

Testimony of Lawrence E. Strickling

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

Hearing on Internet Privacy:
The Views of the FTC, the FCC, and NTIA

Subcommittee on Commerce, Manufacturing, and Trade and
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives

July 14, 2011

I. Introduction.

Chairman Walden, Chairman Bono Mack, Ranking Members Eshoo and Butterfield, and distinguished Committee Members, thank you for the opportunity to testify about the important issue of online privacy. As the principal advisor to the President on communications and information policy, the National Telecommunications and Information Administration (NTIA) within the Department of Commerce (“Department” or “Commerce”) has been working 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. I welcome the opportunity to discuss how we can better protect consumer data privacy in the Digital Age. I am pleased to testify here today with Commissioner Edith Ramirez of the Federal Trade Commission (FTC) and Chairman Julius Genachowski of the Federal Communications Commission (FCC).

In March of this year, the Administration announced its support for legislation that would create baseline consumer data privacy protections through a “consumer privacy bill of rights.”¹ A guiding principle behind our recommendation is that the requirements in legislation should be general, flexible, actionable on their own, and focus on implementation through options outside the traditional regulatory sphere. We urged Congress to consider legislation that would establish these rights and obligations; to create incentives for the private sector to develop legally-enforceable, industry-specific codes of conduct that can address emerging privacy issues while providing companies some assurance that they are in compliance with the law; and to grant the FTC sufficient authority to enforce the law. My testimony today has three purposes. First, I will highlight the reasons that the Administration views consumer data privacy as an essential element of promoting growth and innovation on the Internet. Second, I will explain how the main elements of the Administration’s legislative approach—a consumer privacy bill of rights that is comprehensive but flexible, enforceable codes of conduct developed through a multi-stakeholder process, and clearer FTC enforcement authority—would help to address these issues. Third and finally, I will provide an overview of the Administration’s next steps on consumer data privacy here and internationally.

¹ Statement of Lawrence E. Strickling, Assistant Secretary for Communications and Information, before the Committee on Commerce, Science, and Transportation, United States Senate, Mar. 16, 2011, http://www.ntia.doc.gov/presentations/2011/Strickling_Senate_Privacy_Testimony_03162011.html.

II. The Need to Strengthen Our Consumer Data Privacy Framework.

Strengthening consumer data privacy protections is integral to the Administration's Internet policy agenda. The Internet economy has sparked tremendous innovation, and the Internet is an essential platform for economic growth, domestically and globally. Consumer data privacy is one of the core issues identified by the Commerce Department's Internet Policy Task Force, convened by Secretary Gary Locke to examine how well U.S. policies on privacy, cybersecurity, copyright protection, and the free flow of information serve consumers, businesses, and other participants in the Internet economy.²

A. Privacy Harms to Consumers and Risks to Internet Commerce

Americans deeply value privacy. The value of privacy includes the assertion of a broad "right to be let alone"³ as well as a right to control personal information.⁴ The United States protects privacy in the commercial arena through flexible, adaptable common law and State consumer protection statutes; sector-specific Federal data privacy laws; strong FTC enforcement; open and accountable government; and active policy development efforts that draw on the insights of many stakeholders.

Privacy is also a key requirement for sustaining consumer trust, which is critical to realizing the Internet's full potential for innovation and economic, political, and social development. When consumers provide personal data to a company, they do so in the context of a relationship based on their expectations about how the company will use and disclose the data that it collects. Consumers legitimately expect that companies will use personal data in ways that are consistent with these relationships. Many businesses also recognize that protecting their customers' privacy is critical to maintaining their trust and keeping their business. Many Internet businesses have worked with the FTC and privacy advocates to develop strong privacy

² U.S. Dept. of Commerce, Commerce Secretary Locke Announces Public Review of Privacy Policy and Innovation in the Internet Economy, Launches Internet Policy Task Force, Apr. 21, 2010, <http://www.commerce.gov/print/news/press-releases/2010/04/21/commerce-secretary-locke-announces-public-review-privacy-policy-and-i>.

³ Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890).

⁴ See U.S. Dept. of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, at 10 (2010), http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

practices.⁵ We are seeking to encourage this practice to spread more broadly and cover businesses that are not exposed to the same degree of customer scrutiny as the leading Internet companies.

In addition, consumers experience a variety of harms when their privacy expectations are violated. There is considerable evidence that U.S. consumers are increasingly uneasy with and unsure about how data about their activities is collected, stored, and used.⁶ Web tracking, location tracking, and the exchange of individual-level profiles are all sources of this unease and may feed a reluctance to adopt new applications, services, and devices. The loss of sensitive personal information through security breaches – which can result in identity theft and other harms that cause financial loss, ruin credit, and severely disrupt individuals’ lives – also illustrates some of the potential harms that consumer data privacy protections can address.

Many of these uses of personal data fall between gaps among existing Federal privacy laws, leaving companies and consumers without a clear sense of what standards apply to personal data collection, use, and disclosure. The technical and organizational complexity of the digital economy poses steep challenges to individual consumers who want to understand and manage the uses of their personal data, even if they are technically adept. The lengthy, dense, and legalistic privacy policies that many companies post 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.⁷ In addition, many consumers believe that having a privacy policy guarantees strong privacy rights.⁸ Moreover, a website’s own privacy policy typically does not apply to the potentially numerous third parties that collect information through that site.⁹ In other words, to fully understand the privacy implications of using a

⁵ *See id.* at 15 (discussing the importance of consumer trust in comments on the Department of Commerce’s Notice of Inquiry on consumer data privacy and innovation).

⁶ 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 July 6, 2011).

⁷ 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/>.

⁸ 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.

⁹ For example, a *Wall Street Journal* investigation found that “the top 50 US. websites installed an average of 64 tracking tools on visitors’ computers. Of those files, an average of 44 were installed by outside companies, primarily advertisers and marketers that track consumer behavior across the Internet.” Julia Angwin and Scott Thurn, *Privacy*

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.

B. Stakeholder Input Into Our Consumer Data Privacy Framework

The Commerce Internet Policy Task Force has engaged with a broad array of stakeholders, including companies, consumer advocates, academic privacy experts, and other government agencies. Our work produced the Task Force’s “Green Paper” on consumer data privacy in the Internet economy, released on December 16, 2010.¹⁰ The privacy Green Paper made ten separate recommendations on how to strengthen consumer data privacy protections while also promoting innovation, but it also brought to light many additional questions.

The comments we received on the privacy Green Paper from businesses, academics, and advocates informed our conclusion that the U.S. consumer data privacy framework would benefit from legislation that establishes a clearer set of rules for businesses and consumers, while preserving the innovation and free flow of information that are hallmarks of the Internet. This conclusion reflects two tenets. First, to harness the full power of the Internet, we need to establish norms and ground rules for uses of information that allow for innovation and economic growth while respecting consumers’ legitimate privacy interests. Consumer groups, industry, and leading privacy scholars agree that a large percentage 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 Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.¹²

Defense Mounted: Website Operators Say It Isn’t Possible to Keep Track of All Tracking Tools, WALL ST. JOURNAL, Oct. 8, 2010.

¹⁰ Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Dec. 16, 2010, http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

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/>.

¹² For industry comments in support of legislation, *see, e.g.*, Intel Comment at 3 (“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.”); Google Comment at 2 (supporting “the development of a comprehensive privacy framework for commercial actors . . . that create[s] a baseline for privacy regulation that is flexible, scalable, and proportional”). For consumer groups and civil liberties’ organizations comments in support of legislation, *see, e.g.*, Center for Democracy and Technology, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 (“CDT has long argued and continues to believe that the only way to implement a commercial data privacy framework that fully and effectively incorporates all the Fair Information Practice Principles is through baseline privacy legislation.”); Center for Digital Democracy and USPIRG, Comment on Department of Commerce Privacy Green Paper, at 21 (“[W]e urge the adoption of

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

To achieve the goals of promoting broader adoption of strong privacy in the commercial context and promoting an environment that encourages innovation, the Administration has recommended legislation with three main characteristics. First, it should establish baseline consumer data privacy protections that would apply in commercial contexts. Existing Federal privacy laws apply to some kinds of personal data in specific sectors, such as healthcare, financial services, and education; but they do not apply to much of the personal data that traverses the Internet. The protections in a baseline consumer data privacy law should be flexible, enforceable at law, and serve as the basis for both enforcement and development of enforceable codes of conduct that specify how the legislative principles apply in specific business contexts. Second, we have recommended that legislation provides appropriate incentives for stakeholders in the private sector to develop and adopt enforceable codes of conduct through a multi-stakeholder process. In our proposal, these codes would implement the baseline requirements of legislation in terms that make sense for a specific industry; but their adoption would be voluntary. Third, the Administration supports legislation that strengthens the FTC's consumer data privacy enforcement authority.

A. Enacting a Consumer Privacy Bill of Rights.

The Administration recommended that statutory baseline protections for consumer data privacy be enforceable by the FTC and based on a comprehensive set of Fair Information Practice Principles (FIPPs). In the Department of Commerce Green Paper, we drew from existing statements of FIPPs as a starting point for principles that should apply in the commercial context, in particular the original principles developed by the Department of Health, Education &

regulations that will ensure that consumer privacy online is protected. The foundation for such protection should be the implementation of Fair Information Practices for the digital marketing environment.”); Consumers Union, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 (“Consumers Union supports the adoption of a privacy framework that will protect consumer data both online and offline. ... CU believes this comprehensive privacy framework should be grounded in statute”); Privacy Rights Clearinghouse, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 2 (“[N]oting that consumer trust is pivotal to commercial success online, and that it has diminished with industry self-regulatory practices, PRC advocates comprehensive federal FIPPs-based data privacy legislation.”).

Welfare in 1973¹³ and elaborations developed by the Organisation for Economic Co-operation and Development (OECD).¹⁴ As we are developing in the Administration's forthcoming privacy White Paper, we seek to adapt these principles to the interactive and interconnected world of today in obligations that are enforceable against the organizations that collect, use, and disclose personal data. Transparency, security, accuracy, and accountability are fundamental to privacy protection, and the existing statements of FIPPs that we discussed in the Green Paper hold up well in the digital economy. But other dimensions of privacy protection may require a more dynamic and holistic approach. NTIA is working with our colleagues in the Department of Commerce and throughout the Administration to better address the complexity and dynamism of the digital economy while remaining consistent with existing statements of FIPPs.

One important question in this process is whether information technologies can expand individual control over personal information, and how any such capacity should be incorporated as an obligation in baseline consumer data privacy protections. A second area that we are considering was suggested by several commenters on the Commerce Department's Privacy Green Paper, who argued that FIPPs should be applied flexibly and in a manner that is appropriate to the contexts in which consumers use services in the digital economy.¹⁵ We are examining how we might take this notion of context as a guide to applying other established elements of FIPPs principles, such as specifying the purposes for collecting personal data and limiting the uses of personal data to what is accords with those specified purposes in ways that continue to encourage and enable innovation. These are complex issues that are still under active discussion within the Administration. We look forward to working with Congress and

¹³ See U.S. Dept. of Health, Education & Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, July 1973, <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

¹⁴ See OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

¹⁵ See, e.g., Ann Cavoukian, Comment on Department of Commerce Privacy Green Paper, Jan. 27, 2011, at 6 (emphasizing the importance of applying "practical privacy principles to particular contexts"); Centre for Information Policy Leadership, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 3-4 (arguing that FIPPs "should be applied within a contextual framework in which different principles carry more importance depending on the nature of the data, its sensitivity, or how it is used"); Facebook, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 6 ("[A]ny approach to privacy must give due regard to the context in which the information is collected or used, which necessarily shapes users' privacy expectations."); Google, Comment on Department of Commerce Privacy Green Paper, Jan. 28, 2011, at 6 (arguing that "FIPPs must be flexible enough to take account of the spectrum of identifiability, linkability, and sensitivity of various data in various contexts").

stakeholders to define these protections and enforcement authorities further and enact them into law.

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

The second main element of the Administration's recommended approach to legislation is the development and adoption of legally enforceable codes of conduct developed through a multi-stakeholder process. The process should permit everyone who has a stake in privacy – companies, consumers, privacy advocates, academics, and others – to work together to take the statutory baseline privacy protections and expand them into legally enforceable best practices or codes of conduct. In such a process, the government is an active participant, a convener that brings together all participants and facilitates discussions, but does not prescribe the outcome. This process should be open to any person or organization that is willing to participate in the hard work of engaging with other stakeholders to resolve any substantive differences fairly and openly.

The Administration believes that a multi-stakeholder process can be flexible and could offer the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. This recommendation reflects the Administration'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 to the greatest extent possible. A well-crafted multi-stakeholder process will allow stakeholders to address privacy issues in new technologies and business practices without the need for additional legislation, permit stakeholders to readily reexamine changing consumer expectations, and enable stakeholders to identify privacy risks early in the development of new products and services.

Multi-stakeholder processes can be well suited for illuminating the varying policy concerns inherent in such ideas as security breach notification, data security compliance, and Do-Not-Track. Starting with the commercialization of the Internet, the FTC has used a variety of stakeholder engagements to develop consumer data privacy policies. Its current work on Do-Not-Track carries on this history, and I applaud the leadership of Chairman Leibowitz,¹⁶ as well

¹⁶ See Statement of the Federal Trade Commission, before the Committee on Commerce, Science, and Transportation, United States Senate, Mar. 16, 2011, <http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf>.

as Web browser developers, Internet companies, standards organizations, privacy advocates, and others to provide options for greater control over personal information that may be used for online tracking.¹⁷ I encourage advertisers to work expeditiously with other stakeholders to implement Do Not Track capabilities based on the technical capabilities that have been added to Web browsers. The development of safe harbor programs is another task that can be addressed through the multi-stakeholder process recommended in the Commerce Green Paper.

C. Strengthening the FTC's Authority.

Bolstering the FTC's enforcement authority is the third key element of the Administration's proposed framework. In addition to its leadership in contributing to consumer data privacy policy, the FTC plays a vital role as the Nation's independent consumer privacy enforcement authority for non-regulated sectors. 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 consumer data privacy legislation, I would like to reiterate the Administration's views on the limitations that Congress should observe in crafting privacy legislation. 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 firms have the flexibility to decide how to comply with its requirements and to adopt business models that are consistent with baseline principles but use personal data in ways that we have not yet contemplated. Furthermore, domestic privacy legislation should provide a basis for greater global 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 of Commerce's Next Steps on Internet Privacy Policy.

A. Engaging with Stakeholders

¹⁷ See, e.g., W3C Workshop on Web Tracking and User Privacy, Apr. 28-29, <http://www.w3.org/2011/track-privacy/> (collecting position papers and reporting on a workshop discussion of technical and policy approaches to limit web tracking).

As discussion of consumer privacy legislation moves forward, the Department of Commerce 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 enforceable codes of conduct, in order to provide greater certainty for businesses and necessary protections for consumers. The past 15 years have shown that self-regulation without government leadership can be sporadic and lack a sense of urgency. 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.¹⁸ This will be led by the National Telecommunications and Information Administration (NTIA) but would involve all relevant Commerce components, just as NTIA supports NIST's efforts to convene stakeholders to discuss privacy issues that may arise in the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC),¹⁹ and ITA administers efforts relating to the U.S.-EU Safe Harbor Agreement²⁰ and (in coordination with the State Department and other Federal agencies) the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Data Privacy Rules.

B. Advancing Data Security

The Department will also continue to work with others in the Federal Government to develop the Administration policy on data security. The Nation's digital infrastructure is fundamental to our economy, critical to our national security and defense, and essential for open and transparent government. In addition, without sufficient data security, there can be no effective data privacy. To address these issues, the Administration in May submitted a legislative proposal to improve cybersecurity. Our proposal covers security breach reporting,

¹⁸ See, e.g., Center for Democracy and Technology, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 15; Consumers Union, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2-3; Microsoft, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 6; Walmart, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 2; Intel, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 7; Google, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 5; Facebook, Comment to Department Privacy Green Paper, Jan. 28, 2011, on 13; and Yahoo!, Comment on Department Privacy Green Paper, Jan. 28, 2011, at 11.

¹⁹ National Strategy for Trusted Identities in Cyberspace (NSTIC), Apr. 15, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

²⁰ See Export.gov, Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks (last updated Mar. 31, 2011), <http://www.export.gov/safeharbor/>.

criminal penalties for computer crime, critical infrastructure cybersecurity, protecting Federal Government computers and networks, and protecting individuals' privacy and civil liberties.²¹

I would like to highlight the main elements of the security breach reporting proposal. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal would help businesses by simplifying and standardizing the existing patchwork of 47 state laws with a single, clear, nationwide requirement, and would help ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

The Administration supports security breach notification legislation that addresses reasonable risks of harm to individuals, covers the types of personal data that are most likely to lead to these harms, and contains strong enforcement provisions. To achieve these ends, the Administration defines a set of "sensitive personally identifiable information" (SPII) to which notification requirements would apply and proposes to give the FTC the authority to add to this list. The reporting threshold in our proposal requires businesses to notify their customers of a breach unless there is no reasonable risk of harm to individuals. Businesses must also provide notice without unreasonable delay, presumed to be 60 days or less, subject to limitations for law enforcement and national security purposes. A "safe harbor" provision would exempt businesses from the reporting requirement when there is no reasonable risk of harm to individuals, as determined by applying criteria that are spelled out in the proposal, though businesses would be required to notify the FTC of their invocation of the safe harbor provision. Finally, the Administration's proposal contains strong enforcement provisions by authorizing the FTC to enforce the proposal's requirements. State Attorneys General are also authorized to bring civil actions in Federal district court, and they may obtain civil penalties through these enforcement actions. The Administration looks forward to working with this Committee and others in Congress on legislation in this area.

As a complement to the Administration's cybersecurity legislative package, the Department of Commerce has been developing a policy framework that is directed at increasing

²¹ See Statement for the Record of Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, before the Senate Homeland Security and Governmental Affairs Committee: "Protecting Cyberspace: Assessing the White House Proposal", May 23, 2011.

security beyond core critical infrastructure. Last month the Department released a green paper entitled *Cybersecurity, Innovation, and the Internet Economy*, which addresses cybersecurity the dynamic Internet and information technology sectors.²² We are currently soliciting comments from stakeholders to help us develop this critical strategy, with the goal of improving security at home and around the world so that Internet services can continue to provide a vital connection for trade and commerce, as well as for civic participation and social interaction.

C. Engaging with the Global Commercial Privacy Community

The Department will also support the Administration's efforts to encourage global interoperability by stepping up our engagement in international policymaking bodies. U.S. enterprises continue to incur substantial costs complying with disparate data privacy laws around the world. The need to comply with different privacy laws can lead to compartmentalization of data and privacy practices, can require a significant expenditure of time and resources, and can even prevent market access. Consistent with the National Export Initiative goal of decreasing regulatory barriers to trade and commerce, the Department will work with our allies and trading partners to facilitate cross-border data flows by increasing the global interoperability of privacy frameworks. Privacy laws across the globe are frequently based on similar values and a shared goal of protecting privacy while facilitating global trade and growth. The Department will work with our allies to find practical means of bridging any differences, which are often more a matter of form than substance. Specifically, 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 Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC). The continued development of frameworks for cooperation with other privacy authorities around the world, coordinated with the State Department and other key actors in the Federal Government, could further reduce significant business global compliance costs.

Just two weeks ago, the United States and the 33 other countries that are members of the OECD issued principles for creating policies that will encourage continuing innovation and economic growth through the Internet.²³ One of these principles recognizes that “[s]trong

²² *Cybersecurity, Innovation and the Internet Economy*, June 11, 2011, http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

²³ OECD High Level Meeting on the Internet Economy, Communiqué on Principles for Internet Policy-Making, June 28-29, 2011, <http://www.oecd.org/dataoecd/40/21/48289796.pdf>.

privacy protection is critical to ensuring that the Internet fulfils its full social and economic potential” and calls for strengthening the “consistency and effectiveness in privacy protection at a global level” through mutual recognition of substantively similar privacy laws and increased cross-border enforcement cooperation.²⁴ The legislative approach in the Administration’s overall framework, which preserves the flexibility that is one of the hallmarks of our current privacy framework, could advance the goal of mutual recognition and thus reduce the costs of doing business globally.

In addition, over the past two years, officials from Commerce and other parts of the Executive Branch have met frequently with European privacy officials. While we have much further to go in our discussions with Europe, and much remains uncertain about the final shape of the EU’s revised Data Privacy Directive, we see encouraging signs of potential for interoperability from the other side of the Atlantic. U.S. enactment of legislation establishing comprehensive commercial data privacy protections will help to facilitate further development. Strong leadership in this area could form a model for our partners currently examining this issue, and prevent fragmentation of the world’s privacy laws and its concomitant increase in compliance costs to our businesses that conduct international trade.

V. Conclusion.

Thank you again for the opportunity to provide our views on policies to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you, the FTC and other Federal agencies, the Executive Office of the President, and other stakeholders toward enactment of these consumer data privacy protections. I welcome any questions you have for me. Thank you.

²⁴ *Id.* at 5.