Published on *The National Law Review* https://natlawreview.com

White House & PCAST (President's Council of Advisors on Science and Technology) Reports on Big Data: Telecommunications

Article By:

Drinker Biddle & Reath LLP

The White House recently released its report on big data, "**Big Data: Seizing Opportunities, Preserving Values**" (WH Report). This report was released simultaneously with a report from the P**resident's Council of Advisors on Science and Technology (PCAST),** "Big Data and Privacy: A Technological Perspective" (PCAST Report). Our summary focuses on the implications of the WH and PCAST reports on big data in telecommunications.

This summary describes how the reports analyze the intersection of communications capabilities and big data, describing the ways that big data is dependent on telecommunications and also provides opportunity for innovation in the telecommunications industry. We then describe the benefits that big data offers to consumers and the associated risks. Finally, we highlight the proposed policy and regulatory solutions described by the reports.

Introduction

The focus of both reports is on policy issues posed by "big data" rather than general privacy?infringing use of information technology. Big data is described as "high?volume, high?velocity and high?variety information assets that demand cost?effective, innovative forms of information processing for enhanced insight and decision making."[1] Big data, often mined from the "Internet of Things," hinges on communications products and services, which provide the instruments and channels necessary for the collection, processing, and transfer of data about consumers. Telecommunications providers and supporting functionalities and applications can greatly benefit from the use of big data to provide targeted products and services to customers.

The reports note that there is no comprehensive standard for data privacy that can be scaled to big data. Current regulation governing the collection, transfer, and use of data is sector-specific, placing "fewer broad rules on the use of data, [and] allowing industry to be more innovative in its products and services."[2] The pitfall of this regulatory regime, as highlighted by the WH Report, is that current U.S. privacy protections are modeled on "small data" and therefore must be reevaluated to protect individuals against the complex risks of big data.[3]

The Benefits of Big Data in the Communications Ecosystem

The reports describe the world of big data, where consumer information is collected, aggregated for analysis, transferred to data users, and thereupon used for targeted marketing, consumer engagement, and to accomplish "perfect personalization" of goods and services. Each of these stages in the big data life cycle involves communications. Data is **collected**, for example, when a mobile device or Internet service tracks consumer behavior. Telecommunications providers then facilitate the **transfer** of collected data to parties conducting data analytics and then further transfer this information to data users. Finally, telecommunications providers themselves **use** data to provide targeted products and services to their customers.

The WH Report recognizes that big data and the ability to collect and process vast amounts of consumer information have the potential to bring numerous benefits to individuals. As the communications industry continues to provide businesses direct and interactive ways to engage consumers, big data provides the opportunity for this engagement to be more potent and tailored to consumer needs. As highlighted in the WH Report, big data can increase consumer engagement by providing insight into individual decision making, which in turn allows businesses to provide goods and services to individuals in a manner that suits the individuals' preferences.[4]

In the critical area of health, for example, big data can be used to collect, analyze, and understand patient behavior and health conditions on a much larger scale. The knowledge that can be obtained from large-scale patient data, combined with innovations in telecommunications can lead to the development of new and effective means for health care providers to communicate with patients in real time, detect symptoms early on, and provide immediate and even predictive treatment.[5]

Ultimately, the WH Report highlights big data's ability to create the "perfect personalization," where data is aggregated and processed to predict individual preferences or behaviors and deliver targeted messages, products, or services to consumers.[6] Perfect personalization will, in turn, further the benefits of big data as intimate knowledge of individual behaviors and preferences paves the way for innovation that improves overall quality of life.

Current Challenges

According to the WH Report, "while big data will be a powerful engine for economic growth and innovation, there remains the potential for a disquieting asymmetry between consumers and the companies that control information about them."[7] The WH Report opens by highlighting the pure risk of impinging on individuals' "right to privacy." Particularly, the WH Report discusses the potential application of the third-party doctrine to data stored with cloud service providers, possibly allowing for government surveillance of data stored in the cloud.[8]

The more palpable problem highlighted is the risk that big data will cause actual harm to consumers through the improper use of consumer data, including the pitfalls of perfect personalization. One potential harm stems from the risk of personal information breaches, a risk that is amplified with big data's large-scale storage and exchange of personal information. For example, where a big data controller experiences a data breach that leads to the disclosure of personal information, potentially permanent financial and reputational damage can result. Another risk associated with perfect personalization is the use of data for discriminatory purposes. Discrimination can occur when perfect personalization leads to individuals being unfairly categorized in unfavorable groups and thereby perceived less favorably for jobs, lines of credit, retail discounts, or other social benefits.[9] These

harms are magnified when considering the unbridled capacity within the digital world to capture, copy and share data.[10] Unfavorable data, whether accurate or not, may be retained and used indefinitely, leaving the consumer no means to correct or contain the negative implications.

Because of these risks, the reports recommend reevaluation of the privacy regulatory regime to more equitably balance the interests of businesses and consumers and to provide consumers with more protection and control.

Possible Approaches to Big Data Risks

Both reports note that the pillar of data protection has thus far been notice and consent.[11] However, both reports, PCAST's in particular, emphasize the insufficiency of notice and consent for guarding individual privacy in the world of big data where the uses of data are often too complex and varied for the consumer to knowledgeably consent. Currently, notice and consent places the burden of privacy protection on the individual when it should be on the provider of goods or services requiring the use of that data. Further, as noted in both reports, stringent notice and consent requirements prevent innovation through new, non-obvious, and unexpectedly powerful uses of data.[12]

The reports also highlight the insufficiency of other protective measures, including de-identification and online Do Not Track mechanisms.[13] Neither de-identification nor anonymization can promise true anonymity while retaining the value of the data. "While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to re-identify seemingly 'anonymous' data."[14] Also, the use of Do Not Track signals and similar tools that allow consumers to control the collection and use of their data online present their own problems and risks. For example, Do Not Track signals and similar technologies are unable to discriminate between files (*e.g.*, cookies) issued by web servers for security purposes and those set for non-security purposes. Therefore, when a browser sends out a Do Not Track signal, it may be unintentionally disabling highly effective fraud prevention and online security controls.[15]

Generally, the PCAST Report highlights the opinion that the risks posed by big data cannot be solved by regulation that focuses on the collection and analysis of data, as well as specific technical solutions.[16] Such policies will become rapidly outdated as technology develops. Rather, both reports suggest that efforts aimed at resolving the privacy risks associated with big data focus on the *use* and *context* of data based on a consideration of outcomes.[17] Use, for example, must avoid any discriminatory purposes. As the WH Report clarifies, it is one thing to use big data to segment consumers for useful marketing purposes; it is another to use this information to determine an individual's eligibility for employment, housing, health care, credit, or education.[18]

Conclusion

According to the reports, the existing state of big data regulation both prevents productive innovation and threatens the rights of individuals. Without a reevaluation of national privacy policies and recommendations, it is likely that the legal compliance risks with respect to the privacy of personal information will continue to increase. In the near future, businesses may not be able to rely on the traditional notice and consent framework but will have to base privacy compliance on the use and context of data.

Finally, in considering the future of big data and its regulatory implications, it is worth noting that the reports diverge to some degree in their perception of metadata. Whereas the WH Report cites

difference of opinion over metadata's privacy risks,[19] PCAST indicates that "[t]here is no reason to believe that metadata raises fewer privacy concerns than the data they describe."[20] The ultimate determination of the role of metadata in big data and privacy may compound the hurdles faced by the communications industry.

Overall, the reports do not have significant immediate import for the landscape of privacy regulation. Instead, they provide an additional opportunity to develop discussion and gauge the federal government's future goals with respect to privacy law.

WH Report: click here.

PCAST Report:click here.

---

[1] PCAST Report, p. 2.

[2] WH Report, p. 18.

[3] WH Report, p. 21.

[4] WH Report, p. 7.

[5] WH Report, p. 23.

[6] WH Report, p. 7.

[7] WH Report, p. 39.

[8] WH Report, p. 33.

[9] WH Report, p. 7.

[10] WH Report, p. 9.

[11] WH Report, p. 54; PCAST Report, p. 38.

[12] WH Report, p. 54; PCAST Report, p. 38.

[13] WH Report, p. 54; PCAST Report, p. 38.

[14] WH Report, p. 54.

[15] WH Report, p. 42.

[16] PCAST Report, p. 49-50.

[17] WH Report, p. 51, 56.

[18] WH Report, p. 51.

[19] WH Report, p. 35.

[20] PCAST Report, p. 19.

National Law Review, Volume IV, Number 157