Data Privacy in the Wake of PRISM: A Fundamental Human Right or Unrealistic Expectation?

June 10, 2013

The United States Supreme Court first recognized privacy as within the "penumbra" of constitutional rights almost fifty years ago. Privacy, however, has remained a relative concept in the United States. In a commercial context, we consider privacy in light of its perceived drag on speed and convenience. In a government context, we weigh it against our need for security and safety.

In Europe, privacy is a fundamental human right, like life, liberty and the pursuit of happiness, or as set forth in the UN Declaration of Universal Human Rights. As a result, EU members tend to be more vigilant and demanding than Americans when it comes to the protection of individual privacy.

At the top of today's headlines is the report that the National Security Agency and the Federal Bureau of Investigation are tapping directly into the central servers of US internet companies to access audio and video chats, photographs, e-mails, documents and connection logs. If true, this means the United States government has been given nearly unfettered access to individual user data, not just anonymous, aggregated data. Edward Snowden, the Booz Allen consultant who leaked information about the program, called PRISM, has apparently told the press that "[t]hey quite literally can watch your ideas form as you type." See *The Guardian* and *Washington Post*, June 6, 2013.

Apple, Yahoo, Dropbox, Google, Microsoft, AOL, PalTalk and Facebook have all denied the claims. The Chief Legal Officer for Google, David Drummond, was vehement in the company's denial:

> "We cannot say this more clearly—the government does not have access to Google servers—not directly, or via a back door, or a so-called drop box. Nor have we received blanket orders of the kind being discussed in the media. It is quite wrong to insinuate otherwise."

The outing of PRISM could have a profound effect upon US/EU relations and commerce. Last week, for example, the EU's justice ministers "agreed to a business-friendly proposal that what companies do with personal data would be scrutinized by regulators only if there were 'risks' to individuals, including identity theft or discrimination." See "Europe Continues Wrestling With Online Privacy Rules," NY Times, June 6, 2013, by James Kanter and Somini Sengupta. The ministers debated whether to permit companies to get less than "unambiguous" consent from users regarding collection and use of their data. They also discussed

a proposal on balancing an individual's right to data protection with other rights, including the freedom to do business. One wonders whether such considerations will continue, or whether they would have even been possible had the PRISM story broke a week earlier.

Even if we assume the PRISM allegations are inflated or erroneous, it has been known for some time that Google, Facebook and others respond favorably to government requests for user data. Google is the most transparent in describing the requests. In 2012, Google reports that it received over 40,000 user data requests affecting more than 33,000 users. Around two-thirds of the time, Google complied with the request. Google asserts that the requests must be in the form of a subpoena, court order or search warrant, and subject to review by its legal team.

We have some information regarding the applications for surveillance granted by the Foreign Intelligence Surveillance Court (FISC). According to the 2012 Report, the Department of Justice submitted 1,856 applications to FISC, most of which sought authority to conduct electronic surveillance. The FISC did not deny any of the applications, although it modified 40 requests and one was withdrawn by the government. The process is far from transparent, however, so it is impossible to know the nature of the requests or how they are restricted.

What does this mean for business? All businesses possess data. With that data come legal obligations to store it, protect it and alert the data subjects and data owners of any loss or breach. Businesses engaged in e-commerce often have customers from all over the world, and they must be attuned to the unique privacy obligations imposed by the jurisdictions in which they have customers. At the end of the day, a business must decide what data to store for later use, how and where to store it, and for how long. Government policies on privacy can have a profound effect on those decisions. Data privacy attorneys can help businesses make the appropriate decisions with respect to data, even in the face of conflicting legal obligations.

For more cutting edge insights, news, and commentary, visit our Media, Privacy & Beyond blog at http://www.media-privacy.com.