Before the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

INTERNATIONAL TRADE ADMINISTRATION

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,

U.S. DEPARTMENT OF COMMERCE

Washington, DC

In the Matter of	)
Information Privacy and Innovation in	)
the Internet Economy	)
Docket No. 101214614-0614-01	)

COMMENTS OF

THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

January 28, 2011

Daniel Castro

Information Technology and Innovation Foundation[1]
1101 K Street NW, Suite 610
Washington, DC 20005

[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

Introduction

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Department of Commerce request for comment on the report entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."

The Commerce Department Internet Policy Task Force has put together a detailed framework for online privacy that provides many useful recommendations; however, it also falls short in a number of areas. Specifically, the Task Force should seek to acquire more data to better understand user behavior and tradeoffs as it relates to privacy, rather than simply accept the conclusions of privacy advocacy groups that offer insufficient and outdated evidence; make clear that any new policies, including any fair information practice principles (FIPPs), be created in cooperation with the private sector; put a greater emphasis on fostering policies that enable user choice; and redirect the Commerce Department's efforts to focus more on eliminating barriers to information sharing and allow consumer protection agencies like the Federal Trade Commission (FTC) take the lead on recommending appropriate policies to ensure consumer privacy.

1. Further Data Is Needed To Understand User Behavior and Tradeoffs

There is a widely held belief, echoed in the Commerce green paper, that a minimum level of consumer trust is fundamental to the economic success of the Internet. This much is true. However, the report also suggests that current levels of online trust are insufficient, that imposing stricter privacy laws and regulations are necessary to increase trust, and that all of this must happen to advance our nation's economic goals and online commerce, a claim that is not supported by the facts.[1] Almost all of these claims are made based on user surveys that misrepresent user behavior, fail to capture user tradeoffs, or are outdated. Moreover, many of these surveys only capture user beliefs which may differ in practice from actual user behavior. For example, the report takes evidence that users have used the privacy controls on social networks as evidence that Americans "express disapproval of a variety of common commercial data practices on privacy grounds."[2] Similarly, the report points to a survey that solicited user feedback on issues such as targeted online advertising without asking about tradeoffs. Of course in the absence of tradeoffs, what user would not prefer more privacy (or more security, more features, lower prices, etc.)? The report also highlights a survey conducted in 2005 that indicated many consumers at that time did not fully understand certain aspects of online privacy, such as the implications of privacy policies. However, surveys from five years ago quite clearly fail to capture the intense scrutiny online privacy has received in the last few years, especially in the mainstream media.

While the Commerce Department Task Force has made an attempt to draw a connection between privacy and economic opportunity, by arguing that economic activity will increase with stricter privacy regulations, there is little hard proof that such an outcome will occur. Indeed, there is

ample evidence to the contrary that current privacy regulations have succeeded given the tremendous growth the United States has seen in the Internet Economy.[3] One of the reasons that the United States leads other countries and regions in Internet commerce may be, at least in part, due to the absence of overly strict privacy regulations.

Before embarking on a crusade to create new privacy legislation or regulations, the Department of Commerce should fund additional research in this area to better understand consumer behavior. For example, to what extent are consumers willing to share personal information in exchange for free or discounted products or services? And to what extent do additional privacy safeguards impact consumer behavior online and is the net effect positive or negative? And how do second-order effects, such as a decrease in advertising revenue if consumers adopt a "Do Not Track" feature, impact the broader Internet economy and other consumers? Collecting and analyzing this type of additional evidence about online consumer behavior will equip government leaders with the knowledge needed to make evidence-based policies that strike the right balance between enhanced consumer privacy and continued innovation.

Today, the Internet economy has tremendous importance—ITIF estimates that the annual global economic benefits of the commercial Internet equal $1.5 trillion, more than the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[4] Policymakers should consider carefully any attempts to impose regulations that would destabilize the fundamental building blocks of the Internet economy before tampering with the foundation of its growth.

2. Focus on Eliminating Barriers to Information Sharing

The federal government has many objectives, and at times some federal agencies may find that their goals are at odds with the work of others. For example, one agency may be working to eliminate trade barriers while another agency is working to impose export controls. Sometimes this tension can serve the common good as each side is represented by an advocate who can fully represent its interests. With regards to data privacy, consumers currently have a vocal advocate for strict privacy regulation in the Federal Trade Commission (FTC), but lack a clear advocate for eliminating barriers to information flows which benefit consumers and lower prices. Since the FTC has taken up the mantle of advancing consumer privacy protection (as it should), the Department of Commerce would better serve its mission of advancing economic growth, jobs and opportunities for all Americans by acting as an advocate for reducing barriers to the free flow of information.

Countless examples abound of how sharing information provides many useful benefits to consumers and society as a whole, from more informed consumers to a more politically engaged society. The private sector continues to find innovative ways to unlock the hidden value of data to create value for consumers and society. Social media tools in particular are an important example of useful data sharing. Consumers have enthusiastically embraced online tools for

sharing information with social networking websites like Facebook reporting over 400 million active users worldwide. Political leaders use social networking tools to communicate directly with the public. For example, President Barack Obama has over 8.6 million fans on Facebook and former Governor Sarah Palin has over 1.6 million fans.[5] Consumers share photos on websites like Flickr, videos on sites like YouTube, and opinions and reviews on sites like Yelp. The Wikimedia Foundation hosts various information sharing projects such as Wikipedia, a user-created online encyclopedia, and Wikiversity, an online community for sharing free learning resources. Overall data sharing has created a more useful and interesting experience for Internet users.

Onerous privacy regulations threaten the ability of companies to collect, share, store and use personal data. For example, restriction on sharing information with third parties would limit the ability of organizations to integrate their services with other providers. Organizations would find it more difficult to partner with outside entities to create a combined service. Mash-ups—remixing data across multiple external service providers—are one of the hallmarks of the Web 2.0. For example, Microsoft "Hohm" allows users to monitor, compare and share their home's energy usage. Google offers an application programming interface (API) which allows developers to create their own custom map. This has resulted in many interesting mash-ups. USA Today has used the API to map all of the home foreclosures in Denver since 2006, while websites such as WikiCrimes provide mash-ups of user-submitted crime reports, and Virginia Tech's eCorridors application constructs maps of broadband coverage and speeds from user-submitted data. The more significant risk for most consumers is not a loss of privacy, but the loss of free Internet content and services as a result of overly restrictive privacy regulations.

Policymakers should recognize that consumer privacy should not come at the expense of beneficial uses of individual data. Both for-profit and non-profit organizations collect, share and use individual data routinely to provide important services. Organizations routinely purchase contact lists from companies like Hoover's to find sales prospects and media contacts. Websites like Trulia and Zillow use public databases to collect and share home prices and property tax information. Non-profits and politicians routinely purchase data for outreach and fundraising. Organizations promoting government openness use personal data to provide online tools to foster transparency and public accountability. For example, websites like OpenSecrets.org track money in politics and the website LegiStorm provides salary information on Congressional staffers. And of course many organizations have begun to use personal data for targeted advertising which has provided a boost to the revenue flowing into the Internet ecosystem. Federal data privacy policies should ensure that beneficial uses of data are not curtailed by overly-restrictive data sharing policies.

One way to ensure this does not happen is for the Department of Commerce to champion this cause. It is important for the Commerce Department to look at issues surrounding the use of personal data and creating an office to serve as a resource for policy expertise in this area is a useful step. However, rather than creating a Privacy Policy Office with a limited agenda, it

should create a Data Policy Office that will focus on broader issues related to the information economy. This would be more than a mere change in name. The focus of the Data Policy Office should be to encourage data policies that foster economic activity, including policies that increase data sharing, reduce barriers to global information flows, and protect consumer privacy. By creating an office that looks at data issues more broadly rather than the narrow interest of privacy, the Department of Commerce will be able to play a more strategic long-term role in shaping economic activity in a data-intensive business environment.

3. Create New Policies in Cooperation with the Private Sector

The Commerce Department Internet Task Force has correctly looked to industry to inform its efforts to develop commercial privacy policies. While some privacy advocates are unhappy with the current state of affairs, the private sector has not been asleep at the wheel for the past decade, but has developed a number of tools and techniques to improve consumer privacy while protecting the underlying economic models of the Internet. For example, we have seen substantial progress by industry leaders in giving users more control over their data through the use of new tools for managing their privacy. Take online advertising, for example. Every major web browser includes many features to allow users to manage their online privacy settings, such as the use of cookies and anonymous web browsing modes, and this is a continued source of innovation and differentiation among competing Web browsers. Recently, for example, Microsoft announced that an upcoming version of Internet Explorer would include a feature to restrict access to browser information (such as browser histories). In addition, Google released an extension to its Chrome browser to create a one-step, persistent opt-out solution for users who do not want to receive targeted advertising. And the Mozilla Foundation has announced that it is adding a "Do Not Track" header extension to the Firefox browser.

Web browser developers are not the only ones providing consumers more control over their data. Consumers can also download third-party Web browser plug-ins like AdBlock and NoScript which completely block online advertising. And Internet users can use new applications like Bynamite which provide individuals a third-party interface to the profiles maintained about users by online advertisers and allow users to change, delete or add to their list of interests for targeted online advertising (e.g. a user could specify that they are interested in receiving ads for the categories "politics" and "education" but not "cooking"). In addition, startup companies like Personal are creating services so that users can have better tools to control their data, enforce this control, and monetize their data if they so desire.

Policymakers should rely on industry experts who have been tackling these data privacy challenges for many years to guide their decision-making. Many of the challenges that government wants to address, such as providing users a simple, intuitive interface to manage complex decisions do not have simple solutions. Many in the private sector can be an important resource to help government understand what has been tried and tested. For example, the Digital Advertising Alliance, an industry coalition, has created a self-regulatory program for online

behavioral advertising, a unique icon so consumers can identify interest-based ads, and an online tool to allow consumers to select their advertising preference for over 50 participating ad networks. As with any development, improvements come in response to consumer demand and through an iterative trial and error design process. Policymakers should therefore resist enacting policies that lock in current best practices at the expense of future improvements.

One of the principle recommendations of the Task Force is to create a set of baseline fair information practice principles (FIPPs) for commercial data privacy. Baseline FIPPs should focus on issues such as transparency of data practices that make sense to apply across all sectors. They should not attempt to address difficult questions about issues surrounding the collection, storage, transmission, sharing and use of data that may vary greatly across industries. Even within industries, policymakers should be careful to create flexible regulations since finding clear distinctions between industries is a difficult task. Even within a relatively narrow field, such as online advertising, one can find many important "sub-industries," such as mobile advertising, email advertising, and display advertising, each with its own unique challenges and methods which necessitate different policies. Proponents of comprehensive baseline privacy standards would argue that most sensitive information remains sensitive regardless of context. This is true. For example, a person might suffer harm if certain health information is disclosed, regardless of who discloses this data. However, the expectations for maintaining the privacy of data vary greatly based on context. To continue the previous example, an individual who shares health information with a doctor (e.g. the result of a pregnancy test) should have a higher expectation of privacy and demand greater privacy controls for this data than if that same individual shares health information shared on Twitter (e.g. "BTW having a baby! #excited"). Baseline FIPPs may not be the most appropriate policy tool to address the complexities of data privacy that change depending on the context.

While the green paper endorses a multi-stakeholder approach for the creation of an additional set of voluntary codes of conduct within specific industries, it is silent on the issue of the method for creating baseline privacy standards. Policymakers should make sure to involve the private sector in all discussion on privacy, in particular for specific agency rulemaking and when creating any baseline FIPPs.

4. Foster Policies that Enable User Choice

Encouraging competition that gives consumer choices between service providers is more useful than government privacy regulations that try to impose a one-size-fits-all approach to privacy. Consumers have diverse needs, expectations and interests and policymakers should be wary of imposing a single vision of privacy on all users. Unfortunately, many privacy activists do not want to set the privacy rules just for themselves, they want to set them for everyone else (even though this would hurt, not help, most consumers). Evidence of this can be seen in the recent debate about the privacy settings for Facebook where privacy fundamentalists did not just simply opt not to use the service, but instead advocated for laws to impose their standard of privacy on

all users. For example, Danah Boyd a fellow at Harvard's Berkman Center for Internet and Society, claimed that Facebook is a utility and should be regulated like one.[6] Others, such as Chris Conley at the American Civil Liberties Union (ACLU) stated "People are not necessarily thinking about how long this information will stick around, or how it could be used and exploited by marketer."[7] This type of paternalistic view of Internet users is at the heart of arguments in favor of government regulation to protect consumers from themselves.

Societal values change over time and privacy is no different. Over the course of human history, privacy itself is a relatively new value, and varies from culture to culture (and person to person). Certainly the last decade has seen a sharp rise in individuals willing to share what was previously considered private information publicly on the Internet. For example, the website NetworthIQ allows individuals to share their personal financial information online and the microblogging website Twitter allow individuals to easily share personal information, including their location, publicly and in real-time. While these websites may not appeal to everyone, users should be given the choice whether to use them.

Instead of rigid policies that would inadequately serve a heterogeneous population, policymakers should focus on policies that encourage choice and innovation for consumers. The existing ecosystem of privacy laws and regulations has allowed a variety of online services catering to consumers with different types of privacy demands to prosper. Currently, websites operate under a notice and choice regime whereby consumers can review the privacy policies, if any, offered by an organization, and then decide whether to use the services offered. For example, if a new mobile application or online service does not provide a privacy notice on their website or states that the organization will share personal information with third-parties, consumers can decide that this does not meet their standards and not use the application or service. This allows for a broad array of consumer choice between services offering different levels of privacy.

Freedom of choice to reveal or conceal private information has led to many important innovations that benefit consumers. Many, if not most, individuals routinely choose to make a trade-off of private data in exchange for something of value. In grocery stores and retail stores, consumers use loyalty cards to allow merchants to track their purchases in exchange for discounts. The same is true online—users allow websites to provide them with free or discounted content or services in exchange for targeted advertising based on personal information. This business innovation has generated an entirely new class of ad-supported online businesses. Moreover, targeted ads—advertisements relevant to a particular user—generate more than two times the revenue of non-targeted ads and are, and will continue to be, an important source of revenue for the Internet ecosystem, particularly the so-called "long tail" of small websites supported by ad revenue.[8] In addition, policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.[9]

Individuals who place a high value on their privacy also help drive innovation. Competition between service providers, whether it is for social networking or for medical data, encourages companies to provide users with simple and effective privacy controls and ensure high levels of security to protect data.[10] Competition also encourages the development of privacy-enhancing technologies (PETs). For example, in response to consumers concerns (mostly unfounded) about the ability of advertisers to track users across multiple websites through the use of cookies (small data files stored on a user's computer by a web browser to improve the web user's experience), every major web browser now includes many features to allow users control over their online privacy and the use of cookies. Other PETs, such as anonymous Internet proxies or anonymous peer-to-peer (P2P) clients, that allow individuals to use the Internet without directly revealing their IP address, similarly have come about because of user demand.

Market forces are an important mechanism for protecting user privacy. One of the most effective ways to ensure that consumers can continue to find online services that satisfy their privacy requirements is to encourage a competitive market that responds to consumer demand. For example, although Facebook is routinely criticized by privacy activists, the company has a long history of bending to consumer pressure including in May 2019 when it announced plans to roll out new privacy controls to users in response to consumer feedback.[11] Neither was this the first time that Facebook revised its policies or services in response to consumer opinion. In December 2009, Facebook altered its privacy settings so that certain information including friends list, gender, city, and profile photo, would be public information. In response to complaints from some users, Facebook modified its interface to give users more control over the privacy of different types of information. Similarly, in 2006, Facebook revamped its policy regarding its "news feed" feature that updates users about their friends' activities after receiving negative user feedback.

Conclusion

Thoughtful policy leadership is necessary for the United States to retain its role as one of the leading nations in the Internet economy. The Department of Commerce should be commended for recognizing the vital role that it has in promoting entrepreneurship, innovation and economic development. The Task Force correctly identifies the need for dynamic policy solutions that do not constrain rapid innovation and flexible regulations that adapt to new business models. A combination of basic cross-industry guidelines, voluntary industry-specific standards, and active enforcement by state and federal consumer protection agencies may be the type of moderate solution that addresses legitimate privacy concerns at a minimal cost to the private sector. However, policymakers must remember that while privacy is important, it must be balanced against competing goals including usability, cost and future innovation. Restrictive privacy regulations would likely result in the opposite—less innovation, fewer free services, and higher costs for consumers. To avoid this, policymakers should embrace principles that support consumer privacy, but not at the expense of productivity and innovation.

Endnotes

1. See for example, The Department of Commerce Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," The Department of Commerce (December 16, 2010), p. 3.
2. Ibid.
3. Robert Atkinson et al., "The Internet Economy 25 Years After .com," (Washington, D.C.: Information Technology and Innovation Foundation, 2010), http://www.itif.org/files/2010-25-years.pdf.
4. Ibid.
5. As of June 7, 2010. Source: Facebook.com.
6. Dana Boyd, "Facebook is a utility; utilities get regulated," May 15, 2010, http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.
7. Brad Stone, "For Web's New Wave, Sharing Details Is the Point," New York Times, April 22, 2010, http://www.nytimes.com/2010/04/23/technology/23share.html.
8. "Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads," Network Advertising Initiative, press release, March 24, 2010, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.
9. Robert D. Atkinson, "Federal Trade Commission Workshop on Journalism in the Digital Age," (Washington, D.C.: Information Technology and Innovation Foundation, 2010) http://www.itif.org/publications/federal-trade-commission-workshop-journalism-digital-age.
10. Daniel Castro, "Improving Health Care: Why a Dose of IT May Be Just What the Doctor Ordered," Information Technology and Innovation Foundation, October 2007, http://www.itif.org/files/HealthIT.pdf.
11. Mark Zuckerberg, "Making Control Simple,"Facebook.com, May 26, 2010, http://blog.facebook.com/blog.php?post=391922327130.