

An Update on Big Data in Little Chunks

March 2014

“Big data” has received a great amount of press attention over the past couple of years. Nonetheless, little has changed in the way of law or regulation. There are no “big data” laws; instead, regulators, policymakers, and privacy professionals have sought to identify how the concept and applications of big data fit within the existing legal framework. This, however, may change in the relatively near future.

Snowden Disclosures

Perhaps the most signal development affecting big data has been the numerous revelations initiated by former CIA employee and NSA contractor Edward Snowden regarding the intelligence community's collection and storage of personal data. More than any other event, the Snowden disclosures have brought big data to the forefront of public attention.

One outcome of this is a growing awareness of the many possible meanings of the term “big data.” Although the press and public have largely focused on intelligence community surveillance and data practices and their implications for personal privacy, the scrutiny being accorded big data inevitably will affect businesses in the private sector as well.

This linkage has been made at the highest levels of government. While President Obama has launched an internal review of the intelligence community's activities, he also noted that big data raises privacy concerns in the private sector as well. To that end, he directed the President's Council of Advisors on Science and Technology to undertake a 90-day review of how “big data” does and will affect how Americans live and work. One question that this process is expected to consider is whether the Administration's proposed Consumer Bill of Rights—announced only two years ago—is

Practice Areas

Internet of Things

already out of date, at least insofar as big data is concerned. That effort is well underway. The group has met with privacy and civil liberties groups, and it is in the process of holding several workshops around the nation regarding current uses of big data.

FTC Initiatives

The White House isn't the only one taking a close look at big data. The Federal Trade Commission (FTC) has been looking at big data practices for a while. Notably, Chairman Edith Ramirez has delivered several speeches about risks and legal issues relating to big data. It is worth noting that Chairman Ramirez has particularly challenged the notion that the regulatory focus should be on the use of data, rather than on its collection. She also noted that big data increases the potential risks from data breaches. Similarly, Commissioner Julie Brill has expressed concerns about the use by data brokers of the vast troves of data about persons that they have accumulated. These remarks by two FTC commissioners suggest that businesses should anticipate FTC efforts to reduce the collection of large data sets, instead of merely attempting to regulate their use once collected. However, given the many different ways in which big data is collected and used today, and the absence of any general federal privacy law, the FTC will face a number of challenges if it attempts to restrict collection.

But the FTC has taken initial efforts. Its most recent revisions of its regulation implementing the Children's Online Privacy Protection Act can be seen as an effort to limit data collection. And such efforts will continue. Jessica Rich, chief of the FTC's Consumer Protection Bureau, has stated on several occasions, including earlier this month at a privacy conference, that big data is a major focus for 2014. Look for indications of the FTC priorities and concerns in its upcoming report on data brokers, its recent workshop on tracking customers in retail stores, and other areas in which data about individuals can be gathered and stored.

In this vein, the FTC will be conducting a series of workshops to explore aspects of big data. The first, convened in mid-February, focused on mall tracking, which enables retailers to monitor a customer's movements through a retail store by tracking the customer's cell phone. One issue is whether this type of tracking allows, or in time will allow, retailers to develop profiles of customers. During the workshop, some consumer advocates and FTC staff expressed concern that retailers are tracking customers without their knowledge or consent, and a Washington think tank has created a website where users can "opt-out" of such tracking. Representing retailers, however, the National Retail Federation expressed strong opposition to any requirement that stores post signs to disclose tracking, saying that they already post more signs than customers read and that no need for additional signage has been shown.

Commerce Activities

The U.S. Department of Commerce (DOC) also is taking a role. The DOC's National Telecommunications and Information Administration in February launched its second multistakeholder effort to develop a code of conduct, this time on facial recognition software. One concern underlying this process is a fear that facial recognition software—and particularly facial *identification* software—when deployed on a widespread basis will enable businesses to track, collect, and aggregate information even about people with whom they have

not established a business relationship or previously collected identifying information. Look for this process to test whether, and, if so, how, the Consumer Bill of Rights, announced two years ago, will remain meaningful as technology evolves.

Internet of Things

Finally, yet another front in the big data battles is the potential collection of information about drivers by motor vehicles—one aspect of the so-called “Internet of Things.” For example, earlier this winter Sen. Al Franken (D-MN), who has taken a particular interest in location privacy, asked the Ford Motor Company to elaborate on how it collects personal information via its vehicles' navigation systems. In its response, Ford discussed its navigation and other “connected services,” which transmit location and other information to Ford or other service providers.

In the case of the Internet of Things, as with other forms of big data, the challenge facing policymakers is to identify and address legitimate privacy concerns without interfering in legitimate business practices or harming innovation. Businesses should pay close attention as matters develop over the course of 2014.