wiley

NEWSLETTER

Gleanings from the White House Report on Big Data

May 2014

The first day of May brought the release of a White House report on "Big Data," together with a companion report by the President's Council of Advisors on Science and Technology (PCAST). While the formal White House report attracted most of the headlines because of its specific policy recommendations, the PCAST report may have the more lasting significance.

In January, President Obama launched a 90-day review of the impact big data technologies are having, or will have, on a range of economic, social, and government activities. (*See An Update on Big Data in Little Chunks in March 2014 PIF*). The resulting report focused on the effects of big data activities in the private sector and their effect on how Americans live and work. Concurrently, the PCAST was asked to review the current technologies for managing and analyzing big data and for protecting privacy.

The two reports both contain interesting and insightful discussions of privacy issues related to big data. However, little immediate change is likely. Instead, the most likely effects of the reports will be to advance—and shift—the debate.

Big Data: "Volume, Variety, and Velocity"

The White House report leads off with a summary of how increases in computer processing power, plunging costs of computation and storage, and the explosion in the number of data collecting devices—including the Internet of Things—have created the big data world. It notes that big data has the potential to improve life and society in many ways ?to prevent fraud, to improve energy efficiency, to increase agricultural productivity, and countless others. It then asks

Practice Areas

Internet of Things

whether existing legal, ethical, and social norms are adequate to protect privacy and other values in a big data world.

While the White House report covers a number of privacy-related topics, two will be summarized here. First, the report particularly focused on the potential for big data in the commercial sector to produce "perfect personalization" enabling the delivery of products and services to precise market segments. It notes how targeting enhances the value of advertising that in turn benefits consumers enormously by enabling free access to many Internet services. Interest-based advertising (also known as "behavioral targeting") is one manifestation of this.

On the flip side, the report discusses the risks that "perfect personalization" and the related practice of "alternative scoring" may result in discrimination in pricing, services, and opportunities, often in ways that fall outside of the scope of existing federal laws such as the Fair Credit Reporting Act or the Fair Housing Act, calling that out for greater policy attention.

Second, lawyers will be interested in the report's survey of privacy law in the United States, and particularly in its discussion of the implications of big data on the "reasonable expectation of privacy" test and the "third-party" doctrine. Under those doctrines, personal data entrusted to entities such as banks, telecommunications carriers, and the like receive comparatively scant privacy protection, especially from governmental investigators.

Policy Recommendations

But the major focus of the White House report consists of the identification of a policy framework for big data, with a focus on placing greater emphasis on responsible use by businesses and governments that collect, store, and use data. The report concludes with six specific recommendations:

- The Commerce Department should seek public comment on big data developments with a view towards revising the Consumer Privacy Bill of Rights (CPBR) and drafting of legislative text. This implicitly recognizes that the February 2012 proposal may need tweaking to remain relevant to big data.
- Congress should enact federal data breach legislation, per the President's May 2011 Cybersecurity legislative proposal.
- Extend the protections of the Privacy Act of 1974 to non-U.S. persons.
- Ensure that data collected about students in schools is used for educational purposes.
- Civil rights and consumer protection agencies should improve their technical capabilities to identify and redress discriminatory practices.
- Amend the outdated Electronic Communications Privacy Act to make privacy protections for electronic data equivalent to that accorded physical data.

The majority of these recommendations require Congressional action, which seems unlikely in the waning days of the current Congress. Furthermore, these recommendations focus primarily on commercial uses and steer away from the controversial national security issues which currently dominate discussions in Congress.

PCAST: Technology Affects Policy

The PCAST report to the President, published concurrently, offers more of a technological perspective on the issues involved in addressing privacy in a big data world. PCAST is comprised of academics, policy advisors, and representatives of businesses such as Google. Its report examined the current technologies for managing and analyzing big data and preserving privacy, with particular attention to evolving trends.

In many ways, its analysis may prove to be a more pivotal event in federal privacy policy.

Big data is big because of the quantity and variety of data available to be processed and because of the scale of analysis that can be applied. These characteristics put pressure on current ways of thinking about privacy because they can render current privacy-enhancing technologies ineffective.

For example, the PCAST report observes that some current privacy-enhancing technologies—such as anonymization and data deletion—are less robust in a big data world precisely because big data processes can override them.

PCAST also points out that the notice and comment paradigm that has shaped privacy law in the United States for most of the past decade is inadequate: "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." These inadequacies will grow in a big data world in which future uses are unknown, and the data may be processed and stored by entities far removed from the individual. Thus, "a focus on the collection, storage, and retention of electronic personal data will not provide a technologically robust foundation on which to base future policy."

Instead of notice and consent, PCAST proposes to recast the principles underlying the CPBR by applying them primarily to *context* and *use* instead of collection: "Policy attention should focus more on the actual uses of big data and less on its collection and analysis." It recommends focusing instead on encouraging and facilitating responsible use by the entities in possession of the data. This would mean shifting the burden from the consumer—who currently has the burden of reading, understanding, and acting upon published privacy policies—to the company to conform its uses of personal data to a profile designated by the consumer. The vision is of a world in which policies are associated with particular data and the code that operates on the data, with entities responsible for complying with those codes.

This recognition of the limited effectiveness and future utility of the notice and consent approach that currently dominates privacy law will likely have profound consequences down the road as policy experts seek more effective regimes. Still, the use of privacy policies under the notice and consent approach has become embedded in American law over the past two decades, and that is not likely to be undone for years. The interesting issue will be whether and how governments shift the emphasis to "use" rather than "collection" and how that concept will work its way into the law.