Testimony of Cameron F. Kerry

General Counsel

U.S. Department of Commerce

Hearing on "The Need for Privacy Protections:

Perspectives from the Administration and the Federal Trade Commission"

Committee on Commerce, Science, and Transportation

United States Senate

May 9, 2012

2:30 p.m.

Summary

Commercial privacy protections have not kept pace with the explosive growth of the Internet. Consumers are deeply concerned about their privacy, but are unable to determine which companies respect their privacy and how their personal data are being collected, stored, and used. Similarly, American businesses need to determine and meet the privacy expectations of their customers in order to maintain their customers' trust, but still wish to innovate within these bounds. Consumers and American businesses share a strong interest in defining and protecting privacy interests to protect consumers, provide a level playing field for businesses, and build an environment of trust that benefits innovation and the digital economy.

To this end, the Administration's Privacy Blueprint articulates a Consumer Privacy Bill of Rights – and calls on Congress to give this baseline privacy protection the force of law. The seven basic principles of the Privacy Blueprint (based on globally recognized Fair Information Practices) are (1) individual control, (2) transparency, (3) respect for context, (4) security, (5) access and accuracy, (6) focused collection, and (7) accountability. The Administration supports giving the Federal Trade Commission (FTC) the authority to enforce the principles of the Privacy Bill of Rights, as codified. The FTC also should have the authority to provide safe harbors for companies that adopt context-specific codes of conduct that set forth how they will follow the Privacy Bill of Rights. Such codes of conduct should be developed through multistakeholder processes that include broad participation from all interested parties, including consumer groups and businesses.

The Administration supports legislation that provides strong baseline privacy protections in a manner that promotes growth and innovation in the digital economy. Such legislation would allow businesses to implement privacy protections in ways that are specific and appropriate for their industries. It would avoid being too prescriptive or tailored to specific technologies, potentially stifling innovation and inhibiting the development of new products or services, or being so inflexible that it fails to cover the next generation of changes. Nor should legislation impose unnecessary burdens on our businesses. These considerations will help the United States strengthen consumer privacy protections while promoting continued innovation.

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee Members, thank you for the opportunity to testify on behalf of the Department of Commerce about the Administration's recently-released policy blueprint, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the Privacy Blueprint, attached). I welcome this opportunity to discuss ways to enhance consumer privacy that will foster economic growth, job creation, and exports for American businesses.

As President Obama said in the Privacy Blueprint "[n]ever has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones." The need for privacy protections has grown in proportion to the expansion of the Internet itself. Every day, an increasing share of our commercial transactions, our social interactions, and our participation in public discussion depends on the Internet as a medium. The way we create and share our communications increasingly relies on new technologies that are networked – and increasingly raises new questions about how data associated with these communications are collected, stored, and used. Ultimately, sustaining the social and economic benefits of networked technologies depends on consumer trust. People must have confidence that companies will handle information about them fairly and responsibly.

Privacy protections have not kept up with this explosion of Internet use and new technology. Due to inadequate protection of data, millions of Americans have their personal information exposed in data breaches every year. These breaches lead to concrete harm for consumers: for 12 consecutive years, identity theft has topped consumer complaints received by the FTC, accounting for 15% of all complaints. [1]

Consumers also lack transparency into how companies collect and use data. Not only is it a cliché to say nobody reads privacy policies, but studies have indicated that the effort would be hopeless, because an average user would have to devote 250 hours a year just to read the labyrinthine privacy policies of the websites they visit in a year.[2] Even if those policies all provided a clear roadmap to companies' use of data, that is too much to ask; it is as much as

---

[1] FTC Releases Top Complaint Categories for 2011: Identity Theft Once Again Tops the List, Feb. 28, 2012, *available at* http://ftc.gov/opa/2012/02/2011complaints.shtm.

[2] Aleecia M. 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://www.is-journal.org/.

45 minutes of dense textual reading for each and every site visited in a day, a full one-eighth of a working year, *every year*, just to *read* the privacy policies. All the promise of the Internet, and the benefits and efficiencies it can provide, would be dragged down by the anchor of privacy policies if we had to slog through all that, much less negotiate details of sub-optimal privacy policies or find alternative providers for services with unacceptable ones.[3]

Instead, consumers are subject to terms and conditions they have not read or they decide not to use services that may be beneficial and innovative. Neither is a good result. In the first instance, consumers may give up information and rights without understanding the risks sufficiently. In the second instance, commerce and the adoption of useful technology are slowed. For example, recent articles about new cloud storage services have recounted how privacy concerns are affecting consumer adoption.[4] In the end, some consumers may use cloud services without reading the privacy policies while others may shy away from such services completely.

At the same time, businesses recognize the need and benefit of baseline privacy legislation. Such legislation would provide rules of the road that would facilitate the flow of information and trade globally while protecting consumers.[5] As one commenter stated: "consumers want it, we believe companies need it, and the economy will be better for it."[6]

The Privacy Blueprint seeks to help consumers navigate the patchwork of privacy expectations that currently exists as they traverse the Internet and to give businesses clearer rules of the road. The goal is both to protect consumers and to ensure that the Internet remains a platform of commerce and growth, and an economic driver for our country. This position may become jeopardized if privacy concerns are not addressed, as consumers across all age ranges

---

[3] *See* http://mashable.com/2011/01/27/the-real-reason-no-one-reads-privacy-policies-infographic/.
[4] *See e.g.*, PCWorld, *Google Drive Privacy Policies Slammed*, April 28, 2012, *available at* http://www.pcworld.com/article/254600/google_drive_privacy_policies_slammed.html.
[5] *See*, Department of Commerce Internet Policy Task Force's report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, at 34, Dec. 2010, available at http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.
[6] *See id*, (quoting Hewlett-Packard Comment at 2).

report avoiding companies that do not sufficiently protect their privacy.[7] And these concerns are spreading to quickly developing areas of technology, such as mobile computing.[8]

Consumers and American businesses share a strong interest in sustaining the trust that is essential to supporting innovation, keeping the Internet growing, and maintaining the growth of the digital economy. Consumers need ways to get a better understanding about what information is collected about them and how it may be used, as well as safeguards that ensure the information is adequately protected. Businesses need clearer benchmarks for good practices, and companies that handle personal data responsibly should be able to stand out from companies that behave carelessly.

To this end, the Obama Administration has articulated the Consumer Privacy Bill of Rights and called on Congress to adopt this Bill of Rights in privacy legislation that will establish a minimum set of privacy protections for data collected about individual consumers. Such legislation would provide clear protections to consumers, a level playing field for businesses, and foster an environment of trust that will benefit both.

The Administration is not alone in calling for a new law. A broad array of private sector stakeholders has expressed support for baseline consumer privacy legislation. Consumer advocacy groups and civil liberties organizations, for example, have called for baseline consumer privacy legislation. In addition, many businesses also have supported baseline privacy legislation because they see significant value in obtaining clear privacy guidelines that enable them to earn consumers' trust, and which may also enable them to comply with international expectations. These businesses include large technology leaders that handle significant amounts of personal information and have used personal data to provide innovative new products and services.

My testimony today will cover the recommendations of the Administration's Privacy Blueprint. Looking ahead, it will focus on how legislation can implement the Privacy Bill of Rights, how Department of Commerce multistakeholder processes to develop codes of conduct

---

[7] *See* Harris Interactive/TRUSTe Privacy Index: Q1 2012 Consumer Confidence Edition, Feb. 13, 2012, *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_launches_new_trend_privacy_index (showing that U.S. adults who avoid doing business with companies that do not protect their privacy ranges from 82%, among 18-34 year olds, to 93%, among adults 55 years old and older).

[8] *See TRUSTe, More Consumers Say Privacy—Over Security—is Biggest Concern When Using Mobile Applications on Smartphones*, Apr. 27, 2011 (reporting results of survey of top 340 free mobile apps conducted jointly with Harris Interactive), *available at* http://www.truste.com/blog/2011/04/27/survey-results-are-in-consumers-say-privacy-is-a-bigger-concern-than-security-on-smartphones/.

in specific sectors will move forward, and what the Administration is doing to ensure that our privacy framework promotes growth and trade internationally for American companies.

II. The Consumer Privacy Bill of Rights

In 2009, the Department of Commerce assembled an Internet Policy Task Force. This task force spent two years developing a blueprint for protecting consumer's privacy with extensive consultation of stakeholders including consumer advocacy groups, businesses, academics, and other government agencies. The task force began by using the information learned from consulting stakeholders to craft a Privacy and Innovation Notice of Inquiry (NOI).[9] The NOI requested public comment on ways of improving privacy protections while still protecting technological innovations. The task force also organized a Privacy and Innovation Symposium on May 7, 2010.

The initial conclusions obtained from stakeholder discussions, the comments received in response to the NOI, and discussions from the symposium led to the publication in December 2010 of *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, often referred to as the Commerce Green Paper.[10] This Green Paper proposed a privacy framework and invited further comments on the proposed approach. The framework was refined as a result of further comments and meetings with hundreds of stakeholders representing the full spectrum of privacy interests to come up with a final strategy. This was an effort that engaged agencies across the Executive Branch through the National Science & Technology Council Subcommittee on Commercial Privacy that I co-chaired, and benefited from the valuable partnership and advice of the Federal Trade Commission.

Based on our study, in February the White House released its Privacy Blueprint.[11] This Privacy Blueprint calls for the passage of a Consumer Privacy Bill of Rights; for enforceable codes of conduct to implement that Bill of Rights developed by a spectrum of stakeholders from

---

[9] Department of Commerce, Notice of Inquiry on Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226, Apr. 23, 2010, *available at* http://www.ntia.doc.gov/files/ntia/publications/fr_privacynoi_04232010.pdf.

[10] The Privacy Blueprint builds on the Department of Commerce Internet Policy Task Force's report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, Dec. 2010, *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

[11] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in a Global Digital Economy*, Feb. 2012, *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Privacy Blueprint").

consumer groups, businesses, and others; and for active engagement with international partners to develop privacy protections that enable trustworthy transfer of data across national borders.

Apart from enforcement of consumer protection laws by the Federal Trade Commission and state attorneys general when privacy practices are unfair and deceptive, federal privacy protections in the United States are based on a sectoral approach that provides privacy protections tailored to specific industries such as finance, health care, and education. Industries that are not subject to such specific privacy laws, however, account for large shares of daily Internet usage; these include search engines, social networking sites, behavioral advertisers, and location-based services. For industries that are not covered by more specific laws, the Privacy Blueprint calls for baseline privacy protections in the form of a Consumer Privacy Bill of Rights.

The Consumer Privacy Bill of Rights articulates a set of principles that clarify to businesses and consumers alike what expectations the consumer should have from their Internet experience. The seven basic principles are:

- ***Individual Control***: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- ***Transparency***: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- ***Respect for Context***: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- ***Security***: Consumers have a right to secure and responsible handling of personal data.
- ***Access and Accuracy***: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- ***Focused Collection***: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- ***Accountability***: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

These principles are based on globally recognized Fair Information Practice Principles (FIPPs), which originated in the Department of Health, Education and Welfare's 1973 report,

Records, Computers, and the Rights of Citizens. Congress incorporated these principles into the Privacy Act of 1974. Since then, a consistent set of FIPPs has become the foundation for global privacy policy through, for example, the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Privacy Guidelines") and the Asia-Pacific Economic Cooperation's Privacy Framework. The Administration sought to remain consistent with these existing globally-recognized FIPPs as it developed the Consumer Privacy Bill of Rights.

Many individuals and organizations that commented on the Commerce Department's Privacy and Innovation Green Paper noted that changes in the ways information is generated, collected, stored, and used called for some adaptation of existing statements of the FIPPs. The digital economy of the 21st Century, driven by distribution of devices and connectivity and vast increases in computing speed, storage capacity, and applications, is data-intensive, dynamic, and increasingly driven by consumers' active participation. We therefore updated the traditional FIPPs to suit the challenges posed by the digital economy. The most significant changes are found in the principles of Individual Control, Respect for Context, Focused Collection, and Accountability.

1. ***Individual Control***

The principle of Individual Control addresses two salient aspects of the networked world. First, networked technologies offer consumers an increasing number of ways to assert control over what personal data is collected. Companies should take advantage of these technologies by offering consumers, at the time of collection, usable tools and clear explanations of their choices about data sharing, collection, use, and disclosure.

Second, the Individual Control principle calls on consumers to use these tools to take responsibility for controlling personal data collection, especially in situations where consumers actively share data about themselves, such as online social networks. In these cases, control over the initial act of sharing is critical. Consumers can take significant steps to reduce harms associated with the misuse of their data by using improved tools available to gain a better understanding of what personal data they are disclosing and to control their data.

2. ***Respect for Context***

The second noteworthy way in which the Consumer Privacy Bill of Rights adapts traditional FIPPs is reflected in the principle of Respect for Context. The basic premise of this

principle is simple: the relationship between consumers and a company – that is, the context of personal data use – should help determine whether a specific use is appropriate and what kinds of consumer choices may be necessary. Factors such as what consumers are likely to understand about a company's data practices based on the products and services it offers, how a company explains the roles of personal data in delivering these products and services, research on consumers' attitudes and understandings, and feedback from consumers should also enter these assessments.

The Respect for Context principle embodies the flexibility that is at the core of the Consumer Privacy Bill of Rights: it calls for strong protection when the context indicates – when sensitive personal information is at stake, for example – but personal data can flow relatively freely to support purposes that consumers reasonably anticipate in a given context.

For example, suppose an online social network holds out its service as a way for individuals to connect with people they know and form ties with others who share common interests. In connection with this service, the provider asks new users to submit biographical information as well as information about their acquaintances. As consumers use the service, they may provide additional information through written updates, photos, videos, and other content they choose to post. The social network's use of this information to suggest connections that its users might wish to form is integral to the service and foreseeable from the social networking context. Seeking consumers' affirmative consent to use personal data for the purpose of facilitating connections on the service is therefore not necessary. By contrast, if the social network uses this information for purposes outside this social networking context, such as employment screening or credit eligibility, the Respect for Context principle would call for prominent, clear notice and meaningful opportunities for consumer choice. The Respect for Context principle will help protect consumers against these real harms that can arise when information is lifted out of one context and used unexpectedly in another.

Similarly, explicit consent may not be required for the use of a consumer's address for the delivery of a product ordered online, but if that company sells the information to a third party such consent may be necessary. Requiring explicit consent in every case inures consumers to accepting all terms and conditions presented to them while limiting such consent to unexpected uses of consumer data empowers consumers.

The sophistication of a company's customers is an important element of context. In particular, the unique characteristics of children and teenagers may warrant different privacy protections than are suitable for adults. Children are particularly susceptible to privacy harms.[12] The Administration looks forward to exploring with stakeholders whether more stringent applications of the Consumer Privacy Bill of Rights – such as an agreement not to create individual profiles about children, even if online services obtain the necessary consent from the child to collect personal data – are appropriate to protect children's privacy.

3. ***Focused Collection***

The Focused Collection principle adapts the "data minimization" and "collection limitation" principles found in traditional FIPPs. Some existing versions of these principles provide a strict standard that makes personal data collection permissible only when it is kept to the minimum necessary to achieve specific, identified purposes. Such a one-size-fits-all standard is unworkable for the networked technologies and new data uses that enable the digital age.

Familiar and increasingly essential Internet services, such as search engines, collect a wide range of data and use it in a wide variety of ways that cannot be predicted when the data is collected. Stores of information like these have the potential to provide new frontiers of human knowledge in addition to new pathways for intrusion on privacy. Such services may be consistent with the Focused Collection principle, provided they reflect considered decisions about what kinds of personal data are necessary to provide the services, how long the data needs to be retained, and what measures may be available to make retained data less likely to be associated with specific consumers. Focused collection will help protect consumers from harm associated with misuse of data that never needed to be collected or retained to begin with. The Focused Collection principle, however, does not relieve companies of any independent legal obligations, including law enforcement orders, that require them to retain personal data.

4. ***Accountability***

Finally, the Accountability principle emphasizes that the measures companies take to educate employees about using personal data, prevent lapses in their privacy commitments, and detect and remedy any lapses that occur are crucial to protecting consumer privacy. Accountability also assures that, when consumers feel harmed by the way their data is handled,

[12] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 63, March 2012 ("when health or children's information is involved, for example, the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased.").

their complaints can go to the entity responsible for handling that data. Accountability mechanisms also may provide a route toward greater global interoperability. The Administration is actively exploring how accountability mechanisms, which could be developed through a privacy multistakeholder process, could ease privacy compliance burdens for companies doing business globally.

III. Legislation

A. *Codify Baseline Privacy Protection Principles*

The Privacy Bill of Rights establishes a set of expectations that consumers can use to understand what they should expect from businesses they deal with, and businesses can use to guide their privacy policies and practices. It establishes a benchmark that consumer and privacy groups, journalists, and policymakers can use to gauge privacy practices. Businesses that incorporate the Bill of Rights into their practices will help differentiate themselves as trustworthy stewards of personal information, enhancing competition based on privacy protection.

These changes can begin without legislation, but the Administration urges Congress to strengthen baseline privacy protections for consumers and to support continued consumer trust in the digital economy by codifying the Consumer Privacy Bill of Rights as part of baseline commercial privacy legislation. The Consumer Privacy Bill of Rights sets forth fundamental protections that have been well received by both consumers and businesses, and legislation is supported by businesses as well as civil society.

The Commerce Committee has a long history of avoiding technical mandates in legislation, which the Administration applauds. The principles in the Privacy Bill of Rights are intentionally broad to avoid technical mandates or excessively prescriptive requirements. The digital economy is constantly changing as are the risks and solutions to consumer privacy concerns. Legislation that is too prescriptive or that allows government to dictate specific technologies may stifle innovation and inhibit the development of new products or services. Similarly, legislation should not impose unnecessary burdens on all businesses to address a privacy concern that is relevant only to a subset of companies. Privacy legislation should be broad and flexible enough to cover existing services as well as future products and services that raise unforeseen concerns. Enactment of the Privacy Bill of Rights as a set of legally

enforceable rights would provide strong baseline privacy protections and permit flexibility both in enforcement and in industry compliance.

The Administration Privacy Blueprint recommends two mechanisms to apply the broad principles of the Privacy Bill of Rights to specific circumstances or practices. The first is enforcement of the Bill of Rights by the FTC and state attorneys general. The second is the development of legally enforceable codes of conduct through a voluntary multistakeholder process convened by the National Telecommunications & Information Administration (NTIA) of the Department of Commerce.

B. Grant Direct Enforcement Authority to the FTC

The Administration supports giving the FTC the direct authority to enforce the individual provisions of the Consumer Privacy Bill of Rights as enacted in law rather than relying only on its authority under Section 5 of the FTC Act to address unfair and deceptive practices or acts. Under Chairman Leibowitz as well as under Republican-appointed chairs in the preceding decade, the FTC has developed a body of law as well as expertise in privacy using its Section 5 authority. Giving the FTC direct authority to enforce the Bill of Rights would give future direction to this body of law, strengthen protection of consumers, and permit the FTC to address emerging privacy issues through specific enforcement actions governed by applicable procedural safeguards.

Baseline privacy protections enforced by the FTC would provide a level playing field for companies. Currently, a number of companies offer consumers strong privacy protections. Bad actors, however, are abusing the trust of consumers and using their information in ways not reasonably expected by their customers. Such actions undermine consumer trust in the digital economy to the detriment of businesses and consumers alike. Granting direct enforcement authority to the FTC would enable the Commission to take action against outliers and bad actors even if their actions do not violate a published privacy policy so as to constitute a deceptive practice or act.

C. Safe Harbor for FTC Approved Codes of Conduct Developed Through Multistakeholder Processes

The Administration also supports the use of multistakeholder processes to address consumer privacy issues that arise and change as quickly as networked technologies and the products and services that depend on them. These processes should be open to a broad range of participants, including companies, privacy advocates, academics, and civil and criminal law enforcement representatives, and facilitate their full participation to find creative solutions through consensus building. Specifically, the Privacy Blueprint directs the Department of Commerce, through the NTIA, to convene interested stakeholders to address consumer privacy issues in transparent, consensus-based processes that are open to all interested stakeholders.

The Administration supports codifying this role for NTIA in baseline privacy legislation because legislation would reinforce NTIA's mission and its ability to convene stakeholders. Under the Administration's recommended framework, companies would face a choice: follow the general principles of the statutory Consumer Privacy Bill of Rights, or commit to following a code of conduct that spells out how those rights apply to their businesses. If the FTC determines that this code of conduct adequately implements the Consumer Privacy Bill of Rights, the FTC would forbear from enforcing the provisions of the Consumer Privacy Bill of Rights implemented in the code of conduct against companies that subscribe to it, so long as they live up to their commitment. This approach would provide greater certainty for companies and stronger incentives for all stakeholders to work toward consensus on codes of conduct, but it requires authority from Congress to work most effectively.

There is a model for this safe harbor approach in the context of privacy in the Children's Online Privacy Protection Act of 1998 (COPPA). The FTC has years of experience in implementing COPPA and the statute has been praised for providing parents with the tools they need to protect the privacy of children under 13.

The expected outputs of these multistakeholder processes are context-specific codes of conduct that companies may choose to adopt as public commitments setting forth how they will follow the Privacy Bill of Rights. Once a company publicly commits to follow a code of conduct, the Administration expects that this commitment will be enforceable by the FTC and state attorneys general, just as companies' privacy policies and other promises are enforceable today.

The multistakeholder approach to privacy will strike a balance between certainty for companies, strong protections for consumers, and the flexibility necessary to promote continued innovation. Implementing the general principles in the Consumer Privacy Bill of Rights, as enacted in legislation, across the wide range of innovative uses of personal data should allow for a flexible, fast-paced process to determine how to define concrete practices that embody the broader principles in a specific setting. This process must be capable of addressing consumer privacy issues that arise and change quickly in the networked world. In addition, it should focus on specific business settings to help stakeholders address concrete privacy issues and business requirements, leading to practices that protect privacy without discouraging innovation. The process must also allow a broad range of stakeholders, including consumer groups and privacy scholars to participate meaningfully so they can ensure the codes of conduct carry out the principles of the Privacy Bill of Rights. For consumer and privacy advocates, the privacy multistakeholder process provides an opportunity to influence these practices through direct engagement with companies.

This vision draws from several successful examples of Internet policy development. Private-sector standards setting organizations, for example, are at the forefront of setting Internet-related technical standards. Groups such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) use transparent multistakeholder processes to set Internet-related technical standards. These processes are successful, in part, because stakeholders share an interest in developing consensus-based solutions to the underlying challenges. Successful government-convened Internet policymaking efforts in the past also provide precedents for the multistakeholder approach proposed in the Privacy Blueprint. For example, the Executive Branch led the privacy discussions of the 1990s and early 2000s, which continue to be central to advancing consumer data privacy protections in the United States. More recently, the FTC has encouraged multistakeholder efforts to develop a "Do Not Track" mechanism, which would afford greater consumer control over personal data in the context of online behavioral advertising.

Thoughtful and balanced baseline commercial privacy legislation is good for consumers and industry. As the digital economy opens the world to commerce and social interactions, the United States should provide the leadership necessary to promote consumer privacy and trust in a manner that promotes innovation and competition. We should not cede this role to other

countries that may impose unnecessarily restrictive burdens on U.S. industry with little or no consumer benefit.

The Administration is developing specific statutory suggestions to implement the Consumer Privacy Bill of Rights and welcome the opportunity to work with this Committee to enact baseline privacy legislation.

IV. Developing Enforceable Codes of Conduct through Multistakeholder Processes

The Administration has begun to take action to implement the Consumer Privacy Bill of Rights before baseline legislation is enacted. NTIA has begun to move ahead with stakeholder-driven processes to develop codes of conduct based on the Bill of Rights.

Immediately after the Privacy Blueprint was issued, NTIA sought comment from stakeholders on two sets of questions: which substantive issue is suitable for an initial effort to develop an enforceable code of conduct, and what procedures should the process to address this issue follow. NTIA suggested a number of substantive issues that are relatively discrete and manageable with the potential to deliver significant benefits to consumers through a code of conduct. The request asked stakeholders to comment on the pros and cons of taking up these issues and to offer other issues that meet the criteria of definability and potential consumer benefit. NTIA also asked for input on procedures that will make the process manageable yet open to all interested stakeholders' participation, transparent, and consensus-based.

The comment period closed on Monday, April 2, and the Commerce Department is in the process of reviewing the submissions. NTIA received comments from consumer groups, businesses, academics, and Members of Congress, including the Chairman of this Committee.

I anticipate that NTIA will soon select an initial topic and convene an initial public meeting to begin developing a code of conduct. Part of the business of this initial meeting will be for stakeholders to reach agreement on the procedures they will use to work together. While NTIA likely will provide some guidance and perspective, based on its participation in other multistakeholder processes as well as its review of comments on this process, NTIA will avoid imposing its judgment on the group.

In other words, NTIA's role will be to convene stakeholders and facilitate discussions that ensure all voices are heard, but it will not be the decision-maker on the substantive elements

of privacy codes of conduct. The government's role will be as a convener and a facilitator to forge consensus.

V. International Interoperability

What we do here in America is of paramount importance to U.S. consumers and companies, but we cannot ignore the global dimensions of the Internet. The dynamism of the digital economy is linked directly to flows of data across borders. This is why an essential element of the Administration's Blueprint for consumer privacy is international engagement.

Americans expect to follow blog posts and tweets from around the world. We expect our email to pop-up nearly instantaneously without thinking about whether it crossed national borders to get there. We demand information, goods, and services 24 hours a day, 7 days a week, regardless of whether they are provided from across town or across the globe.

In today's digital economy it is vital to maintain cross-border data flows to keep U.S. businesses tapped into the markets of the world and drive the continued growth of this sector. Over $8 trillion were exchanged over the Internet last year, and this amount is growing.[13] The digital economy accounted for 15 percent of U.S. GDP growth over the five-year period from 2004 to 2009.[14] Total retail e-commerce sales for 2011 reached an estimated $194.3 billion, 16.1 percent more than in 2010, and accounting for 4.6 percent of total retail sales versus 4.3 percent in 2010.[15] We must ensure that American companies that are leaders in Internet technology, cloud computing, and e-commerce, as well as innovative startups, have continued access to markets unimpeded by regulations that erect barriers to information flow at national borders and Balkanize the Internet. To do this, the United States must remain on the cutting edge of the digital economy in terms of both technology and policy-making as it relates to the Internet.

The Privacy Blueprint recognizes that international interoperability should start with mutual recognition of commercial data privacy frameworks. The Department of Commerce has been at the forefront of commercial privacy interoperability efforts, beginning with our negotiation of the U.S.-EU Safe Harbor Framework in 2000 and most recently with our

---

[13] Bipartisan Policy Center, *FCC Chairman Julius Genachowski: Prepared Remarks on Cybersecurity*; Feb. 22, 2012, http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0222/DOC-312602A1.pdf, at 1.
[14] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*, May 2011, http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters at 15-16.
[15] U.S. Census Bureau, *Quarterly Retail E-Commerce Sales: Fourth Quarter 2011*, Feb. 16, 2012, http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf, at 1.

leadership in the development of a system of Cross Border Privacy Rules in the Asia Pacific Economic Cooperation. Recently, Secretary Bryson and European Commission Vice President Reding reaffirmed their commitment to the U.S.-EU Safe Harbor Framework in a joint statement stating, "[t]his Framework, which has been in place since 2000, is a useful starting point for further interoperability. Since its inception, over 3,000 companies have self-certified to the Framework to demonstrate their commitment to privacy protection and to facilitate transatlantic trade. The European Commission and the Department of Commerce look forward to continued close U.S.-EU collaboration to ensure the continued operation and progressive updates to this Framework."

We look forward to exploring additional interoperability mechanisms with our European partners in particular, because they are in the midst of reviewing their privacy framework. Our European partners have taken note of our multistakeholder approach. Although domestically focused, the codes of conduct developed through the multistakeholder process could have global relevance, because consumers around the world are faced with similar privacy challenges.

Alongside these international initiatives, privacy legislation will firmly ground our consumer data privacy system here so that we can set the best example for the world and set the stage for necessary mutual recognition by other countries. Leading by example will encourage other countries to build multistakeholder processes, transparency, and flexibility into their commercial data privacy frameworks. This will help foster the free flow of information, which will benefit U.S. companies and consumers alike. We should anchor our own consumer data privacy system in law to guarantee the international interoperability our companies and our citizens need.

This is a critical time in the world of consumer data privacy. Europe is in the process of honing its approach to data privacy, and other countries around the world are starting to understand the need for rules of the road for the increasingly data-driven digital economy. We have a clear opportunity, as President Obama said to "offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies." It is incumbent upon us to take the reins of the digital economy and ensure its forward momentum.

VI. Conclusion

We ask Congress to give the Consumer Privacy Bill of Rights the force of law. These rights will provide protection for consumers and define comprehensible rules of the road for the rapidly growing marketplace for personal data. As envisioned in the Administration's Privacy Blueprint, the Consumer Privacy Bill of Rights would provide a set of standards that many responsible companies are already meeting, and legislation would serve to put these companies on a level playing field with those who are less careful with personal data.

Mr. Chairman, thank you again for the opportunity to provide our views on legislation to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you and other stakeholders toward enactment of these consumer data privacy protections. I welcome any questions.