TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW.
Room 4725
Washington, DC 20230

Re: Docket No. 101214614-0614-01

Dear Mr. Burstein:

I hereby submit the attached comments in response to the NTIA's December 21, 2010 Notice and request for public comments, "Information Privacy and Innovation in the Internet Economy."

Respectfully,

Thomas M. Lenard
President and Senior Fellow
Technology Policy Institute

Before the
UNITED STATES DEPARTMENT OF COMMERCE
OFFICE OF THE SECRETARY
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
INTERNATIONAL TRADE ADMINISTRATION
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

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

COMMENTS OF

Thomas M. Lenard, Ph.D.
President & Senior Fellow
Technology Policy Institute
1401 Eye Street, NW
Suite 505
Washington, DC 20005
202-828-4405

I. Introduction

The Department of Commerce has invited comments on its December 2010 Green Paper, which contains its recommendations on commercial data privacy.[1] The Green Paper is the result of a year-long review by the DOC's Internet Policy Task Force, including extensive consultations and written comments from various stakeholders and experts.

Although acknowledging that "existing U.S. commercial data privacy policy has enabled the digital economy to flourish,"[2] the Green Paper, without presenting evidence on benefits or costs, suggests that a new "Dynamic Privacy Framework" is needed. This new framework includes:

- Official United States Government recognition of a set of Fair Information Practice Principles (FIPPS), which "should promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability."[3]
- Developing voluntary, enforceable codes of conduct. The Green Paper is agnostic on the need for legislation.
- Establishing a Privacy Policy Office (PPO) in the Department of Commerce to focus on commercial data privacy issues.
- Increasing global interoperability of privacy frameworks.
- Considering a Federal commercial data security breach notification law in order to reconcile different state laws.

---

[1] The Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," December 2010, available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf (hereafter Green Paper).

[2] Green Paper at 1.

[3] Green Paper at 4.

The Green Paper notes that "[p]rivacy protections are crucial to maintaining consumer trust, which is necessary to secure full use of the Internet as a political, educational, cultural, and social medium."[4] At the same time, the Green Paper notes:

> The Internet is also increasingly important to the personal and working lives of individual Americans. Ninety-six percent of working Americans use the Internet as part of their daily life, while sixty two percent of working Americans use the Internet as an integral part of their jobs. Finally, the Internet is creating new kinds of jobs. Between 1998 and 2008, the number of domestic IT jobs grew by 26 percent, four times faster than U.S. employment as a whole. According to one estimate, as of 2009, advertising-supported Internet services directly or indirectly employed three million Americans, 1.2 million of whom hold jobs that did not exist two decades ago. By 2018, IT employment is expected to grow by another 22 percent.[5]

The Green Paper does not provide any data or analysis suggesting that Internet use would be greater or that the Internet would be used for more purposes if privacy protections were increased.

Nor does the Green Paper examine the benefits and costs of alternative privacy policies. Before finalizing its recommendations, the Department should rigorously analyze current privacy practices and alternative policy proposals. This should include:

- Collecting current data on the privacy and data management practices of major web sites. The most recent data available appear to be from 2001.
- Producing evidence showing that current practices are harming consumers. A new privacy framework will only produce benefits to the extent it alleviates identified harms.
- Reviewing what we know about how consumers value privacy and undertaking additional studies as a basis for estimating the benefits of a new privacy framework.
- Estimating the costs of alternative proposals, including direct pecuniary costs to firms from devoting more resources to privacy and the indirect costs of having less information

[4] Green Paper at 13.

[5] Green Paper at 14.

available. The Green Paper does not acknowledge that its proposal would entail any costs.

- Producing sufficient evidence of a reasonable expectation that the benefits of its proposal are greater than the costs. Otherwise, the proposal should not be adopted.

Many types of regulatory proposals are routinely subject to this type of analysis under Executive Order 12866, issued by President Clinton, and preceding executive orders. The principles of E.O. 12866 were just recently reaffirmed by President Obama:

> As stated in that Executive Order [12866] and to the extent permitted by law, each agency must, among other things: (1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); … (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits….[6]

While the DOC is not formally proposing a regulation, and therefore does not technically violate the executive order, the Green Paper violates its spirit. To the extent the Green Paper recommendations are adopted, they will have the effect of regulation, imposing costs on certain parties, including companies and consumers, as well as compelling private action.

It is useful for the Department to gather information from comments from interested parties and other experts, as it has done. However, as the lead executive-branch agency on privacy issues, the agency should generate the data and analysis necessary to evaluate its policy proposals. The PPO that the Green Paper recommends establishing could play an important role in gathering data and undertaking analysis on an ongoing basis.

Privacy regulation is in many respects similar to safety regulation. Agencies such as the Consumer Product Safety Commission (CPSC) or the Occupational Safety and Health Administration (OSHA) propose new safety standards based on data on current industry practices, injury rates, consumers' and workers' willingness to pay for reduced injury risk, the expected benefits of the proposed standard in terms of reduced risk, and a comparison of the

---

[6] Improving Regulation and Regulatory Review – Executive Order, January 17, 2011 available at http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order>

expected benefits with the expected costs. The Department should perform such analysis with respect to its proposed privacy framework.

II. Current Privacy and Data Management Practices

The Green Paper surveys the legal privacy landscape, but provides no data on what firms and consumers are currently doing. Policymakers cannot make informed policy decisions without having an accurate understanding of the practices prevalent in the marketplace.

In addition to failing to collect current data, the Green Paper also fails to refer to the results of relevant studies carried out about a decade ago. Given the changes in the online world, these data are no longer current, but the studies are still informative and illustrate the type of data collection and analysis that should be a prerequisite to privacy policy and that the Department should undertake.

Between 1998 and 2002 researchers undertook four surveys of the privacy practices of commercial web sites:

- A 1998 survey by the FTC.[7]
- A 1999 survey conducted by Professor Mary Culnan, which resulted in a second FTC report.[8]
- A 2000 survey by the FTC.[9]
- A 2001 survey undertaken by The Progress & Freedom Foundation and Ernst & Young, which replicated the FTC's 2000 methodology.[10]

---

[7] Federal Trade Commission, Privacy Online: A Report to Congress (June 1998) ("FTC 1998 Report") (available at http://www.ftc.gov/reports/privacy3/index.htm).

[8] Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (June 1999) (available at http://www.msb.edu/faculty/culnanm/gippshome.html). The results of this study of the top 100 Web sites are reported in Online Privacy Alliance, Privacy and the Top 100 Sites: Report to the Federal Trade Commission (June 1999) (available at <http://www/ftc.gov/os/1999/9907/index.htm#13).

[9] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress (May 2000) ("FTC 2000 Report") (available at http://ftc.gov/reports/privacy2000/privacy2000text.pdf).

The period covered by the studies saw general improvement in the privacy practices of commercial web sites. The results are illustrative of the kind of information that should be collected. They also show that the questions being asked a decade ago are much the same as those being considered now.

The most recent (2001) survey found that relative to the 2000 survey:

- Web sites were collecting less information.
- Fewer web sites were using third-party cookies.
- Privacy notices were more prevalent, more prominent, and more complete.
- Consumers had more opportunities to choose how personally identifiable information (PII) was used.
- More sites were offering opt-in and fewer opt-out.
- More sites were offering a combination of fair information practice elements.
- Seal programs were growing relatively slowly.

The 2001 survey found that 80 percent of the most popular domains implemented notice, choice, and security—up from 63 percent in the 2000 survey—and 48 percent of a random sample (which included much smaller sites) implemented those three practices—up from 27 percent a year earlier.[11]

No one knows whether the period since 2001 saw further improvement in privacy practices or what commercial website practices are today. The Department needs to have updated information in order to make informed recommendations.

III. The Need for Cost-Benefit Analysis

---

[10] William F. Adkinson, Jr., Jeffrey A. Eisenach, and Thomas M. Lenard, Privacy Online: A Report on the Information Practices and Policies of Commercial Websites (March 2002) (available at http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf).

[11] The 2001 survey, while the same as the 2000 survey in all other respects, did not address access practices. The FTC's 2000 Report stated that "the Commission believes that Access presents unique implementation issues … including what categories of data must be made available; the costs and benefits of providing access; and how to ensure adequate authentication." FTC 2000 Report at 17.

The debate about privacy has engendered strong opinions, but relatively little data or analysis. The Green Paper suggests that its goal is "to establish a baseline commercial data privacy framework to afford protection for consumers, and to clarify the U.S. approach to commercial data privacy—all without compromising the current framework's ability to accommodate customer service innovation, and appropriate uses of new technologies."[12]

The Department needs to acknowledge the tradeoffs inherent in greater privacy protections and carefully evaluate the benefits and costs of alternative privacy regimes (including the status quo) to determine which will best serve the interests of consumers. Each element of the proposal will have benefits and costs. Because the Green Paper presents no data on either benefits or costs, it is impossible to know whether the proposed framework, or any or its elements, will improve or reduce consumer welfare.

The commercial use of information online produces a range of benefits, including advertising targeted to consumers' interests, advertising-supported services, such as free email, search engines, fraud detection, and a reduction in other threats such as malware and phishing.[13] More privacy, in the current context, means less information available for the marketplace and therefore potentially fewer benefits to consumers. Indeed, the proposed framework is generally designed to make it easier for consumers to limit the amount of information firms collect and retain. The principal purpose of cost-benefit analysis is to make this tradeoff explicit and evaluate it.

On the cost side, a recent study by Goldfarb and Tucker found that the European Privacy Directive reduced the effectiveness of online advertising by an estimated 65 percent.[14] This means that privacy protections make advertising less useful to consumers and less valuable to advertisers. Advertisers will pay less for less-effective ads, which decreases the resources

---

[12] Green Paper at 2-3.

[13] The benefits of information are laid out in detail in Thomas M. Lenard and Paul H. Rubin, "In Defense of Data: Information and the Costs of Privacy," Policy & Internet, Vol. 2: Iss. 1, Article 7 (2010), 149-183.

[14] Avi Goldfarb and Catherine Tucker, "Privacy Regulation and Online Advertising," Management Science, vol. 57, no. 1, January 2011, at 57-71.

available to support online content. The authors found this was particularly so for more general (less product-specific) websites, such as newspapers.

These results are reinforced by a study by Howard Beales, which shows prices for behaviorally targeted advertising are more than twice the prices for untargeted ads.[15] Again, this result stems from the greater value that consumers receive from ads targeted to their interest, which increases the revenues generated to support content.

Although only a few empirical studies of the costs of privacy regulation exist, even less information is available on benefits. There are two related ways to think about the benefits of privacy. First, the benefits of privacy are the reduced harms associated with too much information being available or misused. A recent FTC Staff Report rejects the harm-based approach because:

> it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.' Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations. For instance, the Commission's online behavioral advertising work has highlighted consumers' discomfort with the tracking of their online searches and browsing activities, which they believe to be private."[16]

Harm can include all those things—whatever consumers think is harmful. Physical or economic injury would appear to be easier to quantify than some of the other forms of harm, but neither the Green Paper nor the FTC Staff Report contains data on any harm, however defined. The reason that demonstrating and, to the extent feasible, quantifying harm is important is that it can be the

---

[15] Howard Beales, "The Value of Behavioral Targeting," available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

[16] "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for businesses and Policymakers," Preliminary FTC Staff Report, at 20-21, available at http://ftc.gov/os/2010/12/101201privacyreport.pdf.

starting point for assessing benefits, which are the reduced harms associated with increased privacy protection.

The other way to approach benefits is by measuring how much consumers are willing to pay for more privacy. Economists usually prefer to base consumers' willingness to pay on observed market behavior, because how people behave when confronted with actual market choices seems to better reflect their real preferences than do responses to survey questionnaires or behavior observed in experiments. The widespread use of free services such as email and online news subscriptions suggests that people routinely give up some information about themselves in return for access to content, more useful advertising, and other services, although the transaction is indirect. This "revealed preference" approach—preference revealed by actual market behavior—suggests that consumers' willingness to pay for privacy is small, or at least smaller than the value they receive.

Acquisti, John and Loewenstein try to estimate the value of privacy with a series of experiments and surveys. They find that the results are greatly affected by factors such as how much money or privacy participants are granted when beginning the experiment and the way in which choices are presented to participants. In their experiments, "the answer to questions such as 'What is privacy worth?' … depend [on] how you ask…."[17] Their findings "cast doubt on the ability to infer consumers' exact evaluations of personal privacy from market experiments."[18] This seems to be the case, at least with respect to the experiments they present. Their conclusion that "this research raises doubts about individuals' abilities to rationally navigate issues of privacy"[19] seems to be premature, however.

---

[17] Alessandro, Leslie John, and George Loewenstein, "What is Privacy Worth," at 33, available at http://www.futureofprivacy.org/wp-content/uploads/2010/09/privacy-worth-acquisti-FPF.pdf

[18] Acquisti et al at 32.

[19] Acquisti et al at 33

Most if not all of the Green Paper's recommendations will involve tradeoffs. For example, one of the FIPPs involves "enhancing transparency to better inform choices."[20] The Green Paper points to the fact that "lengthy and complex disclosure or notice policies may fail to inform; simplicity and clarity are generally preferable and may well be necessary to ensure transparency."[21] Transparency and simplicity are worthwhile goals, but are unlikely to be costless, because the use of information is often complicated. Simplifying privacy notices would not just affect the notices but would likely also affect the ways companies use data, which would be constrained to conform to the notice standards. Thus, implementing transparency and simplicity requirements could reduce benefits to consumers and impose costs on businesses. Whether this is an important issue or not is unclear, but it needs to be analyzed.

The Green Paper proposes that companies should incorporate "purpose specifications" and "use limitations" in their notices and privacy practices. However, the Green Paper also notes that "[t]he current privacy policy framework has created an environment in which 'creative re-use of existing information' has led to innovations."[22] The Green Paper provides a useful hypothetical that illustrates the potential tradeoff:

> Suppose that company executives have grown concerned with security threats against its network equipment and customers' computers. The Chief Executive Officer (CEO) approves a proposal to provide … Internet usage records … to in-house researchers, so that they can analyze network traffic and develop security countermeasures. This use of personal information has the clear potential to bring privacy and security benefits to the ISP and its customers. The proposed use, however, would also be contrary to the ISP's specified purposes for collecting the information in the first place.[23]

Requiring consumers to be afforded the opportunity to consent to such "new uses" of data may mitigate against their use, because of the strong tendency of consumers to stay with the

---

[20] Green Paper at 31.

[21] Green Paper at 31.

[22] Green Paper at 38.

[23] Green Paper at 39.

default.[24] And there are likely to be new commercial uses (unrelated to security) that also might benefit consumers. It is important to carefully weigh the privacy benefits against the costs of not being able to use data for new uses. Obviously, new uses are not going to be known at the time a privacy rule or practice is being implemented. Innovations foregone are, by their nature, difficult to address.

The Green Paper also recommends consideration of a national security breach notification law. A 2005 study by Lenard and Rubin suggested that such measures are dubious on cost-benefit grounds:[25]

- The expected benefits to consumers of a notification requirement were extremely small—on the order of $7.50 to $10 per individual whose data had been compromised. This was because (1) most cases of identity theft did not involve an online security breach; (2) only a very small percentage of individuals compromised by security breaches—perhaps 2 percent—actually became victims of a fraud; (3) most of these were victims of fraudulent charges on their existing credit accounts, for which they had very limited liability, rather than victims of true identity theft; and, (4) even a well-designed notification program would only eliminate about 10-20 percent of the expected costs.
- Because a notification mandate was found to be dubious on benefit-cost grounds, it should be applied carefully if at all. Firms should be able to determine which customers are most at risk and tailor notice to those individuals, perhaps in cooperation with the FTC.
- Federal preemption of state notification laws will reduce compliance costs and improve the benefit-cost balance.

The Lenard-Rubin study is now more than five years old. The Department should undertake a new analysis before finalizing its recommendations.

---

[24] Lenard and Rubin *supra* note 13 at 174.

[25] Thomas M. Lenard and Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," July 2005, available at http://www.techpolicyinstitute.org/files/11.pdf

IV. Conclusion

The DOC Green Paper is in many respects a thoughtful discussion of privacy issues. However, it is seriously deficient as a foundation for new policy recommendations because it contains no systematic data on current privacy practices on the part of either firms or consumers, and no systematic analysis of the benefits or costs of alternative privacy regimes. This violates the spirit, if not the letter, of President Obama's recent executive order on regulation, which stresses the need to evaluate both benefits and costs. Otherwise, there is no way of knowing whether a particular regulatory action will improve or reduce consumer welfare.

The privacy debate is taking place in an empirical vacuum. The Department could make a real contribution if its proposed Privacy Policy Office becomes a locus for data collection and serious privacy-related research.