USCIB
UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

January 28, 2011

National Telecommunications and Information
Administration, U.S. Department of Commerce
1401 Constitution Avenue, NW. Room 4725
Washington, DC 20230
Via electronic filing: privacynoi2010@ntia.doc.gov

Re: Comments on the Department of Commerce Internet Policy Task Force Report on Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

The United States Council for International Business (USCIB) welcomes the Department of Commerce Green Paper, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework," and the opportunity to provide further comments. The Dynamic Policy Framework presented by the Department of Commerce in its recent Green Paper presents a new approach to U.S. privacy informed by business, consumers and government, and while the objectives set forth in the Commerce paper are laudable, as with all things of such enormous impact and complexity, the devil is in the details.

The Role of Expanded FIPPS

Fair Information Practice Principles (FIPPs), as a concept, has already long been established in the U.S., formed the basis of the OECD Guidelines, and has been adopted by many businesses in the development of their privacy practices. A robust privacy regime has developed in the U.S., focused on protection from particular harm. In the privacy arena, it works because businesses share concerns about protecting privacy and can work to implement programs that are market-driven and reflect specific issues of concern.

The Framework alludes to "enhanced" FIPPs to take into account the greater complexities of today's interactions. However, the implications of enhanced FIPPs on their impact on the economy are not clear and might even result in harm. While some commentators in the consultation leading to the Green Paper supported the need for a better baseline, others indicated the need to consider the implications of new technologies, business models and data flows. All of these concerns should be the basis of discussion rather than new requirements that are inconsistent with how business is conducted in the U.S. For example aspects of purpose and use limitations provide a different approach than currently exists in the U.S. and may create requirements that are not consistent with existing business practices that do not pose privacy risks. Alignment of information practices with consumer expectations is better addressed by ensuring that practices are compatible with the notices provided, the purposes for which the data were collected or other reasonable consumer expectations. Unfortunately, the Framework also implies that there is development of a consensus on expanded FIPPs that should coincide with codification of approaches.

1212 Avenue of the Americas
New York, NY 10036-1689
212.354.4480 tel
212.575.0327 fax
www.uscib.org

While regulation or legislation may be well-intended, it may well lead to unintended consequences. Discussions on evolving legal and policy frameworks for commercial privacy should be informed by the President's call for reducing regulatory burdens on industry and innovation. Such an approach should be thought about in terms of practicability in the U.S. of implementation, impact on innovation and business processes, not to mention effectiveness of delivering consumer protection. Our experience in the U.S. has shown that we should continue to address actual harms, rather than merely seek to codify a formulaic recitation and expansion of principles that were meant to and have informed our economy at a high level. This would also allow us to assure that they have the requisite flexibility as well as credibility to address a broad variety of data flows, actors, situations and responsibilities. Flexibility, and the fact that there is 'no one size fits all' in application, are all legitimate arguments recognized in the paper, but are perhaps glossed over in how difficult they are to achieve in the right balance.

Transparency

While Privacy Impact Assessments (PIAs) may be a useful tool for some business in the context of the development of certain new products and services, we disagree that they should be mandated or be seen as a transparency tool externally. In order for PIAs to be frank and truly helpful, companies should not be required to disclose them. They often contain confidential strategy, business plans or other information that is not intended for public consumption. PIAs should be best understood as a way in which companies internally can understand and manage their own risk, but they are just one tool among many that can be tailored to meet this specific need within a product, service or business process privacy review. The Green Paper questions what elements are contained in a meaningful PIA in the commercial context and who should define these elements. Precisely because commercial contexts are so varying by company size, business model, and business sector, there is no single set of elements that can currently apply to all situations and they must be defined by the company using them. While many sophisticated and large organizations do conduct PIAs to manage some of their privacy goals, they are not the only way to ensure appropriate data protection, and should not be mandated and certainly should not be required to be made public. Technology, platform, and business model neutrality must be a cornerstone to any federal framework.

Establishment of a Privacy Policy Office

A centralized privacy office within the Administration could coordinate policy discussions. There are many voices in the debate on privacy that represent "regulatory" and privacy advocacy positions, and there is a critical need to establish a leading voice that understands both the importance of protecting consumer privacy and the significant cost to business of legislating or regulating too quickly or too strictly in an already harsh economic climate. To the extent such an office would be useful and can be funded in keeping with the desire to reduce regulatory burdens and shrink government, the focus should be on assisting U.S. businesses in addressing barriers to trade from foreign privacy laws that purport to restrict the transfer of data to the U.S. Furthermore, the important, distinct role of regulatory agencies in this area must be maintained, including in the context of interfacing with foreign privacy offices, many of which are independent privacy regulators. In addition, multiple enforcement mechanisms, especially private rights of action, pose the danger of inconsistent and burdensome actions.

Global Interoperability

The Green Paper correctly notes that it is time for the U.S. government to "renew [its] commitment to leadership in the global privacy policy debate." However, that leadership should be used to promote the U.S. view that data should be allowed to flow among countries, rather than seeking to adopt a more EU-like approach, which would lead to further restrictions of movement of data around the world. The U.S. should promote development of a international privacy infrastructure that not only increases cooperation among privacy authorities around the world for purposes of enforcement and creation of seamless cross-border compliance solutions, but that also supports mutual recognition in participating countries' national legal frameworks. The Framework references the need for greater interoperability across jurisdictions which is a shared objective, but one which is best accomplished by understanding how practices can work together. As was noted in the foundation elements of the document, the U.S. has been exceptionally successful in using and benefiting from internet services and commerce. Part of that reason is that the U.S. understands the need to foster innovation and avoid needless burdens. As the EU looks to revise its privacy Directive it has taken a new and more target focus on "effective regulation" and concepts of accountability with less favor being shown towards the bureaucratic concepts of registration and filing, if no clear benefit can be seen to be gained from them. While the Framework does not indicate an attempt to meet adequacy requirements, it does seem to be motivated towards harmonization. We believe that there is every benefit to consider alternative approaches that have worked in other jurisdictions, but would caution against being driven too much by any concept of harmonization.

We look forward to a continued dialogue with the Department of Commerce on the development of a privacy framework that balances flexibility and global data flows while enhancing the effectiveness of consumer privacy protection and trust.

Sincerely,

Peter M. Robinson
President and CEO