Testimony of Lawrence E. Strickling

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

Before the
Committee on Commerce, Science, and Transportation
United States Senate

March 16, 2011

I. Introduction.

Chairman Rockefeller, Ranking Member Hutchison, distinguished Committee Members, thank you for the opportunity to testify on behalf of the Department of Commerce ("Department") to discuss Internet privacy policy reform. I welcome the opportunity to discuss how we can better protect consumer data privacy in the rapidly evolving Internet Age. In doing so, I am pleased to testify here today with Jonathan Leibowitz, the Chairman of the Federal Trade Commission (FTC).

As the principal advisor to the President on communications and information policy, the National Telecommunications and Information Administration (NTIA) has been hard at work over the last two years with Secretary Locke's Internet Policy Task Force and colleagues throughout the Executive Branch to conduct a broad assessment of how well our current consumer data privacy policy framework serves consumers, businesses, and other participants in the Internet economy. Over the same period of time, the Internet Policy Task Force has engaged, formally and informally, with a broad array of stakeholders, including companies, consumer advocates, academic privacy experts, and other government agencies. We identified privacy as a key issue in strengthening consumer trust, which, in turn, is critical to realizing the full potential for innovation and growth of the Internet. Our work culminated in the release of the Task Force's "Green Paper" on consumer data privacy in the Internet economy on December 16, 2010. The Green Paper made ten separate recommendations about how to strengthen consumer data privacy protections in ways that also promote innovation, but it also brought to light many additional questions.

We sought public comment on these recommendations, and we have been busy considering the roughly 100 written responses that were filed. One general conclusion to be drawn from the comments is that the commenters believe that American consumers should have stronger privacy protections, and the companies that run our Internet economy should have clearer rules of the road to guide their uses of data about consumers.

II. Stakeholders' Perspectives on Our Current Consumer Data Privacy Framework.

The Internet economy is sparking tremendous innovation. During the past fifteen years, networked information technologies – personal computers, mobile phones, wireless connections and other devices – have been transforming our social, political and economic landscape. A decade ago, going online meant accessing the Internet on a computer in your home. Today,

"going online" includes smartphones, portable games, and interactive TVs, with numerous companies developing global computing platforms in the "cloud."

The Internet is also an essential platform for economic growth, both domestically and globally. Almost any transaction you can think of is being conducted online – from consumers paying their utility bills and people purchasing books, movies and clothes, to major corporations paying their vendors and selling to their customers. According to the U.S. Census Bureau, domestic online transactions currently total about $3.7 trillion annually.[1] Internet commerce is a leading source of job growth as well, with the number of domestic IT jobs growing by 26 percent from 1998 to 2008, four times faster than U.S. employment as a whole.[2] By 2018, IT employment is expected to grow by another 22 percent.[3]

As powerful and exciting as these developments are, they also raise new privacy issues. The large-scale collection, analysis, and storage of personal information is becoming more central to the Internet economy. These activities help to make the online economy more efficient and companies more responsive to their customer needs. Yet these same practices also give rise to growing unease among consumers, who are unsure about how data about their activities and transactions are collected, used, and stored.[4] A basic element of our current consumer data privacy framework is the privacy policy. As we mentioned in the Green Paper, these lengthy, dense, and legalistic documents do not appear to be effective in informing consumers of their online privacy choices. Surveys show that most Americans incorrectly believe that a website that has an online privacy policy is prohibited from selling personal information it collects from customers.[5] In addition, many consumers believe that having a privacy policy guarantees strong privacy rights, which is not necessarily the case.[6]

---

[1] U.S. Census Bureau, Commerce Department, "E-Stats, May 27, 2010, *available at* http://www.census.gov/econ/estats/2008/2008reportfinal.pdf.

[2] Commerce Secretary Gary Locke, Remarks on Cybersecurity and Innovation, Georgetown University, Washington, DC (September 23, 2010).

[3] *Id.*

[4] According to a recent survey, 83% of adults say they are "more concerned about online privacy than they were five years ago." Common Sense Media, Online Privacy: What Does It Mean to Parents and Kids (2010), *available at* http://www.commonsensemedia.org/sites/default/files/privacypoll.pdf (last visited March 5, 2011).

[5] Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: JOURNAL OF LAW & POLICY 723 (2007), *available at* http://www.is-journal.org/.

[6] Chris Jay Hoofnagle & Jennifer King, Research Report: What Californians Understand About Privacy Offline (2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075.

The difficulty of understanding a single privacy policy, however, is modest when compared to the problem of comprehending how personal data flows in today's online environment. A recent study found that 36 of the 50 most-visited websites state in their privacy policies that they allow third-party tracking.[7] This same study found that a few prominent sites allow more than 20 different third-party tracking mechanisms in the course of a month. One site even allowed 100 such mechanisms.[8] As the study points out, the privacy policy of the site that an individual actually visits typically does not apply to these third parties.[9] In other words, to fully understand the privacy implications of using a particular site, individuals will often have to begin by considering the privacy policies of many other entities that could gain access to data about them.

As Americans begin using smartphones and other mobile Internet devices in addition to, or instead of, laptop and desktop computers, the difficulties of understanding personal data flow become even more acute. The small screens that enable us to carry blogs, social networks, and video around in our pockets pose a new challenge to presenting consumers with information about personal data collection and use. These devices may also make location information available, which opens the door to an amazing array of new applications and services, but also adds further complexity to consumer data privacy issues.[10] Assuring consumers that their privacy interests will be protected in this rapidly changing environment is our core challenge.

During the Department's outreach to stakeholders, we received comments from consumer groups, industry, and leading privacy scholars, all of whom agreed that large proportions of Americans do not fully understand and appreciate what information is being collected about them, and how they are able to stop certain practices from taking place.[11] Several consumer advocacy and civil liberties groups expressed these concerns. These groups supported the Department's overall recommendation to develop stronger privacy protections for personal data

---

[7] Joshua Gomez, Travis Pinnick, and Ashkan Soltani, *Know Privacy*, at 27, June 1, 2009, *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

[8] *Id.* at 26.

[9] *Id.*

[10] *See, e.g.*, Frank Groeneveld, Barry Borsboom, and Boy van Amstel, Over-sharing and Location Awareness, Feb. 24, 2010, http://www.cdt.org/blogs/cdt/over-sharing-and-location-awareness (discussing, in the context of their project called "Please Rob Me," how adding location information to information posted on social networking sites can have unintended consequences).

[11] All comments that the Department received in response to the Green Paper are available at http://www.ntia.doc.gov/comments/101214614-0614-01/.

in the commercial setting. One group expressed this shared view about a basic lack of transparency particularly well:

> [C]onsumers face a continuum of risk to personal privacy, ranging from minor nuisances to improper disclosures of sensitive information and identity theft. Such unscrupulous practices, carried out without the consumers' knowledge or consent, lead to diminished consumer trust in Internet data practices, thus stunting growth and innovation.[12]

Moreover, many consumer groups made a strong economic case for consumer data privacy reform. Simply put, the inability to distinguish among companies' privacy practices may lead consumers to conclude that all companies engage in equally invasive practices. As one group noted, "even companies willing to adopt the most stringent privacy policies find that overseas customers are skeptical of those assurances because of the lack of U.S. privacy laws to back them up."[13]

Interestingly, industry shares these views in many respects. Some of the leading innovators in the Internet economy see things the same way. In comments, a leading IT company refuted the argument that baseline consumer data privacy protections would slow innovation: "We disagree with the arguments some have advocated against the adoption of legislation, particularly that privacy legislation would stifle innovation and would hinder the growth of new technologies by small businesses. Instead, we believe that well-crafted legislation can actually enable small business e-commerce growth."[14] Other companies reiterated the call for Federal privacy legislation; one argued that "dramatic and rapid technological advances are testing how the fundamental principles that underpin consumer privacy and data protection law – such as notice, consent, reasonable security, and data retention – should apply."[15] Another stressed that "consumer-facing companies . . . have powerful market incentives to protect user privacy, and must respond to user demands in order to remain competitive."[16] To ensure continued consumer trust, this company "strongly supports the development of a comprehensive privacy framework for commercial actors . . . that create[s] a baseline for privacy regulation that

[12] Consumers Union, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2.
[13] Center for Democracy and Technology, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3.
[14] Intel, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3.
[15] Microsoft, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 1.
[16] Google, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2.

is flexible, scalable, and proportional."[17] In short, uncertainty over keeping the trust of consumers online is as unsettling for some businesses as it is for consumers.

Commenters were not unanimous in their support for legislation, and some expressed opposition to enacting baseline consumer data privacy legislation. Some commenters asserted that legislation is appropriate only where "particularly sensitive privacy interests" are concerned.[18] Others argued that a legislative framework would be "too inflexible,"[19] a "one size fits all"[20] collection of rules that will become "static."[21] The Department took these concerns seriously when developing the Green Paper's Dynamic Privacy Framework for consumer data. A central feature of the Framework is an emphasis on developing industry-specific, enforceable codes of conduct that establish how Fair Information Practice Principles (FIPPs) apply in a given commercial context. And these concerns are reflected in the contours of the recommendations in this testimony.

Thus, based on an initial review of comments, the Department sees a shared set of principles that could help to inform our efforts to reform consumer data privacy in the Internet economy. The general agreement of commenters appears to rest on two tenets. First, to harness the full power of the Internet age, we need to establish norms and ground rules that promote innovative uses of information while respecting consumers' legitimate privacy interests. Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.

III. Strengthening Our Consumer Data Privacy Framework Through Baseline Protections.

Exactly three months ago, the Department published its Green Paper, which contained a set of preliminary policy recommendations to enhance consumer protection, strengthen online trust, and bolster the Internet economy. The paper made ten recommendations and sought comment on a set of additional questions. In response to the paper, the Department received

[17] *Id.*
[18] Financial Services Forum, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 8.
[19] American Association of Advertising Agencies e*t al.*, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 1.
[20] Direct Marketing Ass'n, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4; *see also* American Business Media, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4; Computer & Communications Industry Association, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 18; Keller & Heckman, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 201,1 at 1.
[21] Business Software Alliance, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 4.

thoughtful and well-researched comments from over a hundred stakeholders representing industry, consumer groups, and academia.

Having carefully reviewed all stakeholder comments to the Green Paper, the Department has concluded that the U.S. consumer data privacy framework will benefit from legislation to establish a clearer set of rules for the road for businesses and consumers, while preserving the innovation and free flow of information that are hallmarks of the Internet. The Department's privacy Green Paper – much like the staff report of the Federal Trade Commission (FTC) – highlights the need for stronger privacy protections for American consumers. As pointed out in the Commerce report, the United States has a range of data privacy laws that apply to individual sectors of the economy, such as health care, consumer credit, and personal finance. But these laws may not offer protection to some of the data uses associated with consumers' activities in the Internet economy. An overarching set of privacy principles on which consumers and businesses can rely could create a stronger foundation for consumer trust in the Internet by providing this broadly applicable framework.

Legislation to provide a stronger statutory framework to protect consumers' online privacy interests should contain three key elements. First, the Administration recommends that legislation set forth baseline consumer data privacy protections—that is, a "consumer privacy bill of rights." Second, legislation should provide the FTC with the authority to enforce any baseline protections. Third, legislation should create a framework that provides incentives for the development of codes of conduct as well as continued innovation around privacy protections, which could include providing the FTC with the authority to offer a safe harbor for companies that implement codes of conduct that are consistent with the baseline protections. This statutory framework is designed to be flexible, to keep its requirements well-tailored, and to provide a basis for greater interoperability with other countries' privacy laws.

A. Enacting a Consumer Privacy Bill of Rights.

The Administration urges Congress to enact a "consumer privacy bill of rights" to provide baseline consumer data privacy protections. Legislation should consider statutory baseline protections for consumer data privacy that are enforceable at law and are based on a comprehensive set of FIPPs. Comprehensive FIPPs, a collection of agreed-upon principles for the handling of consumer information, would provide clear privacy protections for personal data in commercial contexts that are not covered by existing Federal privacy laws or otherwise

require additional protection. To borrow from one of the responses we received, baseline FIPPs are something that consumers want, companies need, and the economy will appreciate.[22]

The Administration recommends that the baseline should be broad and flexible enough to allow consumer privacy protection and business practices to adapt as new technologies and services emerge. As noted by two privacy scholars, "[b]roadly worded legislation . . . motivates firms to produce an industry code of conduct as a way to construe and clarify the statutory scheme. Thus, baseline privacy legislation and incentives for industry to develop codes of conduct can go hand-in-hand."[23]

Finally, a baseline law holds the promise of making our consumer data privacy framework more interoperable with international frameworks. Again, leading Internet innovators support baseline legislation as a means of achieving this objective. For example, a leading online company noted that "FIPPs is a common language used by many governments worldwide, so use of similar terminology will enhance opportunities for agreement and practical approaches to data policy."[24] A Web standards organization stated that "[e]stablishing baseline commercial data privacy principles contribute[s] to the further harmonization of the global e-commerce market at least for the countries attached to the OECD, and improve[s] the transatlantic relations on online services of all sorts."[25] Other comments, which represent a wide variety of American companies, consumer advocates, and academic scholars, also supported this position, often noting that improving global interoperability could benefit companies by reducing their compliance burdens overseas.[26]

---

[22] *See* Comment of Hewlett-Packard Co. on Notice of Inquiry, at 2, June 14, 2010, *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/HP%20Comments%2Epdf.

[23] Professors Ira Rubinstein and Dennis Hirsch, Comment to the Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=D120453B-FB2B-4034-962C-C0A352328531.

[24] Yahoo!, Comment to the Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=F6A50C0B-00CC-44A6-B475-FE218170CA02.

[25] World Wide Web Consortium, Comment to the Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/ResponseW3C.pdf.

[26] *See, e.g.*, Professors Ira Rubinstein and Dennis Hirsch, Comment to the Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=D120453B-FB2B-4034-962C-C0A352328531; Intel, Comment to Department Privacy Green Paper, January 28, 2011, available at http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Intel%20Corp%20Dept%20Commerce%20green%20paper%20comment.pdf ("Intel supports federal legislation based on the Fair Information Practices (FIPs) as described in the 1980 Organization for Economic Co-Operation and Development (OECD) Privacy Guidelines.")

The Green Paper suggested that comprehensive FIPPs can serve as a basis for stronger consumer trust while also providing the flexibility necessary to define more detailed rules that are appropriate for the relationships and personal data exchanges that arise in a specific commercial context. The FIPPs that the Green Paper presented for discussion were transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing. We received many thoughtful comments on how each of these principles might apply to the commercial context, and we are continuing to assess whether these principles provide the right framework for online consumer data privacy. The Administration looks forward to working further with Congress and stakeholders to define these baseline protections.

B. Implementing Enforceable Codes of Conduct Developed Through Multi-Stakeholder Processes.

To encourage specific but adaptable rules for businesses and consumers in the implementation of baseline privacy principles, the Administration recommends a framework that can promptly address specific privacy issues as they emerge. In this framework, stakeholders from the commercial, consumer advocacy and academic sectors, as well as the FTC and other government agencies would come together to develop enforceable best practices or codes of conduct based on the principles in baseline legislation. This process would allow stakeholders to develop codes of conduct that address privacy issues in emerging technologies and business practices, without the need for additional legislation. In this framework, the FTC could have the authority to provide appropriate incentives, such as a safe harbor, for business to develop and adopt codes of conduct. Compliance with an approved code of conduct might be deemed compliance with the statutory FIPPs. Of those stakeholders that supported legislation, most shared one telecommunication company's conclusions that "[a]s the Green Paper observes, such a safe harbor provision will reinforce the industry's incentives to develop self-governance practices that address emerging issues, and to follow such practices."[27] In addition, legislation should ensure that stakeholders have appropriate incentives to revise enforceable codes of conduct as changes in technology, market conditions, and consumer expectations warrant.

[27] Verizon, Comment to the Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/comment.cfm?e=6BFB924F-75DD-4472-94F3-F76DB8EE0376.

This recommendation reflects the Department's view that government must support policy development processes that are nimble enough to respond quickly to consumer data privacy issues as they emerge and that incorporate the perspectives of all stakeholders. Industry, consumer groups, and civil society, as well as the government, all have vital roles to play in putting baseline privacy protections into practice in the United States. A leading IT company captured this multi-stakeholder perspective well, commenting that "no single entity can achieve the goal of building trust . . . as it is clearly a shared responsibility. There is a role for governments, industry, and Non-Governmental Organizations/advocacy groups (NGOs) working together to form a 'triangle of trust.'"[28] A multi-stakeholder strategy for implementation ensures that government establishes the base of this trust triangle. Such a strategy will be critical to ensure that we end up with a framework that is rational, that provides businesses with better information about what consumers expect (and vice versa), but that is also dynamic. Below, I explain in greater detail the leading role that the Department of Commerce could play in putting this multi-stakeholder model into practice.

C. Strengthening the FTC's Authority.

The independent expertise of the FTC is another key element of this framework. In addition to its leadership in developing consumer data privacy policy, the FTC plays a vital role as the Nation's independent consumer privacy enforcement authority. Granting the FTC explicit authority to enforce baseline privacy principles would strengthen its role in consumer data privacy policy and enforcement, resulting in better protection for consumers and evolving standards that can adapt to a rapidly evolving online marketplace.

D. Establishing Limiting Principles on Consumer Data Privacy Legislation.

As the Committee considers these recommendations, we would also like to provide our thoughts on limitations that Congress should observe in crafting consumer data that strengthens consumer privacy protections and encourages continuing innovation. Legislation should not add duplicative or overly burdensome regulatory requirements to businesses that are already adhering to the principles in baseline consumer data privacy legislation. Legislation should be technology-neutral, so that it allows firms flexibility in deciding how to comply with its

[28] Intel, Comment to Department Privacy Green Paper, January 28, 2011, *available at* http://www.ntia.doc.gov/comments/101214614-0614-01/attachments/Intel%20Corp%20Dept%20Commerce%20green%20paper%20comment.pdf

requirements and encourages business models that are consistent with baseline principles but use personal data in ways that we have not yet contemplated. And, domestic privacy legislation should provide a basis for greater transnational cooperation on consumer privacy enforcement issues, as well as more streamlined cross-border data flows and reduced compliance burdens for U.S. businesses facing numerous foreign privacy laws.

IV. The Department's and NTIA's Next Steps on Internet Privacy Policy.

With or without legislation, the Department and NTIA will continue to make consumer data privacy on the Internet a top priority. We will convene Internet stakeholders to discuss how best to encourage the development of privacy codes of conduct. And, the Department will support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policymaking bodies. Finally, we will continue to work with Congress and all stakeholders to develop consensus on reforms to our consumer data privacy policy framework.

A. Convening Voluntary Efforts to Define Baseline Privacy Protections.

The Department of Commerce can play a leading role in bringing stakeholders together rapidly to develop enforceable codes of conduct, in order to provide greater certainty for businesses and necessary protections for consumers. The Green Paper notes that the Department—and particularly NTIA—has the necessary expertise and can work with others in government to convene companies, consumer groups, academics, and Federal and State government agencies. It will be important to bring NTIA's experience to bear in these activities, since NTIA can work with other agencies and provide a center of consumer data privacy policy expertise. The Department received significant stakeholder support for the recommendation that it play a central role in convening stakeholders. A broad array of organizations, including consumer groups, companies, and industry groups announced their support for the Department to help coordinate outreach to stakeholders to work together on enforceable codes of conduct.[29]

Indeed, the Department is pleased to be part of an Administration effort in which this approach to protecting consumer data privacy may be immediately useful: The National

[29] *See, e.g.*, Comments of Center for Democracy and Technology; Comments of Consumers Union; Comments of Microsoft; Comments of Walmart; Comments of Intel; Comments of Google; Comments of Facebook; Comments of Interactive Advertising Bureau; and Comments of Yahoo!

Strategy for Trusted Identities in Cyberspace (NSTIC).[30] The NSTIC, which is a separate Administration initiative being developed in close consultation with the private sector, and is not part of the legislative proposal discussed in this testimony, envisions enhancing online privacy and security through services that provide credentials that improve upon the username and password schemes that are common online. The NSTIC proposes a system that would provide individuals the option of obtaining a strong credential to use in sensitive online transactions. The NSTIC calls for the participants in this digital identity marketplace to implement privacy protections that are based on the FIPPs. Developing enforceable codes of conduct through multi-stakeholder processes is one way that the Department can work with the private sector to implement these protections.

We thank you, Chairman Rockefeller, for supporting the announcement that the Department of Commerce will host the National Program Office to coordinate the federal activities to implement NSTIC. With the leadership of the private sector, the Department is ready and willing to support the implementation of NSTIC by leveraging the tremendous resources of NTIA and the National Institute of Standards and Technology.

B. Encouraging Global Interoperability.

Consistent with the general goal of decreasing regulatory barriers to trade and commerce, the Department will work with our allies and trading partners to reduce barriers to cross-border data flow by increasing the global interoperability of privacy frameworks. While the privacy laws across the globe have substantive differences, these laws are frequently based on similar fundamental values. The Department will work with our allies to find practical means of bridging differences, especially those that are often more a matter of form than substance.

The Department will work with other agencies to ensure that global privacy interoperability builds on accountability, mutual recognition and reciprocity, and enforcement cooperation principles pioneered in the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC). Agreements with other privacy authorities around the world (coordinated by key actors in the Federal Government) could reduce significant business global compliance costs.

C. Developing Further Administration Views on U.S. Internet Policy.

[30] For further information, see NIST, About NSTIC, http://www.nist.gov/nstic/ (last visited Mar. 14, 2011).

Finally, we are working to ensure that our work on consumer data privacy policy complements and informs other Internet policy development efforts that are underway in the Department and throughout the Administration. An invaluable mechanism for making this happen is the Privacy and Internet Policy Subcommittee of the National Science and Technology Council. The Subcommittee, which the White House announced last fall, is chaired by Commerce Department General Counsel Cameron Kerry and Justice Department's Assistant Attorney General Christopher Schroeder. The Subcommittee provides a forum for Federal agencies and key White House offices to coordinate and exchange ideas on how to promote a broad, visible, forward-looking commitment to a consistent set of Internet policy principles. These core principles—all of which apply to the consumer data privacy context—include facilitating transparency, promoting cooperation, strengthening multi-stakeholder governance models, and building trust in online environments.

The Subcommittee has already provided the substantive policy discussions that led to the legislative reform recommendations that I am presenting today. The Department of Commerce looks forward to continuing to work with this Committee.

V. Conclusion.

In the end, the Obama Administration's goal is to advance the domestic and global dialogues in ways that will protect consumers and innovation, and to provide leadership on information privacy policy, regulation, and legislation.

Working together with Congress, the FTC, the Executive Office of the President, and other stakeholders, I am confident in our ability to provide consumers with meaningful privacy protections in the Internet economy, backed by effective enforcement, that can adapt to changes in technology, market conditions, and consumer expectations. Establishing and maintaining this dynamic consumer data privacy framework is not a one-shot game; it will require the ongoing engagement of all stakeholders. The Department and the Administration are firmly committed to that engagement. The legislative approach that I have outlined today would lend extremely valuable support to the dynamic framework that we envision. I welcome any questions you have for me. Thank you.