Testimony of Daniel J. Weitzner

Associate Administrator for Policy Analysis and Development
National Telecommunications and Information Administration
United States Department of Commerce

Before the
Subcommittee on Commerce, Trade and Consumer Protection
Committee on Energy and Commerce
United States House of Representatives

"Do-Not-Track" Legislation: Is Now the Right Time?

December 2, 2010

I. Introduction.

Chairman Rush, Ranking Member Whitfield, and Members of the Subcommittee, thank you for your invitation to testify on behalf of the U.S. Department of Commerce. As the Associate Administrator for the Office of Policy Analysis and Development at the National Telecommunications and Information Administration (NTIA), I welcome the opportunity to testify before you to discuss how best to protect consumer privacy in the rapidly evolving Internet Age.

Establishing a strong U.S. framework for commercial data privacy is important to ensuring continued consumer trust and innovation in the Internet environment. The Commerce Department's Internet Policy Task Force has been hard at work over the last year to develop a framework for an updated approach to online privacy that will strengthen consumer protection in a manner that encourages continued innovation in the Internet marketplace. My testimony today will first focus on the overarching principles guiding the Commerce Department's review of Internet policy. I will then highlight general ideas for reform which will be discussed in more detail in a forthcoming report. I will elaborate on how we intend for our report to feed into the work of the recently-formed White House task force on "Privacy and Internet Policy." Finally, I will conclude with a discussion of "do-not-track" proposals.

I am especially pleased to be here today with my colleague David Vladeck, the Director of Consumer Protection at the Federal Trade Commission (FTC). Under the leadership of Chairman Leibowitz, the FTC has strengthened its vital role as the leading consumer data protection agency in the United States and continues to conduct itself as a consumer protection and privacy enforcement agency that is the envy of the world. Effective enforcement and leadership by the FTC needs to remain a pillar of U.S. commercial data privacy protection.

During the past fifteen years, networked information technologies – personal computers, mobile phones, and other devices – have been transforming the nation's – indeed, the world's – social, political and economic landscape. The Internet has grown into an essential platform not only for trade, but also for democracy and free speech that is celebrated in America and around the world and a vital engine of the global economy. Almost any transaction you can think of is being done online – from consumers paying their utility bills and

people buying books, movies and clothes, to major corporations paying their vendors and selling to their customers. According to the U.S. Census, domestic online transactions are currently estimated to total $3.7 trillion annually.[1] Digital 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.

E-commerce statistics capture only one portion of the economic, social, and political change brought on by the Internet. We are experiencing not only an economic transformation, but also tremendous innovation. For example:

- A decade ago, going online meant accessing the Internet on a computer in your home. Today, it also includes iPhones, portable games, and interactive TVs.
- Numerous companies are creating "cloud computing" platforms, which offer on-demand, super-computing capacity.
- Single purpose "smart applications" – like smart air conditioners – will connect to the smart grid, enabling greater energy efficiency and conservation.

As powerful, exciting, and innovative as these developments are, they also bring with them new privacy concerns. Increased collection, analysis, and storage of personal information by private entities is becoming central to the Internet economy, making the online economy more efficient and companies more responsive to their customer needs. Yet these same practices also feed into a growing concern among consumers about how their data and transactions are being monitored and preserved.[3] This is the policy challenge that confronts us today. It is one that must be approached both deliberately and with care. In a word: to harness the full power of the digital age, we need to establish ground rules that promote innovative uses of information while still respecting consumers' legitimate privacy interests. At the same

[1] U.S. Census Bureau. "*E-Stats*," 27 May 2010, http://www.census.gov/econ/estats/2008/2008reportfinal.pdf.
[2] Secretary Gary Locke, *Remarks on Cybersecurity and Innovation*, Georgetown University, Washington, DC (September 23, 2010); *see also* US Ambassador to the OECD Karen Kornbluh, *Remarks on Internet Intermediaries*, OECD Workshop, Paris, France (June 16, 2010).
[3] According to a recent survey, 85% 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), http://www.commonsensemedia.org/sites/default/files/privacypoll.pdf (last visited Nov. 26, 2010).

time, as we go about creating these privacy guidelines, we also need to be careful to avoid creating an overly complicated regulatory environment.

II. Overarching Principles Guiding the Internet Policy Task Force's Review of Commercial Data Privacy.

Over the past year, the Department of Commerce and NTIA have been focused on developing and sharing policy ideas to ensure that we continue to have an Internet environment that encourages innovation and creativity and that fosters trust with users. This effort is guided by two overarching principles:

First, preserving consumer trust is essential to the sustainability and continued growth of the digital economy. If users do not trust that their personal information is safe from misuse, they will worry about using new Internet-based services, thus threatening economic growth.

Second, commercial data privacy implicates a broad array of interests—industry, consumer, civil society, academic, and governmental—and we need a policy development process that includes input from all of these stakeholders. We can learn from the unique multi-stakeholder processes that have helped build and operate the Internet in order to arrive at best practices that can protect user privacy according to an appropriate, enforceable set of rules.

There is little question that multi-stakeholder organizations have played a major role in the design and operation of the technical aspects of the Internet and are directly responsible for its success. Indeed, many point to one specific multi-stakeholder institution known as the Internet Corporation for Assigned Names and Numbers (ICANN) as strengthening the Internet's infrastructure and thus ensuring that the Internet continues to be a significant medium for conducting research, communicating with others, and conducting business. As many of you know, ICANN was created out of an effort to bring more coordination and sustainability to the management of the Internet domain name system (DNS), as the Internet grew into a large-scale global network. Government has played a role in creating and sustaining ICANN as a multi-stakeholder model. The key role for the Commerce Department and NTIA was to convene private sector and other Internet stakeholders to discuss important DNS-related issues, bring these matters to the public's attention, and work together with interested parties to tackle

challenging problems. This multi-stakeholder process provides foundational stability and predictability, on the one hand, and agility to keep up with the Internet's dynamism, on the other.

Commercial data privacy similarly must respond to changes in networked technologies and their uses. In the years following the commercialization of the Internet in the early to mid 1990s, the government imperative was to seek unrestrained growth of the Internet as a medium. During this first phase of Internet policymaking, early online privacy engagements between the Commerce Department, the FTC, and commercial and non-commercial private sector stakeholders set out a model for addressing emerging privacy challenges such as those posed by the new and rapidly growing online advertising industry. These efforts led to progress toward voluntary, enforceable privacy disclosures, whose premise was that industry commitments would develop faster and provide more flexibility than legislation or regulation.

The Internet grew rapidly through the 2000s and supported tremendous economic growth and social innovation. Personal data available on the Internet also grew rapidly in volume and granularity, which in turn expanded the market for personal information. Congress acts on discrete challenges, such as combating spam and protecting children's personal information. Meanwhile, the over-arching "notice-and-choice" model of privacy policy – posting privacy policies on websites to inform consumers' choices about whether to use the site – remained basically unchanged. The FTC, of course, continued to enforce companies' obligations under this framework, but the previous Administration pulled back from earlier efforts to promote industry codes that addressed new privacy challenges.

Today, we are in the third decade of Internet policy-making. Government must continue to convene stakeholders to discuss critical technology issues, bring these issues to the public's attention, and work together with all interested parties to solve challenging problems. This convener role is an important way to provide leadership on these issues, while preserving the benefits of a multi-stakeholder approach. These principles have been practiced at the Commerce Department. In April of this year, Commerce Secretary Gary Locke formally announced the creation of the Department's Internet Policy Task Force. As the President's principal advisor on telecommunications and information policy, NTIA was asked to play a

leading role in the Task Force. Through its Task Force, the Department is conducting a broad review of the four key public policy and operational challenges facing the Internet: (1) enhancing commercial data privacy; (2) ensuring cybersecurity in the commercial context; (3) protecting copyrights; and (4) ensuring the global free flow of information. On the issue of protecting copyrights, we are working closely with the U.S. Intellectual Property Enforcement Coordinator and the interagency enforcement committee she chairs that Congress created to coordinate Federal efforts to combat unlawful uses of intellectual property.

Commercial data privacy has been the Internet Policy Task Force's first order of business. Our effort began by listening to everyone who was willing to talk to us: consumer groups, companies, trade associations, civil society, and academics. This past spring, these conversations helped NTIA to shape a Notice of Inquiry, which posed a number of questions about the connections between privacy, policy, and innovation in the Internet economy. NTIA held a public symposium in Washington, where experts from all sectors shared their views on topics ranging from international frameworks to specific voluntary codes of conduct. And NTIA has been working informally, but closely, with our colleagues at the FTC, which is the U.S. federal government's main commercial data privacy enforcement agency.

We have learned a great deal from this early effort. It is clear that we need to strengthen our framework. The current U.S. commercial data privacy framework is the product of diverse political and cultural forces, as well as decades of exchange with foreign and international systems. The U.S. framework has also had international influence since 1970, when Fair Information Privacy Practices -- first promulgated by the Department of Health, Education & Welfare as a response to mainframe computing -- were adopted and expanded by international bodies, such as the Organization for Economic Cooperation and Development (OECD). The U.S framework remains robust: our privacy protections stem from common law, state law, and specific federal protections, and are bolstered by FTC enforcement and self-regulatory mechanisms. But the U.S. framework leaves some areas out and does not provide consumers, businesses, or our international partners with a clear set of rules for the handling of commercial data.

Now, it is time to shore up commercial data privacy protection in the U.S. and abroad, and to preserve the unique online environment that has allowed sustained commercial growth on a domestic and global scale.

Like so many Internet and telecommunications issues, safeguarding consumer privacy should remain a bipartisan concern. This has been the case from the very beginning of Internet policy making. Section 230 of the Communications Decency Act, and the notice-and-takedown provisions of the Digital Millennium Copyright Act (DMCA), benefitted from the leadership and support of Republican and Democratic Members of Congress. Similarly, I have been heartened to hear recent comments from both this Subcommittee's Chairman and Ranking Member that online privacy will continue to remain a priority in the next Congress. Working together, I am confident that we can achieve meaningful reform.

III. Commerce Department's Forthcoming Report on Commercial Data Privacy.

The Commerce Department will soon publish a series of policy ideas and questions through a Department of Commerce "green paper," which are intended to play a key role in our effort to close gaps in consumer protection, strengthen online trust, and bolster the Internet economy. The paper will contain both proposed recommendations for discussion and a further set of questions on topics about which we seek further input.

So what have Internet stakeholders expressed to us about what specifically needs to be done to strike a better balance between privacy and innovation? First, they feel that it is time that consumers be provided, essentially, a privacy baseline regarding the handling of their consumer information. This baseline would be based on a full set of fair information practice principles (FIPPs) – guidelines that represent widely-accepted concepts concerning how online entities collect and use personal information – and would provide transparent disclosure to consumers, businesses, and Internet stakeholders across the various commercial contexts in which recorded data is being used. To borrow from one of the responses we received to our Notice of Inquiry, baseline FIPPs are something that consumers want, companies need, and the economy will appreciate. If desired, industry, consumer groups, civil society, and the U.S. Government all have important roles to play in helping this framework take hold. We take note of the fact that many commenters in our Notice of Inquiry, including leading Internet

companies and many civil society groups, support a legislated set of privacy baselines. In assessing a range of tools to support dynamic, baseline privacy protection, our report will address the role that properly tailored legislation could play in this framework.

Second, consistent with our multi-stakeholder model, we agree with Internet stakeholders that government is not going to have all the answers. Along with government, there are vital roles for industry, consumer groups, and civil society to play in putting FIPPs into practice in the United States. A multi-stakeholder strategy for implementation will be critical to ensure that we end up with a framework that is rational, that provides businesses with clear markers about how to meet their obligations, but that is also dynamic, to keep information practices in line with consumer expectations as technologies and markets evolve.

With or without legislation, Internet stakeholders suggested that the centerpiece of Internet privacy protection may be upgrading the role of voluntary but *enforceable* codes of conduct, developed through open, inclusive processes. This approach recognizes that technologists and entrepreneurs, privacy and consumer advocates, businesses, and the government have to work together to develop best practices for managing commercial data in particular circumstances. Launching such multi-stakeholder processes is, indeed, challenging. But, given the success of using this model in other Internet contexts, such as development of standards and protocols, we are confident that it will be successful.

Voluntary but enforceable codes of conduct are an important mechanism by which all companies would adopt some strategy for implementing FIPPs. The specific means of doing so would be flexibile and able to adapt to changing business models as they are introduced, as opposed to having to wait for lengthy and contentious agency rulemaking procedures. After-the-fact oversight by the FTC is an essential to provide consumers the assurance that companies adhere to the commitments made in the codes of conduct.

The Commerce Department's Internet Policy Task Force will continue to make commercial data privacy reform a top priority. Our future efforts on privacy reform have been motivated by listening to everyone willing to talk to us: companies, consumer groups, civil society, state regulators, and academics. We began our conversation with these stakeholders this past spring and we will continue to engage experts from all sectors on topics ranging from

international frameworks to voluntary codes of conduct. Our work will also complement, not supplant, the FTC, which fully maintains its independent enforcement and policy making roles as the main privacy enforcement agency. Nor would the Commerce Department change how the federal government goes about managing its own information practices through the Office of Management and Budget and individual agency Chief Privacy Officers. Instead, the key role for our new Task Force would be to bring together the many different parties that are necessary to help develop commercial data privacy practices for new circumstances.

As new online business models emerge, the Commerce Department and NTIA can help convene stakeholders to develop best practices by providing more cohesive Executive Branch leadership on commercial data privacy issues. These best practices can be developed faster than any regulatory proceeding would allow, while providing greater certainty for businesses and necessary protections for consumers. An institutional commitment to engage on information privacy issues in a dynamic, multi-stakeholder manner over the long term would do more than just help voluntary industry codes to develop; it would also be a better vehicle for us to better engage with Congress in addressing the commercial data privacy issues we are all confronting.

On the overall architecture for privacy reform there are three basic tools of government – prescriptive, before-the fact regulation; after-the-fact enforcement; and government-as-convener, which enables cooperation and better convergence on best practices. Our overall efforts on commercial data privacy can be explained by an effort to develop an architecture that puts each of these in its proper place. As a convener, the Commerce Department's role is much different than a regulator conducting after the fact enforcement. Rather, our role is to encourage standard setting, effective cooperation, and sharing of best practices – as well as challenging firms to attend to privacy issues.

And finally, stakeholders have requested that the Obama Administration help renew our commitment to global interoperability by redoubling our collaboration with multilateral organizations engaged in developing with global privacy standards and principles. The legal and policy framework surrounding the Internet, especially privacy, is complicated both domestically and internationally. While they understand that governments must act to protect their citizens,

they also wish to avoid fragmented sets of inconsistent and unpredictable rules that frustrate innovation and create needless barriers to the free flow of information, goods, and services on the global Internet.

In furtherance of this agenda, on October 24th, the White House announced the formation of a Privacy and Internet Policy Subcommittee to further advise the Obama Administration on commercial data privacy policy. This Subcommittee – which Commerce Department General Counsel Cameron Kerry co-chairs with Assistant Attorney General Christopher Schroeder – is working to coordinate federal agencies, while engaging public stakeholders, in an effort to promote a broad, visible, forward-looking commitment to a consistent set of Internet policy principles. These core principles include facilitating transparency, promoting cooperation, strengthening multi-stakeholder governance models, and building trust in online environments.

The idea of the Subcommittee is to consult with stakeholders to address the direction of U.S. laws and regulations on Internet privacy, with a focus on commercial data privacy. The Subcommittee will work closely with private companies and consumer groups in endeavoring to strike the appropriate balance between the privacy expectations of consumers and the needs of industry, law enforcement, and other Internet stakeholders. The Subcommittee will begin its review of Internet commercial data privacy policy with the Commerce Department's green paper and stakeholder comments responding to the recommendations and questions set forth in the green paper. We have always viewed the Commerce Department's green paper as one step in an ongoing conversation, rather than a final statement of policy views, and we are working with the Subcommittee as it begins its inter-agency consideration of this critical Internet policy issue. 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 commercial data privacy policy, regulation, and legislation.

IV. Do-Not-Track.

Turning to the question of do-not-track proposals, let me start by saying that individual choice and individual control over the flow of information to and from the user has been a foundation of Internet policy from its inception. For example, user empowerment technology

(including filtering, blocking, and monitoring tools) has provided families with the means to protect their children from viewing inappropriate material online. There have been some similar developments in the area that the "do-not-track" concept is intended to address—online behavioral advertising. As Web users became aware that cookies could be used to track their activities on a single Web site as well as across multiple sites, browser developers provided their users with the means to block and manage cookies in a variety of ways. More recently, members of the online advertising industry developed common principles about the collection and use of tracking information, and the industry is rolling out a system to help consumers manage their tracking preferences online. To the extent that these tools provide effective protection for individual choices, government properly avoids regulations that would otherwise restrict the flow of information.[4]

I am pleased that discussions of any "do-not-track" requirement similarly focus on how to maximize individual choice and individual control of access to information. The Commerce Department generally supports these types of consumer empowerment. Significant challenges face the online industry, consumer advocates, regulators and policy makers, regardless of whether Do-Not-Track features are enacted pursuant to legislation or developed through voluntary agreement. Any Do-Not-Track system would necessarily have two components: first, a technical mechanism (such as one built into Web browsers) that provides the user a way to signal his or her intent not to be tracked or profiled depending on the context; and second, an understanding between individual web users and all of the various commercial (and non-commercial) services on the Web that engage in tracking as to exactly what sort of behavior those services would avoid. The technical mechanism may take some work to implement, but is presumably manageable. The second, agreement on what is meant by the "do-not-track" sign on, say, the user's browser, is a more complex task, requiring agreement on policy and best practices among a number of players including users, advertisers, marketers, technology companies, and other intermediaries.

Some users want to avoid tracking altogether. That is, they want to be sure that no Web site or third party service collects or stores any data about their Web browsing behavior.

[4] *See Reno v. ACLU*, 521 U.S. 844 (1997).

That goal can largely be accomplished with existing browser settings (to block any cookies) and additional tools that enable the user to unilaterally block other Web tracking features. For these users, greater consumer education about tools already available might be all that is needed. But many users want more nuanced choices. That is, users might be happy to have certain Web sites collect and store some information about browsing habits when it serves the users' interests, but they might want to avoid other tracking or profiling that they consider intrusive or simply of no benefit to them. In the first instance, a user may want sites to remember his or her preferences, account information, or even to provide certain types of customization. However, that same user might also want to prevent the creation and use of profiles that allow marketers or advertisers to learn details about his or her buying habits. Reaching agreement on these more complex set of choices, beyond just the technology, will require careful work. So, the best approach to achieving the important goals motivating the Do-Not-Track concept is through a voluntary, multi-stakeholder process, backed up, in the end, by FTC enforcement of the privacy commitments made to consumers through such a system.

Thus, today's debate over the feasibility of "do-not-track" may actually be an illustration of a larger problem: the overarching need for a more dynamic commercial data privacy framework that can incentivize the creation of industry codes of conduct, while also being flexible enough to keep pace with innovation. The robust, dynamic commercial data privacy framework to be discussed in the Commerce Department's green paper will help us explore ways to address new applications and technologies like do-not-track. Specifically, the Commerce Department's Internet Policy Task Force will start to convene industry and consumer groups to discuss the next steps toward achieving voluntary agreements on implementation methods for a do-not-track requirement. Our Department's Task Force is also well situated to work collaboratively with the FTC and other government agencies to encourage industry to create a workable model. Once crafted and adopted by stakeholders, the FTC's enhanced enforcement authority can ensure compliance with these voluntary agreements, as appropriate.

V. Conclusion.

As we embark on these active discussions of how to enhance our commercial data privacy framework, we should keep in mind the broad recognition that privacy protections are crucial to maintaining the consumer trust that is essential to nurturing the Internet as a political, educational, cultural, social, and business medium. Our challenge is to create a framework that enlarges U.S. prosperity and democratic values while providing meaningful tools to empower individuals to make informed and intelligent choices for protecting their privacy.

Mr. Chairman, I thank you again for the opportunity to testify on this critical issue of commercial data privacy. Over the next few months, the Obama Administration will remain engaged with all of you as Congress continues its consideration of commercial data privacy legislation. Working together with Congress and the FTC, I am confident in our ability to achieve meaningful progress. I welcome any questions you have for me. Thank you.