



UNITED STATES COUNCIL FOR INTERNATIONAL BUSINESS

Peter M. Robinson
President & CEO

June 14, 2010

National Telecommunications and Information Administration
US Department of Commerce
Room 4725
1401 Constitution Avenue NW
Washington, D.C. 20230

Re: Docket No. 100402174-0175-01

Dear Sirs and Madams,

We are pleased to provide comments in response to the Notice of Inquiry on Privacy and Innovation. Given our specific mandate and expertise, we have focused our remarks on the portions of the NOI pertaining to the global privacy system and international cooperation to protect privacy.

The United States Council for International Business (USCIB) promotes open markets, competitiveness and innovation, sustainable development and corporate responsibility, supported by international engagement and prudent regulation. Its members include top U.S.-based global companies and professional services firms from every sector of our economy, with operations in every region of the world. With a unique global network encompassing the International Chamber of Commerce, the International Organization of Employers and the Business and Industry Advisory Committee to the OECD, USCIB provides business views to policy makers and regulatory authorities worldwide, and works to facilitate international trade and investment.

USCIB's ICT Policy Committee represents businesses from diverse industry sectors. The committee advocates for sound international policy frameworks, characterized by free and fair competition, targeted government intervention limited to addressing clearly defined market failures, free information flows and a user orientation, that ensure the continued growth of ICTs and extend their benefits around the world. The committee also increases awareness of the potential impact of policies, laws, and regulations related to ICTs and e-business. USCIB and its members work to enhance trust and promote privacy while enabling global information flows by developing solutions to possible restrictions on transborder data flows through the ICC model contracts and other tools, working on the implementation of the APEC Privacy Framework, active engagement on the dialogue around the review of the OECD Privacy Guidelines and general policy debates, providing input on ISO privacy initiatives and continuing to monitor developments worldwide. We promote self-regulation and the application of existing global privacy guidelines to ensure responsible and accountable implementation of new technologies and applications such as radio-frequency identification (RFID) and social networking. We promote a global culture of cyber-security through ICC and BIAC, and in regional fora. USCIB has a long history of working through the ICC to communicate business views to the EU, and recently concluded a new model contract for controller to processor transfers.

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

Global Business Leadership as the U.S. Affiliate of:
International Chamber of Commerce (ICC)
International Organization of Employers (IOE)
Business and Industry Advisory Committee (BIAC) to the OECD
ATA Carnet System

USCIB encourages the Department of Commerce to take a proactive role promoting the US privacy regime as a part of a global privacy system that works for U.S. companies. As the Department gathers input on our own regime, 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. In that regard, we also welcome continued involvement by other governmental agencies and appreciate the international efforts of all USG agencies over the past several years.

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. We hope to continue our dialogue on these issues with the Department and the Internet Policy Task Force on the NOI responses.

I. Impact of diverse privacy laws and obstacles to cross border data transfers

The sheer complexity associated with understanding and implementing policies and practices that are compliant with multiple laws, regulations and case law across multiple countries, languages and cultures increase the difficulty and cost of doing business internationally. Conflicting privacy and data protection laws across different countries, and the impact of laws and regulations in other areas that conflict with domestic or foreign privacy laws further hamper international trade and investment and the general economic growth they contribute towards. Prescriptive international standards make it difficult to create a global company wide solution without adopting the most restrictive standard. Currently, companies employ a variety of mechanisms, discussed below, to try to overcome these obstacles.

Variations in laws and compliance requirements can result from:

- technical specificity (Italian Data Protection law specifies an 8 digit alpha numeric passcode),
- compliance architecture (the need in some countries for a local data protection officer, creating a compliance position that replicates global or regional staffing)
- variations in definitions (what is sensitive information)
- variation in substance and bureaucratic processes (recent court decision in Dusseldorf which questions whether safe harbor certification provides evidence of compliance with legal requirements).

Given the borderless nature of the Internet, it is often difficult to determine the location of a person or entity, and thus to establish jurisdiction or applicable law. Disputes often arise as a result of different interpretations. Moreover, some countries are aggressive in claiming jurisdiction, subjecting companies to laws they were not expecting. For example, the EU Article 29 Working Party has issued opinions that assert that the use of cookies, commonly placed on end user computers for a range of purposes, is considered 'equipment located in the EU' to establish jurisdiction. Companies that have no physical presence and are not necessarily knowingly doing business within the EU do not expect to be subject to EU jurisdiction or have the Directive apply over websites find that they are.

Jurisdiction also comes into play with the complexity of information flows. For example, US-based companies that have posted privacy policies are subject to enforcement by their U.S. regulators. If they use a service provider in the EU they are also subject to EU Member State laws. So, to the extent that they have a follow-the-sun service model, they may also be subject to the procedural and substantive aspects of the laws of the various support locations that may be involved. Further complexity is involved for companies providing third party services, who may also have to consider issues of multiple sectors which may have varying or additional restrictions. Another layer of complexity comes from legal and investigatory issues which might not be purely related to privacy; these include whistle-blowing and conflicts between SOX and EU privacy law as well as discovery requests from the US to EU or other countries related to non-US citizens that conflict with local law. Discovery is especially relevant as the discovery regimes in the EU are much more limited; thus, the more expansive discovery rights under US law are difficult for EU DPAs to understand and recognize.

As global information flows expand and remote services such as those facilitated by cloud computing expand, the question of jurisdiction and its resolution will become even more important. Cloud services may rely upon multiple data centers with geographical spread. They will of necessity require fluid ability to move information for optimization, security and business continuity/disaster recovery. Actual and constructive limitations on such transfers, assuming that systems are in place to assure compliance with obligations, are artificial rather than substantive or effective. More and more consolidated data centers are accessed globally – making the notion of location of data less relevant over time.

Many laws, either in letter or spirit, favor local storage of information and limitation on access to information based on geography rather than need. They are a vestige of the time the law was developed when information flows were based on EDI and processing was often point to point batch processing. These restrictions may currently require the creation of redundant facilities to meet legal requirements imposing geographical limitations, or the difficulty in creating a system where consent is needed due to the location. How do you deploy a centralized HR system when a handful of employees may object to the transfer of their information? Such a limitation would mean having an automated system supplemented by multiple manual systems.

Economies of scope and scale are achieved through centralization of resources and expertise. They are also optimized when you can take advantage of pools of skilled labor that are either more cost effective or provide the needed geographical dispersion to create a 24 hour service platform (follow-the-sun model). Furthermore cloud computing has created significant cost benefits by allowing individuals, SMEs, companies and governments to access platform, software and hardware in an on demand environment for a tiny fraction of what those resources cost to implement by any one entity. All of these services are predicated on information flows that must be agnostic to location. Location is determined by need and availability. Laws should not be focused on perpetuating requirements of location.

We continue to believe that existing legal and other requirements –including robust enforcement – have been effectively protecting customer privacy interests in the U.S. The U.S. regime has undoubtedly fostered a more robust environment for free information flows and rapid deployment of services than many if not most of its counterparts.

Laws that permit governments to have access to personal information can be an impediment to innovation or global trade and investment. For example, concerns over access to SWIFT data and expanded access under the PATRIOT Act have created a backlash in the EU and British Columbia, Canada respectively, which have led to increased sensitivity to US data transfers and have led to the prohibition of transfers of British Columbia provincial information to the US. Additionally, while India is currently developing rules related to access to information, concerns still exist that companies may be caught between other countries' privacy rights and due process restrictions and Indian requirements related to the production of information. Also, the IRS interest in assuring compliance with US tax laws may become an issue due to other countries' privacy and bank secrecy laws. These requests create situations where companies are the battleground between multiple countries and their customers. There is no positive outcome for the company in this kind of dispute, and yet the company is merely a custodian of the information unable to resolve the equities of the dispute as they may involve the legitimate laws of the counties and the personal interests of the customer.

Despite the necessity of data flows across borders in today's global business environment, businesses face internal compliance and regulatory challenges when trying to do so. Companies must deal with differing or conflicting laws in multiple jurisdictions where data is collected and transferred. In some cases, laws prevent or limit the cross border transfer of data.

Finally, not only are there a plethora of differing and conflicting laws, there are also an abundance of unnecessary requirements. A prime example of such unnecessary requirements are those restricting cross border data flows. These restrictions are a burden on commerce and in some cases reflect an unachievable goal. Moreover, the original rationale for these restrictions are outmoded and unworkable in today's networked world. It is noteworthy that the body of law otherwise generally applicable to electronic

commerce and the internet has been developing successfully without such restrictions. In addition, some of the more recent privacy laws adopted in other countries recognize these cross border restrictions as obstacles and have not included such restrictions in their laws.

II. Business Solutions

In order to address privacy regulations, requirements and cross border restrictions, businesses implement a variety of solutions which must be maintained and managed both in parallel and in combination in order to create a compliance infrastructure. While solutions have been created to permit the continued and vital cross border transfer of personal information, none are perfect and some actually hamper international trade and investment.

The complexities of the global privacy regime, with diverging approaches and different requirements and standards, necessitates that companies establish an internal structure and employ resources specifically to handle privacy issues, which may entail establishing one or more internal data protection officers.

Companies often use contracts when transferring personal information to ensure accountability or to satisfy specific regulatory requirements, though when this mechanism is used to satisfy EU cross border requirements, it has become increasingly complex and difficult to implement.

In the EU, some companies are eligible to self-certify under the Safe Harbor to permit transfers from the EU to the US and are also increasingly relying on binding corporate rules. In addition, companies use master contract architectures, policies and compliance programs, and emerging accountability mechanisms such as private sector Trust- marks and seals.

Companies address jurisdictional conflicts and any resulting conflicting legal and regulatory obligations in several ways. Companies work with local regulators and various global, regional or local bodies that bring economies together, directly or through various intermediaries, to discuss and address policy issues.

III. Conclusion

Core privacy principles are similar around the world, however, based on region and country specific histories and customs, local jurisdictions have developed and applied privacy requirements in different ways. Therefore, any cooperative approaches to privacy must recognize the economic, legal and social contexts of the economies in which they operate. We believe that any workable business solutions must facilitate cross border transfers, permitting companies to transfer and access data globally for business purposes without additional cross border restrictions.

We look forward to a continued dialogue on these issues.

Regards,

A handwritten signature in black ink, appearing to read 'Peter Robinson', written in a cursive style.

Peter Robinson