

**Written Questions of Senator Patrick Leahy,  
Chairman, Senate Committee On The Judiciary  
to Department of Commerce General Counsel Cameron Kerry,  
Hearing On “The Electronic Communications Privacy Act:  
Government Perspectives on Privacy In The Digital Age”**

**CLOUD COMPUTING**

1. Recently, the Commerce Department released a report entitled “Commercial Data Privacy and Innovation in the Internet Economy,” that recommended, among other things, that the Administration address the privacy protections needed for cloud computing.
  - a. How does the current uncertainty in the law about the privacy protections for cloud computing impact American businesses?

**Response:** My testimony and that of private sector representatives before this Committee in September 2010, discussed the benefits of cloud computing for American businesses.<sup>1</sup> As defined by the Commerce Department’s National Institute of Standards and Technology, cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”<sup>2</sup> According to Gartner, Inc., cloud computing was a \$59 billion marketplace in 2009, with revenues predicted to increase to \$150 billion in 2014.<sup>3</sup> It is important to the retooling and regrowing of the domestic economy and to the competitiveness of American businesses globally.

Research on the willingness of both business and consumers to use cloud computing shows trust is an important barrier.<sup>4</sup> As I testified last September, in an April 2010 Harris Interactive poll, 50 percent of the adults surveyed had limited interest in using cloud-based services or applications.<sup>5</sup> Of those surveyed, 81% expressed concerns about the security of those services. And in a 2009

---

<sup>1</sup> See September 2010 Statement of Cameron Kerry, at 9-10, available at <http://judiciary.senate.gov/pdf/10-09-22KerryTestimony.pdf>. See also Statement of Brad Smith, at 4-5, available at <http://judiciary.senate.gov/pdf/10-09-22SmithTestimony.pdf>; Statement of James X. Dempsey, Center for Democracy & Technology, at 6, available at <http://judiciary.senate.gov/pdf/10-09-22DempseyTestimony.pdf>.

<sup>2</sup> NIST Special Publication 800-145 “The NIST Definition of Cloud Computing (Draft)”, available at [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf).

<sup>3</sup> Andrew Hickey, “Cloud Computing Services Market to Near \$150 Billion in 2014, CRN, June 22, 2010, available at <http://www.crn.com/news/channel-programs/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm>.

<sup>4</sup> See Department of Commerce Green Paper, “Commercial Data Privacy and Innovation in the Internet Economy,” at 13, available at [http://www.ntia.doc.gov/reports/2010/IPTF\\_Privacy\\_GreenPaper\\_12162010.pdf](http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf).

<sup>5</sup> Harris Interactive, “Cloud Computing – Are Americans Ready?” (Apr. 21, 2010), available at <http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/80/Default.aspx>.

survey conducted for Microsoft, more than 90 percent of those surveyed expressed reservations about the privacy and security of personal data stored in the cloud.<sup>6</sup> While cloud computing services have experienced robust growth in recent years, customer privacy concerns are one factor that stakeholders will need to further address in the future.

International rules can contribute to uncertainty about the rules applicable to cloud computing because of competing legal requirements and potential restriction on the transfer of data across borders. Two Canadian provinces --, British Columbia and Nova Scotia -- passed laws in 2004 and 2006 respectively, prohibiting personal data held by public sector entities from being stored outside of Canada. The reason given for adopting these laws was unfounded concern that the PATRIOT Act would give the U.S. government undue access to information on Canadian citizens stored in the United States. In comments on the Department of Commerce's Notice of Inquiry on consumer privacy, Salesforce.com cited several foreign country restrictions on transborder data flow, including the British Columbia and Nova Scotia laws. Salesforce.com noted that in addition to the barriers that these laws create, they have fostered the misperception that private and public sector organizations not subject to the laws are prohibited from using U.S.-based cloud computing services. The company also stated that the resulting confusion has "at times, prevented outright sales of enterprise cloud services."<sup>7</sup> In 2011, the privacy authority in the German State of Schleswig-Holstein concluded that the transborder transmission of German citizens' personal information for storage outside the European Union likely violates German privacy law, and that storage in the United States is likely illegal for a variety of reasons, including very significantly the paucity of privacy laws in the United States.<sup>8</sup> That decision would, at a minimum, raise the costs for U.S. firms to offer cloud-based services in Germany or other countries that adopt similar requirements as these firms duplicate server locations. Trading partners such as India, Saudi Arabia and United Arab Emirates have threatened to restrict market access for certain firms which do not comply with onerous data security restrictions. While these threats have been resolved on an ad hoc basis thus far, countries (e.g. India) are contemplating new rules and requirements which could result in preferential treatment for local data providers at the expense of U.S. firms.

International privacy protection laws can significantly affect American businesses in another way as well. An American business that stores data in the United States and has a presence in a foreign country must follow United States law and also navigate the foreign court system's demands for information. For example, the local employees of U.S. companies are often threatened with jail if they do not produce data stored in the United States and protected by U.S. laws. If the business cannot follow both sets of laws simultaneously, it may be forced to choose among being sanctioned by the foreign country, leaving the foreign country, and moving data outside the United States.

---

<sup>6</sup> See September 2010 Statement of Cameron Kerry, at 10.

<sup>7</sup> Comments of Salesforce.com, at 2, in *Information Privacy and Innovation in the Internet Economy*, Docket No. 100402174-0175-01 (filed June 9, 2010), available at <http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/Salesforce%20Comments.pdf>. See also Fred H. Cate, "Provincial Canadian Geographic Restrictions on Personal Data in The Public Sector," at 13-16 (2008).

<sup>8</sup> Dr. Thilo Wiechert, "Cloud Computing & Data Privacy," at 6-7 (Feb. 2011), available at <https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>.

- b. How does the current uncertainty in the law about privacy protections for cloud computing impact American consumers?

**Response:** The impact on consumers is a mirror image of the impact on businesses. As noted in our Privacy Green Paper, trust is necessary to secure the full potential of the Internet as a political, economic, educational, and social medium.<sup>9</sup> In the digital economy, enterprises operate with private information, and consumers must be able to trust that enterprises will operate in accordance with their expectations of privacy. To the extent consumers pass up cloud-based services because of uncertainties about the privacy protections afforded, they will not enjoy the benefits that cloud services can provide to them.

Variance in privacy protection across the country adds to uncertainty about whether information in the cloud is as secure and private as information in other environments. Opened emails may receive greater protection in the 9<sup>th</sup> Circuit than in other federal jurisdictions; after *Warshak*, emails will be more “private” in the 6<sup>th</sup> Circuit than in other jurisdictions. As a result, the privacy protection afforded to an individual’s communications may turn on the accidents of where the individual lives or where his or her information is stored. A clear set of rules that are consistent with 21<sup>st</sup> century consumer experiences and expectations that also appropriately take into account public safety and other stakeholder needs could diminish this uncertainty.

- c. How does the current uncertainty in the law about the privacy protections for cloud computing impact internet service providers, and other companies offering cloud computing services?

**Response:**

As a general matter, the impact on Internet service providers (ISPs) is similar to that of other businesses that provide computing services. Indeed, as forms of access to the Internet and the varieties of services offered by ISPs multiply, the distinctions diminish. Nevertheless, email remains the most widely-used form of stored electronic content subject to the Stored Communications Act, extensively discussed in my testimony, Associate Deputy Attorney General Baker’s, and that of other witnesses in September. Since most ISPs also offer email among their services, their business model and relationship with the customers who store email communications with them are especially affected by uncertainties about the scope of protection afforded to those emails under the Stored Communications act and the Fourth Amendment .

**USE OF INFORMATION FOR COMMERCIAL PURPOSES**

2. The Electronic Communications Privacy Act does not prohibit Internet Service Providers from sharing consumer information for commercial purposes, if the consumer gives his or her consent. But, I am concerned that this consent could be obtained through complicated user agreements that consumers may not fully understand. Should ECPA be

---

<sup>9</sup> Green Paper, at 13.

amended to prohibit, or restrict, the disclosure and/or use of personal information for commercial purposes?

**Response:** The Administration has urged Congress to enact a “consumer privacy bill of rights” with a comprehensive set of fair information practice principles to provide baseline consumer data privacy protections.<sup>10</sup> As the Department of Commerce noted in our Privacy Green Paper, consumers may not have enough information about the ways in which providers use and disclose their personal information to make informed choices about whether, or on what terms, to grant consent.<sup>11</sup> We therefore recommended adopting principles to promote greater transparency between service providers and their customers, including “simple notices, clearly articulated purposes for data collection, commitments to limit data use to fulfill these purposes, and expanded use of robust audit systems to bolster accountability.”<sup>12</sup>

In my testimony before this Committee on April 6, I stated that, for online information as in the physical world, the legal protection and procedures should be determined by reference to a number of factors, including the privacy expectations of the parties involved, who has access to or control of the information, and the reasonable needs of law enforcement and national security. It is consistent with this principle that the extent to which individuals allow third-party access to their data is relevant to drawing standards under ECPA. What kinds of third-party access to electronic data service providers can or cannot allow, what forms of consent should be required, and what other rights consumers should have are questions best resolved in the context of comprehensive consumer privacy legislation that can address the full range of consumer privacy and business competitiveness issues, rather than in the context of law enforcement access.

---

<sup>10</sup> See Testimony of NTIA Administrator Lawrence E. Strickling before the Senate Committee on Commerce, Science, and Transportation, Mar. 16, 2011, at 6, *available at* [http://commerce.senate.gov/public/?a=Files.Serve&File\\_id=9e90bd89-dcb9-42c3-a8b7-e59c126b8fad](http://commerce.senate.gov/public/?a=Files.Serve&File_id=9e90bd89-dcb9-42c3-a8b7-e59c126b8fad).

<sup>11</sup> Green Paper, at vi.

<sup>12</sup> *Id.* at 4.