Testimony of Cameron F. Kerry

General Counsel

U.S. Department of Commerce

Hearing on Privacy and Data Security:

Protecting Consumers in the Modern World

Committee on Commerce, Science, and Transportation

United States Senate

June 29, 2011

I. Introduction.

Chairman Rockefeller, Ranking Member Hutchison, and distinguished Committee Members, thank you for the opportunity to testify about the important issue of online privacy on behalf of the Department of Commerce ("Department" or "Commerce"). I welcome the opportunity to discuss how we can best protect consumer data privacy in the Digital Age. And I am pleased to testify here today with Commissioner Julie Brill of the Federal Trade Commission (FTC) and a fellow General Counsel, Austin Schlick of the Federal Communications Commission (FCC).

At this Committee's March 16, 2011, hearing on "The State of Online Data Privacy," the Administration announced its support for legislation that would create baseline consumer data privacy protections through a "consumer privacy bill of rights."[1] We urged Congress to consider legislation that would establish these rights and obligations; to encourage 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 the proper authority to enforce the law.

We are encouraged that members of this Committee and others have introduced several bills that reflect a bipartisan effort to address significant consumer data privacy issues affecting our society and our economy.

Since this Committee's hearing in March, we have been hard at work fleshing out Administration views on the issues we highlighted then. These views will inform an Obama Administration "White Paper" on consumer data privacy, which we are in the midst of drafting. I am here today to say we look forward to working with this Committee and other members of Congress to pass legislation that will protect consumers' interests and provide businesses clear and consistent rules of the road.

As we stated in March, the Administration supports legislation that, first, creates a set of basic privacy protections in the commercial context for all American consumers. Second, the Administration supports creating incentives for the private sector to develop legally-enforceable rules that specify how to implement this bill of rights in specific business contexts. Third, because enforcement is critical to ensuring that any consumer privacy bill of rights is effective,

---

[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.

the Administration supports granting the FTC clear authority to enforce the privacy obligations established by legislation.[2]

I will outline briefly how we arrived at these premises, and then elaborate on each one.

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

Strengthening consumer data privacy protections is integral to the Department's Internet policy agenda. Consumer data privacy is one of the core issues under assessment by the Department's Internet Policy Task Force, which Secretary Gary Locke convened 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.[3]

The Internet economy has sparked tremendous innovation, and the Internet is an essential platform for economic growth, domestically and globally. Digital technology linked by the Internet has enabled large-scale collection, analysis, and storage of personal information. These tools enable new service options and capabilities but they also create risks to individual privacy.

Privacy is a key ingredient for sustaining consumer trust, which in turn is critical to realize the full potential for innovation and the growth of the Internet. The technical and organizational complexity of this environment makes it challenging for individual consumers to understand and manage the uses of their personal data even if they are technically adept.

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 on December 16, 2010.[4] 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 business, academics, and advocates informed our conclusion that the U.S. consumer data privacy framework will benefit from legislation that establishes a clearer set of rules for businesses and consumers, while

---

[2] *Id.*

[3] 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.

[4] 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.

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.[5] Second, as we go about establishing these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.[6]

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

To achieve these goals, the Administration recommended legislation to establish baseline consumer data privacy protections that will apply in commercial contexts and help fill in gaps in current privacy laws. These protections 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. Though we are still reviewing the details of the various bills introduced, we note they generally adopt an approach of defining baseline obligations for companies that handle personal data; giving the FTC enforcement

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

[6] 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 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.").

authority; and encouraging the development of industry-specific codes of conduct to implement these baseline requirements.

A. Enacting a Consumer Privacy Bill of Rights.

The Administration recommended that statutory baseline protections for consumer data privacy be enforceable at law 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 & Welfare in 1973[7] and elaborations developed by the Organisation for Economic Co-operation and Development (OECD).[8] 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. We are considering how best to incorporate principles that enable greater individual control over personal data and respect for the context in which such data was collected and that bring commercial data practices into alignment with reasonable consumer expectations. Notice and choice are fundamental to privacy protection, but today a more dynamic and holistic approach to privacy protection is needed, and obligations must be enforceable against the organizations that collect, use, and disclose personal data.

The Administration looks forward to working with Congress and 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 Administration called for a dual approach to privacy protection, coupling legislative protection enshrined in a consumer privacy bill of rights with the 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, civil liberties advocates,

---

[7] *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.

[8] *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.

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 the flexibility provided by multi-stakeholder processes could offer the most effective solution to the challenges posed by a rapidly changing technological, economic, and social environment. 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 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 policy tradeoffs inherent in such ideas like data 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,[9] as well as 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.[10] The development of safe harbor programs is another task that can be addressed through the multi-stakeholder process recommended in the Commerce Green Paper.

[9] *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.

[10] *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).

C. Strengthening the FTC's Authority.

Bolstering the FTC's enforcement authority is a key element of the Administration's proposed 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 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 legislation 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 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 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 of Commerce's Next Steps on Internet Privacy Policy.

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 insufficiently motivated. 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.[11] 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 effort to convene stakeholders to discuss privacy issues that may arise in the implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC),[12] and ITA administers efforts relating to the U.S.-EU Safe Harbor Agreement[13] and the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Data Privacy Rules. Through the National Science and Technology Council subcommittee I co-chair with Assistant Attorney General Christopher Schroeder, it will involve other Federal government components, including the FTC.

The Department will also continue to work with others in the Federal Government to develop the Administration policy on data security. Without data security, there can be no effective data privacy. Last month, the Administration submitted a legislative proposal to improve cybersecurity, which includes a national data breach reporting provision.[14]Such a law 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.

Earlier this month, the Department of Commerce released a green paper on Cybersecurity, Innovation, and the Internet Economy directed at increasing security beyond core

---

[11] *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.

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

[13] *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/.

[14] *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.

critical infrastructure in the vital Internet and information technology sectors.[15] 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.

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 OECD and APEC. The continued development of agreements 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.

Congressional action in this area at this time can have a significant global impact. The Administration's work on consumer data privacy is having a significant and positive effect on our discussions with members of the European Union. One illustration of this direction comes from a May 18, 2011, speech about the reform of the EU Data Protection Directive by European Justice Commissioner Viviane Reding. Commissioner Reding stated that "EU-U.S. cooperation on data protection is crucial to protect consumers and enhance legal security for businesses online. I welcome a draft Bill of Rights just introduced in the US Congress as a bi-partisan

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

initiative of Democrats and Republicans." Commissioner Reding also stated that "[t]his is a good opportunity to strengthen our transatlantic cooperation." Last week I was in Budapest to speak with European data privacy commissioners and, 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 and harmonization from the other side of the Atlantic. U.S. enactment of legislation establishing comprehensive commercial data privacy protections will help. 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.

Mr. Chairman, thank you again for the opportunity to provide our views on legislation to protect consumer privacy and promote innovation in the 21st Century. We look forward to working with you, 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.