TECHNOLOGY POLICY INSTITUTE
Studying the Global Information Economy

April 2, 2012

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

Re: Docket No. 120214135-2135-01

Dear Mr. Burstein:

I hereby submit the attached comments in response to the NTIA's March 5, 2012 Request for Public Comments, "Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct."

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

In the Matter of:	)	
	)	
Multistakeholder Process To Develop	)	
Consumer Data Privacy Codes of	)	**Docket No. 120214135-2135-01**
Conduct	)	
	)	

COMMENTS OF

Thomas M. Lenard, Ph.D.
President & Senior Fellow
Technology Policy Institute
1099 New York Ave., NW
Suite 520
Washington, DC 20001
202-828-4405

I. Introduction

In February, the Executive Office of the President released a "Privacy and Innovation Blueprint", which proposes a Consumer Privacy Bill of Rights for personal data used for commercial purposes and a multistakeholder (MSH) process to develop legally enforceable codes of conduct to implement the Bill of Rights.[1] The National Telecommunications and Information Administration (NTIA) has been tasked with convening the MSH process. NTIA is requesting comments both on the procedures the MSH process should follow and the substantive issues it should consider.

The NTIA MSH process falls somewhere between regulation and self-regulation. A regulation would be generally applicable and not voluntary. A code of conduct developed by a self-regulatory body would typically not be legally enforceable. The code developed through the NTIA MSH process will, for those who adopt it, be enforceable by the Federal Trade Commission. Once a code is endorsed by the NTIA MSH process, there will be considerable pressure for many firms to adopt it.

Whatever the procedures NTIA may adopt for obtaining stakeholder input, however, it is not possible for the vast majority of stakeholders to be directly represented. This is because stakeholders include everyone who uses (or may in the future use) the Internet. As the overseer of the process, NTIA needs to assure that their interests are represented too. It can do this by building into the process an analysis component that assesses the costs and benefits, to whomever they accrue, of code provisions under consideration.

II. The Need for Cost-Benefit Analysis

The commercial use of information online produces a range of benefits, including advertising-supported services, such as free email, more accurate search engines, advertising

[1] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, February 2012, available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

targeted to consumers' interests, fraud detection, and a reduction in other threats such as malware and phishing.[2] More privacy, in the current context, means less information available for the marketplace and therefore potentially fewer benefits to consumers. The principal purpose of cost-benefit analysis is to make this tradeoff explicit and evaluate it.[3]

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 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….[4]

While the DOC is not formally proposing a regulation, the code of conduct produced by the MSH process will be similar to agency guidance. Significant policy and guidance documents are subject to review under Executive Order 12866 by OMB's Office of Information and Regulatory Affairs.[5]

Elements of a cost-benefit analysis should include:

- Collecting current data on online privacy and data management practices.

---

[2] 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: Issue 1, Article 7 (2010), 149-183.

[3] In comments on the 2010 Department of Commerce Green Paper, I emphasized the need for assessing benefits and costs before arriving at final recommendations. Such an assessment has not yet been undertaken. See http://www.techpolicyinstitute.org/files/lenard_docprivacycomments1.pdf

[4] 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>

[5] See OMB Memorandum M-09-13, March 4, 2009 at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-13.pdf

- Producing evidence showing that current practices are harming consumers. A new privacy code of conduct will only produce benefits to the extent it alleviates identified harms.
- Reviewing what is known 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 available.
- Producing sufficient evidence of a reasonable expectation that the benefits of a code of conduct are greater than the costs. Otherwise, the code should not be adopted.

A potential cost of a privacy code of conduct is a reduction in the value of online advertising, as indicated by a recent study that found that the current European Privacy Directive reduced online advertising effectiveness by an estimated 65 percent.[6] This means that the privacy protections in the Directive make advertising less useful to consumers and less valuable to advertisers. Advertisers will pay less for less-effective ads, which decreases the resources available to support online content. The authors found advertising effectiveness was reduced particularly for more general (less product-specific) websites, such as newspapers.

These results are reinforced by a study by former FTC Bureau of Consumer Protection Director Howard Beales, which shows prices for behaviorally targeted advertising are more than twice the prices for untargeted ads.[7] 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

---

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

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

privacy. First, the benefits of privacy are the reduced harms associated with too much information being available or misused. Harm can include whatever consumers think is harmful, including but not limited to physical or economic injury. The reason that demonstrating and, to the extent feasible, quantifying harm is important is that it can be the 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 in return for their information.

Most if not all of the code of conduct will involve tradeoffs. For example, NTIA is considering implementing the Transparency right in the privacy notices for mobile applications.[8] Transparency is a worthwhile goal, not just for mobile apps but generally. It is unlikely to be costless, however, because the use of information is often complicated. Simplifying privacy notices is, as the NTIA notes, especially challenging for small screens. A transparency standard might 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 requirements could reduce benefits to consumers and impose costs on businesses. The importance of this issue is unclear, but it needs to be analyzed.

[8] The Transparency right states, "Consumers have a right to easily understandable and accessible information about privacy and security practices." See "Privacy and Innovation Blueprint," at 9.

III. Potential for Anticompetitive Behavior

All aspects of the MSH process remain to be specified, including how stakeholders can be involved and how consensus is defined and achieved. Because this process will be driven by stakeholders, it needs to be sensitive to the potential for anticompetitive behavior. For example:

- Large businesses and trade associations will be able to devote more resources to the process than small entities. Privacy standards often impose disproportionate costs on small entities. Procedures for achieving consensus should take this into consideration.
- New entrants into the Internet space comprise an important group of stakeholders that can't be directly represented because they don't yet exist. A process that is dominated by incumbents may tend to raise the costs of entry and inhibit innovation. Procedures for achieving consensus should guard against such effects, which reduce innovation and lock in current technology.
- Organizations and Internet ecosystems use information in different ways. Some firms are more vertically integrated than others. Some platforms are more open, some more closed. A privacy code should be neutral with respect to business model and organizational structure. This diversity should be reflected in the procedures for achieving consensus.
- Firms collect and process information using different technologies. A privacy code should be technology neutral. This should also be reflected in the procedures for achieving consensus.

IV. Conclusion

The code of conduct developed by the MSH process will apply to many more consumers and firms than can be directly involved in the process. Therefore, the code should be analyzed in much the same way as a regulation in order to assure that the code produces net benefits for consumers. Indeed, because the code is similar to agency guidance, it is arguably subject to review under E.O.12866.

In addition, because the MSH process will be dominated by stakeholders who have their own strategic interests, NTIA should be especially sensitive to the possibility that the code will favor some firms, business models, or technologies. Procedures for achieving consensus should guard against this.