Before the
DEPARTMENT OF COMMERCE
Internet Policy Task Force

In the Matter of	)	
Information Privacy and	)	Docket No. 100402174-0175-01
Innovation in the Internet Economy	)	

COMMENTS OF TECHAMERICA

Chris Wilson, Esq.
TECHAMERICA
601 Pennsylvania Ave, NW
North Building, Suite 600
Washington, D.C. 20004
(202) 682-4451

June 14, 2010

TechAmerica hereby submits these comments to the Department of Commerce ("Department"). TechAmerica's members have a vested interest in the success and future of the Internet and TechAmerica is pleased to be able to file comments on their behalf in this proceeding.[1]

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association (AeA), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics and Information Association (GEIA).

TechAmerica's members include: manufacturers and suppliers of broadband networks and equipment; consumer electronics companies; ICT hardware companies; software and application providers; systems integrators; Internet and e-commerce companies; Internet service providers; information technology government contractors; and information technology consulting and sourcing companies.

TechAmerica welcomes this opportunity to provide the Department's Internet Policy Task Force with a viewpoint shared by such a diverse membership.

The U.S. Privacy Framework

TechAmerica is pleased to provide the Department with some important concepts that its Internet Policy Task Force must consider in its deliberations and its external advocacy.

First, any privacy regulatory framework adopted in the United States must be technologically neutral. Technology neutrality ensures that any prospective regulatory model will provide sufficient flexibility to allow Internet-related technology companies the ability to innovate and respond effectively to consumer needs into the future. In that vein, TechAmerica does not believe there is a "one-size-fits-all" approach to privacy policy. Second, we understand that "customary notice and choice" may be outdated in certain contexts, but TechAmerica believes that notice and choice should still maintain a foothold in any comprehensive privacy policy. In addition, TechAmerica believes that additional privacy models can and should be considered to complement the traditional notice and choice system. Indeed, as Web-based services become more interactive and information-intensive, some form of a "use-based" model, for example, could very well be applicable. Simply put, TechAmerica recognizes that the dynamic and ever-changing Internet economy and infrastructure requires an equally flexible and dynamic privacy regime.

Further, as the Department reviews various privacy models and their efficacy in the future, it should strongly consider, and encourage, two core guiding privacy principles currently at work. The first, "accountability," is a well-established principle of data protection, having longstanding roots in many of the privacy and security components comprising global trust legislation. The second, "privacy by design,"

asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation.

"Accountability" requires an organization to make responsible, disciplined decisions regarding privacy and security. The accountable organization complies with applicable laws and then takes the further step of implementing a program ensuring the privacy and protection of data based on an assessment of risks to individuals. For example, companies can demonstrate accountability by innovating to build trust, such as by developing and selling more secure and privacy-enhancing component parts that have been vetted through processes such as development lifecycles that have privacy and security integrated as foundational elements. Several companies are currently committing significant resources to "being accountable" in this way now.

With regard to "privacy by design," the principle should encourage the implementation of accountability processes in the development of technologies. To achieve its objective, the principle should avoid mandatory compliance to detailed standards, or mandatory third party detailed product reviews, as this would decrease time to market and increase product costs. This would be particularly the case when it is unclear whether third parties would have the appropriate resources or skill sets to effectively review the technology. Instead, a "privacy by design" accountability model should focus on making certain privacy is included as a foundational component of the product and service development process.

TechAmerica requests that the Department, in its report, encourage organizations to take steps towards accountability and to ensure that privacy is included as a principle in product and service development processes.

International Privacy Laws and Regulations

As the Department is well aware, there are a variety of foreign laws governing how companies collect, use, and disseminate consumer data. Unfortunately, this matrix of laws has served as an unnecessary, if not intentional, barrier to effective trade in the digital economy. For example, the European Union's data privacy laws, in contrast to the U.S.'s more flexible standards, have proven to be not only burdensome in compliance but also inefficient in implementation.

For example, as defined by the European Data Protection Directive 1995, "personal data" is data that relates to or can identify a living individual. This threshold for protection, based on mere identity and rooted in the jurisdiction of "collection," contrasts sharply with the privacy laws of some other countries, such as in the U.S., where data use and the risks attributable to misuse is the basis for sector-specific regulations.

To be sure, however, TechAmerica and its member companies applaud the Department's efforts to mitigate the impact of the EU privacy laws, especially the Department's role in negotiating the U.S.-EU Safe Harbor Framework. This Framework has facilitated the rapid development of a global Internet economy.

In addition to the U.S.-EU Safe Harbor Framework, the APEC Privacy Framework has been extremely helpful for U.S. technology companies seeking to do business globally. TechAmerica commends the leadership of the Department on the

development of the APEC Cross Border Privacy Rules (CBPR). Since the APEC Privacy Framework was endorsed by APEC Ministers in 2005, the Department, in conjunction with other U.S. agencies, has been instrumental in working with its counterparts across APEC economies on a series of Data Privacy Pathfinder projects to develop a system in the APEC region that ensures accountable cross-border flows of personal information for the protection of consumers while facilitating business access to the benefits of electronic commerce. TechAmerica member companies are of the view that the APEC Privacy Framework and the Data Privacy Pathfinder projects represent an important step forward in privacy protection in the 21 APEC economies in which new and flexible approaches to accountability and compliance are envisioned.

Further, notably, we are thankful that the Department has striven to include opportunities for the business community to engage and provide input throughout the APEC CBPR development process. This collaborative effort has been essential given the pace of innovation in electronic commerce. The Pathfinder projects enable a system that allows businesses to create their own CBPRs and consumers to rely upon 'accountability agents,' as well as regulators, in the APEC region to make sure businesses are held accountable to their privacy promises. This self-regulatory "trustmark" model has proven effective in a number of economies to date. As the APEC Privacy Framework demonstrated, a voluntary set of common and broadly-applicable principles can coincide with self-regulation and a risk-based approach to compliance obligations and enforcement.

With the APEC success in mind, TechAmerica believes a strong consistent global framework is needed in order for the digital economy to truly flourish. Without

such a harmonized framework, technology companies will be forced to make difficult decisions as to whether or not to do business in certain countries for fear of being held civilly or even criminally liable for actions that would otherwise be lawful in the U.S. and elsewhere. Such uncertainty would inevitably lead to less investment and, subsequently, less economic growth. Considering how interconnected the global economy already is, the repercussions of such choices will be felt throughout the world.

This global interconnection is especially true with regard to cloud computing, for example. As cloud computing continues to grow, so too will the amount of data crossing national borders. If divergent claims to jurisdiction over user content remain, then it becomes quite difficult for providers to manage their legal obligations and their global technology operations while at the same time protect their consumers.

The Role of Government/Commerce Department

The Department, with its history of working with the global community on privacy matters, is uniquely positioned to lead the way in developing a consistent privacy model. TechAmerica stands ready to assist the Department as it moves forward in this regard, especially as the U.S. hosts APEC next year.

Further, one factor often cited by data protection regulators as a weak point internationally of the U.S. privacy regime is the lack of a central U.S. authority on privacy issues. As the Department gathers input on whether or how to strengthen our own regime in the U.S., it would be helpful for U.S. positioning on privacy to receive greater and more focused representation internationally by the U.S. government. International coordination will continue to be key to free flows of information and deployment of new and innovative services. Whether the U.S. chooses to develop new

broadly-applicable privacy rules or revisits the application and scope of existing privacy laws, there are four key principles that should help guide this effort:

- **Flexible Compliance Options** – Continue to favor self-regulatory approaches, but where rules are deemed necessary, enable authorities to approve appropriate industry and NGO-developed compliance contracts, codes and procedures;
- **Relevant Risks** – Where rules are necessary, they must focus on the risk attributable to misuse of certain types of data in setting the level of protection for that data;
- **Consistent Implementation** – Seek a consistent approach to principles that put the onus on data users to take accountability – not added protections that frustrate the possibility of cross-border compliance;
- **Consultation** – Industry understands that its role in protecting privacy supports its mission to achieve and retain customers, and thus, industry consultation at all levels of this continuing dialogue will improve compliance and enforcement.

Further coordination among governmental and non-governmental entities domestically is also an area where the Department can be helpful. For example, the Federal Government's Information Security and Privacy Advisory Board and the President's National Security Telecommunications Advisory Committee each released reports last year outlining important information security and management issues deserving of fuller consideration, including how to treat metadata, cookies, and other tags that may be shared. These efforts, as well as the efforts of non-governmental

entities, such as the Kantara Initiative, and other governmental efforts, such as the White House's National Strategy for Secure Online Transactions, illustrate how scattered and varied the review of information security and privacy practices is throughout the country. As much as possible, these efforts should be coordinated and the Department should assist in this regard.

Conclusion

TechAmerica thanks the Department for creating its Internet Policy Task Force. A committed and focused effort by the Department with regard to the development of the digital economy is welcomed and appreciated. The Department can and must play a key role in developing a unified privacy regime. Consumer privacy protection will require a multi-faceted solution that includes industry commitments and government involvement. To be sure, privacy is vitally important to not just consumers, but to Internet technology companies as well. Entire business models are built on the trust established between a company and its customers. Industry principles such as transparency, user control, and security in Internet services should and must remain at the foundation of any privacy model going forward. TechAmerica looks forward to working with the Department in the months and years ahead as it plays a role in achieving a comprehensive and flexible privacy plan.

---

[1] *Information Privacy and Innovation in the Internet Economy*, Notice of Inquiry, 75 FED. REG. 21226 (April 23, 2010).