Testimony of Lawrence E. Strickling

Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce

Hearing on "Privacy and Innovation: Does the President's Proposal Tip the Scale?"
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce

United States House of Representatives

March 29, 2012

I. Introduction

Chairman Bono Mack, Ranking Member Butterfield, and distinguished Committee Members, thank you for the opportunity to testify about the Administration's views on consumer data privacy in the digital economy. This hearing comes at a pivotal time in the development of privacy policies in the United States and throughout much of the world. The Administration appreciates your interest in these issues, and I welcome this opportunity to discuss how we can protect consumers' privacy and promote innovation in our networked world.

Last month, the Administration released its blueprint for consumer data privacy policy in the 21st Century ("Privacy Blueprint").[1] The Privacy Blueprint is the result of more than two years of work by the Department of Commerce ("Department") Internet Policy Task Force, as well as extensive discussions with stakeholders in the private sector and the government. The Privacy Blueprint sets forth a four-part approach to protecting consumer privacy. The first pillar is the Consumer Privacy Bill of Rights, which tells consumers what they should expect from companies that handle data about them and provides companies with guidelines to help them meet those expectations. Second, the Privacy Blueprint outlines a stakeholder-driven approach to apply the Consumer Privacy Bill of Rights in developing enforceable, context-specific codes of conduct that companies may choose to adopt. Third, the Privacy Blueprint emphasizes that continued vigorous enforcement by the Federal Trade Commission (FTC) and State Attorneys General is crucial to protecting consumers while maintaining the flexibility that companies need to innovate. Fourth, the Privacy Blueprint sets forth global interoperability, based on recognition of common privacy values, enforceable codes of conduct, and enforcement cooperation, as a guiding principle for protecting consumer privacy and promoting innovation in a global digital economy that will continue to be governed by different privacy laws and regulations.

My testimony today has three purposes. First, I will explain how the Consumer Privacy Bill of Rights establishes a baseline of privacy protections that Congress should enact in legislation. Second, I will explain why the multistakeholder approach outlined in the Privacy Blueprint provides the right approach to apply the Consumer Privacy Bill of Rights in specific markets or business settings. Third and finally, I will discuss the steps that the National Telecommunications and Information Administration (NTIA) is taking now to implement the Privacy Blueprint.

II. The Consumer Privacy Bill of Rights Addresses Real Harms and Will Preserve Consumer Trust

A. The Importance of Recognizing a Broad Array of Consumer Privacy Interests

Americans cherish their privacy. From the Fourth Amendment's recognition of a right to be free from unreasonable invasions of our homes and papers, to statutory guarantees of privacy in the mails enacted in the early years of the Republic, to the Supreme Court's recognition of a right to anonymous political speech, the United States has recognized that appropriate privacy protections promote commerce, encourage political discussion, and allow individuals to form and strengthen social bonds.

Privacy is also an important element of the trust that sustains digital commerce. As the President stated in introducing the Consumer Privacy Bill of Rights, citizens who have "confidence that companies will handle information about them fairly and responsibly, . . . have turned to the Internet to express their creativity, join political movements, form and maintain friendships, and engage in commerce."[2] These results are evident in the rapid growth of online commerce,[3] the adoption of smartphones,[4] the explosion of mobile applications that run on them,[5] and the integral role that Internet-based business-to-business transactions play in the U.S. economy.[6] The United States leads the world in developing and providing many of these services. Maintaining this position depends, in part, on maintaining consumer trust.

Unfortunately, companies do not always meet this expectation of fair and responsible handling of personal data. As a result, consumers suffer individual harms. These harms range from minor inconveniences, to damaged reputations and severe embarrassment, to identity theft and financial harm. Breaches involving certain types of personal data may lead to identity theft and other crimes that inflict financial harm on consumers and companies.[7] Severe embarrassment can come from something as simple as associating individuals' names, which could be gleaned from leaked email addresses or other account identifiers, with the content of a website.[8] And inconveniences arising from managing personal data in the absence of consistent baseline principles can frustrate or even mislead consumers. For example, consumers may find that they need to go through cumbersome or repetitive procedures to opt out of certain kinds of personal data collection or use.[9] This kind of process may be manageable in small doses, but it does not provide a workable template for consumers to exercise control over personal data in the modern Internet environment, in which hundreds of different entities may collect information about them.

In areas of commercial activity that are not covered by existing Federal data privacy laws, consumers have few guideposts to inform them of how information about them is collected and used. Consumers have been surprised to learn—often after a security breach—of the variety of companies that hold personal data about them.[10] They express concern about having their Internet use tracked[11] and face a steady stream of reports indicating that they are caught in an arms race for personal data.[12] Consumers also report avoiding companies that do not sufficiently protect their privacy.[13] These concerns are spread across age groups,[14] and they are spreading to new domains, such as mobile computing.[15] In addition to providing a basis for enforcement under Section 5 of the FTC Act, privacy policies are the principal mechanism to inform consumers of a company's privacy practices. Unfortunately, many privacy policies do not address consumers in an intelligible manner and have even further to go in the mobile realm. Clearer policies will help consumers understand what they can expect from companies that handle data about them and allow them to more meaningfully assess their choices.

Consumers and American businesses share a strong interest in better defining and protecting privacy interests in the digital age to maintain the trust that is necessary to keep the Internet growing and supporting innovation. Consumers should not be subject to constant uncertainty about what information is collected about them and how it may be used. They need and deserve a baseline set of protections. Conversely, companies should have clear obligations to meet, and companies that handle personal data responsibly should not be disadvantaged by those who behave carelessly.

B. Addressing Consumer Privacy Harms Through the Consumer Privacy Bill of Rights

The Consumer Privacy Bill of Rights provides these guidelines. It addresses the highly diverse privacy interests that consumers have (and, consequently, the diverse harms they may experience) and the fact that these interests change quickly, in two main ways. First, it articulates a set of rights which provides a baseline of principles to identify and analyze consumer privacy interests. Second, it outlines a multistakeholder approach to develop specific practices that implement these guidelines on a timescale that matches changes in technology, markets, and consumer expectations.

The Consumer Privacy Bill of Rights provides the right foundation for consumer privacy in the digital age. Each element of the Consumer Privacy Bill of Rights addresses consumers directly and affirmatively, to give consumers a stronger sense of what they should expect from companies. In addition, each right explains how companies that handle personal data can implement the right through their data practices.

The Consumer Privacy Bill of Rights includes:[16]

- **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.

C. The Consumer Privacy Bill of Rights Adapts Globally Recognized Fair Information Practice Principles to the Digital Economy

The Consumer Privacy Bill of Rights is 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*.[17] Congress incorporated these principles into the Privacy Act of 1974.[18] Since then, a consistent set of FIPPs has become the foundation for global privacy discussions 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")[19] and the Asia-Pacific Economic Cooperation's Privacy Framework.[20] The Administration sought to remain consistent with these existing FIPPs as it developed the Consumer Privacy Bill of Rights.[21]

At the same time, many individuals and organizations that commented on the Department's Privacy and Innovation Green Paper noted that the digital economy, which is data-intensive, dynamic, and increasingly driven by consumers' active participation, requires some adaptation of existing statements of the FIPPs.[22]

The most significant adaptations to traditional FIPPs are found in the Individual Control, Respect for Context, Focused Collection, and Accountability principles.

1. Individual Control

The principles of Individual Control encompasses two signature traits of the networked world.[23] First, networked technologies offer an increasing number of ways to allow consumers to assert control over what personal data is collected. Companies should take advantage of these technologies by offering to 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 understand their responsibilities for controlling personal data collection, particularly in situations in which 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 gaining a better understanding of what personal data they are disclosing and using the increasing number of tools available to control this data.

2. Respect for Context

The second noteworthy way in which the Consumer Privacy Bill of Rights adapts traditional FIPPs is through the Respect for Context principle.[24] The basic premise of this principle is simple: The relationship between consumers and a company—that is, the context of personal data use[25]—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. Personal data should flow relatively freely to support the purposes that consumers seek to achieve 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 to form ties with others who share common interests. In connection with providing this service, asks new users to provide biographical information about themselves 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 online social network's use of this information to suggest connections that its users might wish to form is integral to the service and obvious from the social networking context. Seeking consumers' affirmative consent to use personal data for the purpose of facilitating connections on the service is not necessary. By contrast, if the online social network uses this information to achieve purposes that fall outside the social networking context, such as employment screening or credit eligibility, the Respect for Context would call for prominent, explicit 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.

The sophistication of a company's customers is also 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, in particular, are particularly susceptible to privacy harms. 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 to collect personal data—are appropriate to protect children's privacy.

3. Focused Collection

Third, 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 purposes. Such a strict standard is unworkable for the networked technologies that support the digital economy. Familiar and increasingly essential Internet services, such as search engines, collect a wide range of personal data and use it in a wide variety of ways. Such services may be consistent with the Focused Collection principle, provided they reflect careful 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, 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.[26]

D. The Administration Supports Enacting the Consumer Privacy Bill of Rights into Law

Congress should act to protect consumers from violations of the rights defined in the Administration's Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data. As framed in the Privacy Blueprint, the Consumer Privacy Bill of Rights would provide a set of standards that many responsible companies are already capable of meeting. Legislation would put these companies on a level playing field with those who are less careful with personal data, and it would provide stronger and more specific consumer protections.

Enacting the Consumer Privacy Bill of Rights in a manner that provides sufficiently clear legal obligations will require drafting beyond the text offered in Consumer Privacy Bill of Rights itself. Accordingly, the Administration is committed to working with Congress to develop legislation that captures the flexibility and comprehensiveness of the Consumer Privacy Bill of Rights.

The Privacy Blueprint provides other recommendations for legislation based on the Consumer Privacy Bill of Rights.[27] Specifically, the Administration recommends that legislation:

- Permit the Federal Trade Commission (FTC) and State Attorneys General to directly enforce the statutory Consumer Privacy Bill of Rights.
- Authorize the FTC to review codes of conduct based on the statutory Consumer Privacy Bill of Rights, and grant an enforcement safe harbor for companies under its jurisdiction that adhere to an approved code of conduct.
- Preempt State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted in statute.
- Preserve existing sector-specific Federal laws that effectively protect personal data, to minimize the duplication of legal requirements and provide consumers with a clear sense of what protections they have and who enforces them.
- Set a uniform national standard for requiring companies to notify consumers of unauthorized disclosures of certain kinds of personal data.
- Enable enforcement that builds on the FTC's expertise and current role as the Federal Government's leading consumer privacy enforcement authority.

Just as importantly, the Administration recommends that consumer data privacy legislation incorporate certain limitations. Specifically, such legislation should avoid:[28]

- Adding duplicative or overly burdensome regulatory requirements on companies that are already adhering to legislatively adopted privacy principles.
- Prescribing technology-specific means of complying with the law's obligations.
- Precluding new business models that are consistent with the Consumer Privacy Bill of Rights in general but may involve new uses of personal information not contemplated at the time the statute is written.
- Altering existing statutory or regulatory authorities pursuant to which the government may obtain information necessary to assist in conducting border searches, investigating criminal conduct or other violations of law, or protecting public safety and national security.
- Contravening the ability of law enforcement to investigate and prosecute criminal acts and ensure public safety.Altering existing statutory, regulatory, or policy authorities that apply to the government's information practices.

The Administration has begun to think carefully about how the Consumer Privacy Bill of Rights can best be put into law, and we look forward to working with this Committee, and with the entire Congress, to that end.

III. Promoting Adoption of the Consumer Privacy Bill of Rights Through Stakeholder-Developed, Enforceable Codes of Conduct

Implementing the general principles in the Consumer Privacy Bill of Rights—as envisioned in the legislation discussed above and as planned in the processes that NTIA will pursue in parallel with legislative discussions—across the wide range of innovative uses of personal data requires 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 as quickly as networked technologies and the products and services that depend on them. 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. In addition, The process must also allow the broad range of stakeholders affected by personal data collection, use, and disclosure to participate meaningfully in determining how the Consumer Privacy Bill of Rights ought to apply in specific contexts. Finally, the process should be capable of producing practices that apply globally.

The Administration supports the use of multistakeholder processes, rather than rulemakings under the Administrative Procedure Act, to achieve these goals. Specifically, the Privacy Blueprint directs NTIA to convene interested stakeholders to address consumer privacy issues in transparent, consensus-based processes that are open to all interested stakeholders. The expected outputs of these processes are context-specific codes of conduct that companies may choose to adopt, rather than government regulations. Once a company publicly commits to follow a code of conduct, however, the Administration expects that this commitment will be enforceable by the FTC and State Attorneys General. Thus, the privacy multistakeholder approach will strike a balance between certainty for companies, strong protections for consumers, and the flexibility that is necessary to promote continued innovation.

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.[29]

Stakeholders have ample incentives to participate in this process under existing law. For companies, it is a way to build consumer trust and gain certainty as to what consumers expect from companies' personal data practices. For consumer and privacy advocates, the privacy multistakeholder process provides an opportunity to influence these practices through direct engagement with companies.

Still, consumer data privacy legislation could provide a significant boost to this flexible approach. 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 this code of conduct sufficiently implements the Consumer Privacy Bill of Rights in the context in which a company (or group of companies) plans to use it, the FTC should forbear from enforcing the Consumer Privacy Bill of Rights against it, so long as the company lives up to its commitment. The latter course would provide greater certainty for companies and stronger incentives for all stakeholders to work toward consensus on codes of conduct, but it requires Congress to act.

The legislative approach that the Administration recommends could also expand international recognition of codes of conduct. Baseline consumer privacy legislation would clarify the legal standards that underlie codes of conduct as well as their enforceability. This approach to legislation could have a broader influence on global Internet policy debates. It is important to demonstrate to our international partners that a principles-based framework, combined with a stakeholder-driven process to create more specific guidelines, can effectively address consumer data privacy issues. More generally, demonstrating that the government can facilitate the development of effective policy solutions without imposing top-down regulations will send a strong message to other countries that are increasingly turning to this approach. Still, even without baseline legislation, enforceable codes of conduct play an important role in global interoperability. For example, the U.S.-EU and U.S.-Swiss Safe Harbor Agreements are a source of legally enforceable privacy commitments and will continue to play a key role in facilitating transatlantic trade.[30]

IV. NTIA's Plans to Implement the Administration's Privacy Blueprint

A. Developing Privacy Codes of Conduct Through Multistakeholder Processes

NTIA has already begun to initiate stakeholder-driven processes to develop codes of conduct based on the Consumer Privacy Bill of Rights. Our first step was to seek 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 follow.[31] NTIA suggested a number of substantive issues that are relatively well-definable and have the potential to deliver significant benefits to consumers if they are addressed

through a code of conduct. Our request asked stakeholders to comment on the pros and cons of these candidates and to offer others that meet the criteria of definability and potential consumer benefit. We also asked for input on procedures that will make the process manageable while also open to all interested stakeholders' participation, transparent, and consensus-based.

The comment period closes next Monday, April 2, following which we will move promptly to select a substantive issue 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 will likely provide some guidance and perspective, based on its participation in other multistakeholder processes as well as its review of comments on this process, we will avoid imposing our 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 we will not be the decision-maker on the substantive elements of privacy codes of conduct.

B. Engaging Our International Partners

NTIA is also actively involved in implementing the international recommendations of the Privacy Blueprint. Consumer privacy is an increasingly important trade issue. Companies that do business globally face a complex set of privacy challenges, and complying with disparate privacy laws across the world imposes significant costs on U.S. enterprises. Moreover, these laws are in flux, as many of our trading partners in Europe, Asia, and Latin America are developing or revising their privacy frameworks.[32] Though the United States shares many privacy values with other countries, we expect that differences will remain between our consumer data privacy framework and those of our international partners.

As a result, the Privacy Blueprint recommends pursuing a course of creating greater interoperability—based on mutual recognition of common privacy values, shared efforts to develop internationally recognized codes of conduct, and enforcement cooperation—with other privacy frameworks, rather than seeking uniformity or full harmonization.[33] As the Joint Statement issued on March 19 by Secretary Bryson and European Commission Vice-President Viviane Reding states, "[t]he European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger transatlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital transatlantic common market."[34]

We at NTIA are working closely with our counterparts in the Department and throughout the Executive Branch to pursue greater interoperability of privacy frameworks. An important activity for NTIA over the next year will be to promote the privacy multistakeholder approach internationally. We expect that a diverse array of stakeholders will participate in the processes we will convene and welcome those stakeholders who have a practical perspective on global privacy compliance challenges. Finally, we will continue to coordinate with our U.S. Government counterparts to keep a close watch on legal developments in Europe and other regions and to participate in privacy discussions in forums such as the OECD and APEC. [35]

V. Conclusion

Thank you again for the opportunity to articulate the Administration's consumer data privacy policy and to discuss the steps NTIA is taking to put this policy into practice. NTIA is eager to bring stakeholders together to address privacy issues through practices that protect consumers, provide businesses with greater certainty, and allow continuing innovations that benefit our economy. We also look forward to working with you and other stakeholders to work toward the enactment of the Consumer Privacy Bill of Rights into law. I welcome any questions you have for me.

Attachment: U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson

Today's High Level Conference on Privacy and Protection of Personal Data, held simultaneously in Washington and Brussels with the participation of Vice-President Viviane Reding and Secretary John Bryson, represents an important opportunity to deepen our trans-Atlantic dialogue on commercial data privacy issues. The United States and the European Union clearly share a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes.

The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger trans-Atlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital trans-Atlantic common market. This work will also encourage innovation and entrepreneurship and support the jobs and growth agenda as outlined by President Obama and Presidents Van Rompuy and Barroso at the November 28, 2011 U.S.-EU Summit.

This is a defining moment for global personal data protection and privacy policy and for achieving further interoperability of our systems on a high level of protection. On January 25, 2012, the European Commission adopted legislative proposals to reform and strengthen the fundamental right to data protection and unify the EU's data protection laws and enforcement rules. On February 23, 2012, the United States released its privacy blueprint, including the Consumer Privacy Bill of Rights. President Obama emphasized the administration's commitment to privacy in the U.S., and called for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors not subject to existing Federal data privacy laws and development of enforceable codes of conduct through multistakeholder processes.

Stakeholders in the U.S. are very interested in the ongoing data protection reform in the European Union– notably in the proposal for a "one-stop-shop" and a consistent regulatory level playing field across all EU Member States. Additionally, as expressed in the Obama administration's privacy blueprint, the United States is committed to engaging with the European Union and other international partners to increase interoperability in privacy laws and regulations, and to enhance enforcement cooperation. The European Union is following new privacy developments in the United States closely. Both parties are committed to working together and with other international partners to create mutual recognition frameworks that protect privacy. Both parties consider that standards in the area of personal data protection should facilitate the free flow of information, goods and services across borders. Both parties recognize that while regulatory regimes may differ between the U.S. and Europe, the common principles at the heart of both systems, now re-affirmed by the developments in the US, provide a basis for advancing their dialog to resolve shared privacy challenges. This mutual interest shows there is added value for the enhanced EU-U.S. dialogue launched with today's data protection conference.

We hope to also work with international stakeholders towards a global consensus on how to tackle emerging privacy issues.

In line with the objectives of increasing trade and regulatory cooperation outlined by our leaders at the U.S.-EU Summit, the United States and the European Union reaffirm their respective commitments to the U.S.-EU Safe Harbor Framework. This 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. As the EU and the United States continue to work on significant revisions to their respective privacy frameworks over the next several years, the two sides will endeavor to find mechanisms that will foster the free flow of data across the Atlantic. Both parties are committed to work towards solutions based on non-discrimination and mutual recognition when it comes to personal data protection issues which could serve as frameworks for global interoperability that can promote innovation, the free flow of goods and services, and privacy protection around the world. The EU and the United States remain dedicated to the operation of the Safe Harbor Framework-as well as to our continued cooperation with the Commission to address issues as they arise-as a means to allow companies to transfer data from the EU to the United States, and as a tool to promote transatlantic trade and economic growth.

While this conference was convened to discuss commercial data privacy questions and not issues of exchanges of information related to law enforcement, we note that our presidents announced at the November 2011 summit that the US and the EU are determined to finalize negotiations on a comprehensive EU-U.S. data privacy and protection agreement that provides a high level of privacy protection for all individuals and thereby facilitates the exchange of data needed to fight crime and terrorism.

---

[1] 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 [4] ("Privacy Blueprint"). 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 [5].

[2] Privacy Blueprint at i.

[3] Online retail sales provide one measure of this growth. In 2000, online retail sales in the United States totaled $29 billion. U.S. Census Bureau, *E-Stats*, at 3, Mar. 18, 2002, *available at* http://www.census.gov/econ/estats/archives.html [6]. According to preliminary estimates, in 2011, online retails sales could total around $200 billion. *See* U.S. Census Bureau, Quarterly Retail E-Commerce Sales – 4th Quarter 2011, at 2, Feb. 16, 2012, *available at* http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf [7].

[4] Smartphone ownership among U.S. adults increased by 11 percent between May 2011 and February 2012. Pew Internet & American Life Project, 46% of American Adults Are Smartphone Owners, at 4, Mar. 1, 2012, *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/Smartphone%20ownership%202012.pdf [8].

[5] *See* Gartner, Inc., Gartner Says Worldwide Mobile Application Store Revenue Forecast to Surpass $15 Billion in 2011, Jan. 26, 2011, *available at* http://www.gartner.com/it/page.jsp?id=1529214 [9].

[6] *See, e.g.*, U.S. Census Bureau, *E-Stats*, at 2, May 26, 2011, *available at* http://www.census.gov/econ/estats/2009/2009reportfinal.pdf [10] (reporting that business-to-business digital commerce transactions totaled $3.1 trillion in 2009, the latest year for which final statistics are available).

[7] *See* Sasha Romanosky, Richard Sharp, and Alessandro Acquisti, *Data Breaches and Identity Theft: When Is Mandatory Disclosure Optimal?* at 1, Ninth Workshop on the Economics of Information Security (WEIS 2010), *available at* http://weis2010.econinfosec.org/papers/session1/weis2010_romanosky.pdf [11] (asserting and provideing citations showing that information obtained through data breaches "can then be used to commit crimes" such as filing fraudulent unemployment claims and tax returns and committing various types of financial fraud).

[8] *See* Timothy Stenowick, YouPorn: Up To 1 Million Adult Chat Users' Email Addresses and Passwords Exposed, The Huffington Post, Feb. 22, 2012, *available at* http://www.huffingtonpost.com/2012/02/22/youporn-hacked-email-addresses-passwords_n_1294502.html [12].

[9] *See, e.g.*, In re *Chitika, Inc.*, FTC Docket No. C-4324, June 17, 2011, *available at* http://www.ftc.gov/os/caselist/1023087/110617chitikacmpt.pdf [13] (alleging that an online advertising network's opt-out was effective for only 10 days).

[10] *See, e.g.*, United States v. ChoicePoint, Inc., No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006),

http://www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf [14]; *see also* FTC Preliminary Staff Report, Dec. 2010, at 9-11 (reviewing FTC data security cases).

[11] *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities That Enable It*, at 3-4 (Sept. 2009), http://ssrn.com/abstract=1478214 [15].

[12] *See generally* Wall St. Journal, *What They Know*, *available at* http://online.wsj.com/public/page/what-they-know-digital-privacy.html [16] (last visited Mar. 21, 2012).

[13] *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 [17].

[14] *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 [17] (reporting survey results 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).

[15] *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/surveyresults-are-in-consumers-say-privacy-is-a-biggerconcern-than-security-on-smartphones/ [18].

[16] For brevity, we provide only the consumer-directed portion of each right. For the full statement of the Consumer Privacy Bill of Rights, see Privacy Blueprint, App. A, at 47-48.

[17] Department of Health, Educ., and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of* Citizens, July 1973, *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm [19] (outlining a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government).

[18] *See* Privacy Act of 1974, Pub. L. No. 93-579 (codified at 5 U.S.C. § 552a).

[19] The OECD Privacy Guidelines are available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [20].

[20] The APEC Privacy Framework is available at http://publications.apec.org/publication-detail.php?pub_id=390 [21].

[21] *See* Privacy Blueprint, Appendix B, at 49-52 (mapping the Consumer Privacy Bill of Rights to the OECD Privacy Guidelines, the APEC Privacy Framework, and a generalized version of the Department of Homeland Security's Privacy Policy).

[22] *See, e.g.*, AT&T Comment on the Privacy and Innovation Green Paper, at 7 (warning against adopting an "unduly prescriptive iteration" of FIPPs); CCIA Comment on the Privacy and Innovation Green Paper, at 14-15 (raising concerns about traditional principles of purpose specification and use limitation and advocating "a middle way that recognizes the value in these principles but still gives a data collector some latitude to develop novel and beneficial uses for the data"); GE Comment on the Privacy and Innovation Green Paper, at 2 (asserting that the purpose specification and use limitation principles are "a logical extension of transparency").

[23] *See* Privacy Blueprint at 11-14.

[24] *See* Privacy Blueprint at 15-19.

[25] For simplicity, this discussion refers to personal data uses. The discussion applies equally to personal data collection and disclosure.

[26] *See* Privacy Blueprint at 31-33.

[27] *See* Privacy Blueprint at 35-39.

[28] Privacy Blueprint at 35-36.

[29] *See* World Wide Web Consortium, Tracking Protection Working Group, *available at* http://www.w3.org/2011/tracking-protection/ [22] (last visited Mar. 21, 2012).

[30] *See* International Trade Administration, Safe Harbor, *available at* http://export.gov/safeharbor/ [23] (last updated Mar. 22, 2012).

[31] *See* NTIA, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098, Mar. 5, 2012, *available at* http://www.ntia.doc.gov/federal-register-notice/2012/multistakeholder-process-develop-consumer-data-privacy-codes-conduct [24].

[32] *See, e.g.*, European Commission, Commission Proposes a Comprehensive Reform of the Data Protection Rules, Jan. 25, 2012, *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm [25]*;* Hunton & Williams*,* Mexico Issues New Privacy Regulations Effective December 22, 2011, Privacy and Security Law Blog, Dec. 21, 2011, available at http://www.huntonprivacyblog.com/2011/12/articles/mexico-issues-new-privacy-regulations-effective-december-22-2011/ [26]; ABS-CBN News, Senate Approves Data Privacy Act on 3rd Reading, Mar. 20, 2012, *available at* http://www.abs-cbnnews.com/business/03/20/12/senate-approves-data-privacy-act-3rd-reading [27] (reporting on legislation in the Philippines); Kevin Kwang, Singapore Seeks Input for Data Protection Law, ZDNet, Sept. 14, 2011, *available at* http://www.zdnetasia.com/singapore-seeks-input-for-data-protection-law-62302071.htm [28].

[33] The Department's International Trade Administration (ITA) has played an integral role in establishing frameworks for interoperability. For example, the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks establish significant interoperability between the United States and Europe. These Frameworks allow companies to self-certify that they comply with requirements under the EU Data Protection Directive, subject to FTC enforcement of these representations. More than 3,000 companies have participated in the Safe Harbor Frameworks, enabling them to transfer personal data from the EU to the United States. As a result, the Safe Harbor Frameworks have effectively reduced barriers to personal data flow and thereby support trade and economic growth. *See generally* Department of Commerce, Export.gov – Safe Harbor, *available at* http://export.gov/safeharbor/ [23] (last visited Mar. 16, 2012). In addition, ITA, along with the FTC, is helping to implement the Asia-Pacific Economic Cooperation's (APEC) voluntary system of Cross Border Privacy Rules, which will facilitate transnational mutual recognition among APEC's 21 member economies. *See* APEC, Electronic Commerce Steering Group, *available at* http://apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx [29] (last visited Mar. 16, 2012).

[34] U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson, Mar. 19, 2012, *available at* http://www.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re [30]. The full text of the Joint Statement is included as an attachment to this testimony.

[35] These objectives of encouraging international cooperation for effective commercial data privacy protections and promoting and enhancing multistakeholder venues to discuss Internet policy issues are important elements of the Administration's overall cyberspace policy framework. *See* The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, at 22, 24, May 2011, *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [31].