advantage of U.S.-based cloud computing services. With our advanced technology and infrastructure, U.S. companies and the U.S. economy are poised to lead adoption of this hugely important new generation of cloud-based services.[36] However, the lack of a comprehensive privacy protection framework puts U.S.-based companies at a disadvantage to other providers.

3. The Administration's framework supports privacy and innovation

The proposal contained within the Administration's "Consumer Privacy Bill of Rights" is a modest step toward protecting consumer's expectation of privacy rights and building trust to support innovation. To understand why, it's important to situate the Administration's Proposal in a broader context and compare it to other self-regulatory and legislative efforts.

Modern privacy advocacy has centered squarely around the "Fair Information Practices,"[37] or FIPPs. These high-level principles are the fundamental building blocks of any modern privacy

---

[35] Sara Jerome, *Intel, Microsoft, eBay support Rush's privacy bill, while noting concerns*, Hillicon Valley Blog, October 7, 2010, http://thehill.com/blogs/hillicon-valley/technology/123197-intel-microsoft-ebay-support-rushs-privacy-bill-while-noting-concerns-.

[36] Article 25 of the EU Data Protection Directive states that the personal information of EU citizens may not be transmitted to nations outside of the EU unless those countries are deemed to have "adequate" data protection laws. The Article 29 Working Party does not consider U.S. law "adequate" (in part because the U.S. has no comprehensive data protection law), and thus in general personal information about EU data subjects may not be transferred to the U.S. for storage or other processing. While there are several compliance mechanisms, such as the U.S.-EU "Safe Harbor" agreement, that allow U.S. companies to process personal information from the EU, each comes with its own compliance challenges. For an in-depth discussion of these compliance challenges, see Comments of the Center for Democracy and Technology on Information Privacy and Innovation in the Internet Economy, CDT (2010), http://www.cdt.org/files/pdfs/20100613_doc_privacy_noi.pdf.

[37] FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. A recent government formulation of the FIPPs offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy frameworks. These principles, as described by the Department of Homeland Security in 2008, include:

framework. They are found in the Administration's Consumer Bill of Rights,[38] strongly echoed in the FTC's Final Report on consumer privacy,[39] and have a long history throughout other federal privacy laws. The FIPPs include concepts like "transparency," control," and "purpose specification" — together, these concepts provide a roadmap for empowering individuals to both understand and impact how their data is collected and used. In simpler terms, FIPPs aim to offer consumers a sense of control, insights into the tradeoffs they're making with their data, and assurances of security. By nature and design, FIPPs are flexible and open to interpretation.

Theoretically, there are a number of ways we could translate the high-level principles contained in the FIPPs into actionable policy across a range of diverse technologies and industry business models:

> • **Transparency**. Entities should be transparent and provide to the individual regarding their collection, use, dissemination, and maintenance of information.
>
> • **Purpose Specification**. Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.
>
> • **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 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.
>
> • **Data Quality and Integrity**. Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.
>
> • **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.
>
> • **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.

U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. The Administration's Consumer Bill of Rights is based on a slightly reworded, but fundamentally comparable set of FIPPs. *See generally Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, The White House, February, 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[38] *See id.*

[39] *See generally Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

- prescriptive, industry-specific legislation;
- flexible, principles-based legislation with detailed FTC rulemaking;
- flexible legislation with targeted FTC enforcement;
- flexible legislation with safe harbors for FTC-approved voluntary codes of conduct;
- self-regulation

As the FTC made clear in its Final Report on privacy earlier this week, and as documented above, we've already witnessed a general failure of self regulation to adequately inform consumers or give them control over their personal information.[40] On the other hand, a highly inflexible, prescriptive piece of legislation could lose relevance as technology develops and could deter innovation. CDT suggests that both of these solutions come at an unacceptable cost to either trust or innovation. The solution falls somewhere in between.

CDT has long supported a carefully-crafted framework that gives industry segments flexibility to develop tailored privacy solutions that benefit consumers. We believe that these codes would be best developed through multistakeholder discussions with civil society advocates and regulators, but in any event, the voluntary codes must be formally endorsed by the Federal Trade Commission to ensure they are sufficiently robust and to garner consumer confidence in them. We believe this is the best way to create certainty for companies, encourage privacy innovation over time, and reward the adoption of accountable practices. Traditionally, this support has come in the context of advocating for flexible baseline consumer privacy legislation that also protects innovation.[41] We continue to believe this is the best path forward. However, the Administration's interim process of voluntary convenings provides a path to make substantial progress on privacy through enforceable voluntary codes on emerging privacy problems as new technologies develop (on the spectrum above, the Administration's interim measure would fall somewhere between the fourth and fifth options).

The voluntary, multistakeholder approach offers an open, transparent forum for good faith negotiations among industry, advocates, and regulators. The codes will not be written in stone and will be open to innovation over time. The FTC is prepared to enforce the promises made in the negotiated codes, offering important assurance to consumers and certainty for those companies that step up to the negotiating table.[42] Our greatest concern is that absent a law to incentivize companies to negotiate interpreting rules for the treatment of personal data, not all companies will be interested in negotiating these codes, and others may eventually walk away and fail to adopt the codes, with limited consequences.[43]

CDT agrees with both the Administration and the FTC that a baseline privacy law will ultimately be needed, and we call on this Subcommittee to move forward toward that goal. But we cannot

---

[40] *Id.*

[41] *See, e.g.,* Statement of Leslie Harris Before the House Committee on Energy and Commerce*, The Best Practices Act of 2010 and Other Federal Privacy Legislation*, July 22, 2010, http://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf.

[42] Justin Brookman, *Two Step Forward for Privacy*, CDT Blog, February 24, 2012, https://www.cdt.org/blogs/justin-brookman/2402two-steps-forward-privacy.

[43] *Id.*

wait to make progress; and we believe that in certain industries, the incentives may well be already aligned to develop strong, industry-wide codes of conduct, offering progress on privacy now and a model that should inform the shape of privacy legislation in the future.

4. Conclusion

CDT would like to thank the Subcommittee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring encouraging the development of privacy frameworks that foster innovation. CDT looks forward to working with the Members of the Subcommittee as they pursue these issues further.

For more information, contact Justin Brookman, justin@cdt.org, (202)637-9800.