Information Technology
Industry Council

Submission to the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce

Docket No. 140514424–4424–01
RIN 0660–XC010

Comments of the Information Technology Industry Council in response to NTIA's Request for Public Comment on *Big Data and Consumer Privacy in the Internet Economy*

August 1, 2014

I. Introduction

The Information Technology Industry Council (ITI) appreciates this opportunity to respond to NTIA's recent Request for Public Comment (RFC) relating to big data and privacy. ITI, a U.S.-based global trade association representing 58 of the world's most dynamic and technologically innovative companies, works to advance effective policies that promote privacy and that also enable the technology sector to continue to innovate and develop new products and services. As discussed more fully below, ITI makes a number of recommendations with regard to big data focusing on three main areas: (a) a responsible use and risk-based approach; (b) accountability mechanisms; and (c) data security and breach notification.

NTIA's RFC followed the release of two reports delivered to President Obama in response to the president's January 17, 2014 request for an examination of issues surrounding big data. The first report, *Big Data: Seizing Opportunities, Preserving Values* (the "Big Data Report"), prepared by an inter-agency working group led by Counselor to the President John Podesta, explored big data opportunities and challenges, particularly as they relate to privacy.[1] The working group made several policy recommendations.

The second report, *Big Data and Privacy: A Technological Perspective* (the "PCAST Report"), prepared by the President's Council of Advisors on Science and Technology, focused on the current state of technology—and technology's trajectory—for managing and analyzing big data and preserving privacy.[2]

II. Big Data and Policy-making

The Big Data Report discusses the capabilities of big data and the significant societal benefits big data analysis—often in real time—can yield. Big data offers tremendous opportunities in many areas, among them health care (both medical research and delivery of health care), agriculture, energy efficiency, transportation, and education. The report highlights that big data can save lives—it has enabled the detection of early warning signs of infections in premature babies. The report further emphasizes that in areas such as electricity efficiency, vehicle maintenance, and combatting government insurance fraud, big data supports powerful analysis that could not previously be done. In addition, the report discusses how big data enables marketers to provide consumers with more tailored offers, and the enormous benefits associated with personalized web experiences and targeted advertising—a practice that subsidizes many free Internet services.

[1] "Big Data: Seizing Opportunities, Preserving Values," *Executive Office of the President*, May 2014, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[2] "Report to the President: Big Data and Privacy: A Technological Perspective," *Executive Office of the President: President's Council of Advisors on Science and Technology*, May 18, 2014, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

At the same time, the report articulates concerns and seeks policy solutions. It cautions that big data analysis could lead to discriminatory outcomes as more decisions are determined by algorithms and automated processes. Specifically, the working group urges that "[w]e must prevent new modes of discrimination that some uses of big data may enable, particularly with regard to longstanding civil rights protections in housing, employment, and credit."[3]

ITI appreciates that the report recognizes the myriad of opportunities created by big data. Further, ITI supports the report's urging that discriminatory outcomes relating to the protection of civil rights should be prevented and that this area is important for policymakers. Accordingly, we encourage NTIA and the administration to devote resources to identifying and examining *actual* harms caused by particular uses of big data.

We welcome the report's recommendation that the U.S. government's lead civil rights and consumer protection agencies expand their technical expertise to identify such discriminatory practices and outcomes and to develop a plan to investigate and address violations of law. U.S. laws that outlaw discrimination and the Fair Credit Reporting Act—the law that promotes the accuracy, fairness, and privacy of information held by consumer reporting agencies—must be enforced. We also note that self-regulatory codes of conduct currently in use prohibit certain discriminatory uses of data, and we urge that self-regulatory mechanisms be encouraged.[4] Companies that

[3] "Fact Sheet: Big Data and Privacy Working Group Review," *The White House: Office of the Press Secretary*, May 1, 2014, accessed July 31, 2014, http://www.whitehouse.gov/the-press-office/2014/05/01/fact-sheet-big-data-and-privacy-working-group-review.

[4] For example, codes of conduct developed by the Digital Advertising Alliance (DAA) include restrictions on the use of data for eligibility purposes in connection with employment, credit, healthcare, and insurance. See: "Self-Regulatory Principles for Multi-Site Data," *Digital Advertising Alliance*, November 2011, accessed July 31, 2014, http://www.aboutads.info/msdprinciples and "Self-Regulatory Principles

represent that they abide by such a code of conduct but then violate its requirements could become subject to an action by the Federal Trade Commission (FTC) for engaging in a deceptive practice in violation of Section 5 of the FTC Act.

ITI strongly supports a thorough examination of the current foundation of privacy and anti-discrimination protections currently afforded consumers, including privacy laws related to health, financial information, children, and credit, and anti-discrimination laws in the areas of employment, education, housing and credit worthiness. This examination should determine whether gaps actually exist and if so, their scope. If gaps in the law are identified, NTIA and the administration should carefully consider whether they are unique to big data, or whether they exist regardless of the technology used. Any policy proposals that would address privacy and discrimination harms should be "technology neutral."

As policymakers continue to examine big data, it is important that they take into account the data environment as it exists today, and recognize that the ecosystem continues to evolve. In addition, we note—as the Department of Commerce did—that, consumer trust in networked technologies empowers consumers to turn to the Internet to "express their creativity, join political movements, form and maintain friendships and engage in commerce."[5] ITI member companies recognize that consumer trust in our products and services is critical to economic growth. This trust includes consumer confidence that companies both are providing innovative products and services, and being transparent and fair in connection with the consumer information to which they

for Multi-Site Data," *Digital Advertising Alliance*, July 2009, accessed July 31, 2014, http://www.aboutads.info/msdprinciples.

[5] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," *The White House*, February 2012, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

have access. These principles guide ITI's comments below, which focus on three main areas: (a) a responsible use and risk-based approach; (b) accountability mechanisms; and (c) data security and breach notification.

A. Responsible Use and Risk-based Approach to Privacy

(i) Responsible Use of Big Data

The Big Data Report discusses the "3Vs" that distinguish big data from traditional modes of data capture and analysis. The "3Vs"—the volume and variety of data, and the velocity at which it is collected—enable big data to reveal insights that are unexpected or were previously unknowable.

The Big Data Report acknowledges that in certain instances, it is more appropriate to focus greater attention on how data is used, and less on its collection. The report points out that "a shift to focus on responsible uses in the big data context allows us to put our attention more squarely on the hard questions we must reckon with: how to balance the socially beneficial uses of big data with the harms to privacy and other values that can result in a world where more data is inevitably collected about more things."[6] ITI supports this approach.

(ii) Risk Assessment and Mitigation

Question 3 in NTIA's RFC seeks input on how a responsible use framework might address some of the challenges posed by big data. As described below, a responsible use framework based on risk-based assessment and mitigation could meet the challenges of big data by encouraging organizations to thoroughly consider the privacy issues involved in decisions about whether data should be used for a given purpose.

[6] "Big Data: Seizing Opportunities, Preserving Values," *Executive Office of the President*, May 2014, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

A responsible use framework requires an organization to implement robust procedures and mechanisms to determine, based on the risks involved, which uses of data should be pursued and which should not. Thus, a use-based framework involves examining the potential risks of a particular data use. A risk-based analysis would be based on a common set of factors, such as the type of data being analyzed and used, how the data was amassed, the public interest in the use of the data, the consumer benefits of the use, the security measures in place, whether the data is shared with third parties, and the potential harmful impact to individuals resulting from the use. This risk assessment would serve not only to determine whether a particular use or analysis should go forward, but also to identify how privacy protecting safeguards might be implemented to mitigate risks. By assessing the privacy risks at the outset (through what might be thought of as a privacy risk assessment), data scientists could identify how to derive the maximum benefit from the data while minimizing the risks to individuals. As question 16 in the RFC highlights, the development of a framework for privacy risk management can be an effective mechanism to address the challenges posed by big data.

(iii) The Role of De-identification

As noted above, the "type of data being analyzed and used" is one factor to be considered in determining the appropriateness of a data use. For example, whether data is de-identified will be a consideration in a company's overall risk-based assessment and mitigation strategy. If the data an organization plans to analyze is de-identified, the potential privacy risk is lessened. If the data is not presently de-identified, a company may choose to de-identify the data in order to mitigate potential privacy risks. In Question 11 of the RFC, NTIA points out that the PCAST Report indicates that it is becoming "increasingly easy to defeat" de-identification of data.

However, NTIA, (in Question 11 of the RFC) and the PCAST have noted that de-identification "may remain useful in some contexts, particularly when employed in combination with policy safeguards."

De-identification remains a useful tool to mitigate risks related to data use. While depending on the circumstances, the likelihood of re-identification varies, recent research indicates that the "real world" risk of re-identification may be far lower than expected.[7] We note that examples of re-identification often involve datasets that were publicly accessible, enabling robust efforts to defeat identification. When datasets are kept confidential, the risk of re-identifying the data is significantly lessened.

We further note that new techniques continue to improve our ability to de-identify data. ITI encourages NTIA and the administration to support technological research into more effective de-identification methods. In addition, policies that encourage de-identification should be pursued. For example, the Federal Trade Commission, in its 2012 privacy report, stated that the agency's privacy framework applies to data that is reasonably linkable to a specific consumer, computer, or device. Thus, data that is not "reasonably linkable" would not be subject to the requirements of the framework.[8] The FTC Report outlines the steps it expects companies to take to render information not reasonably linkable. Organizations, as part of their risk mitigation techniques, can develop processes to de-identify data where appropriate, and processes to prevent re-identification. We emphasize that de-identification may

[7] Daniel Castro and Ann Cavoukian, "Big Data and Innovation, Setting the Record Straight: De-Identification Does Work," *Office of the Information and Privacy Commissioner, Ontario, Canada and Information Technology Industry Council*, June 2014, accessed July 31, 2014, http://www2.itif.org/2014-big-data-deidentification.pdf.

[8] "Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers," *Federal Trade Commission*, March 2012, accessed July 31, 2014, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

serve as one tool among many that an organization deploys to mitigate privacy risks raised by the use of big data.

B. Accountability Mechanisms

In highlighting the value of a responsible use framework, the Big Data Report points out a significant advantage: "[f]ocusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection."[9] In the big data context, and particularly in developing a responsible use and risk-based approach to privacy, holding companies accountable for decisions they make about the processing, management and protection of data is critical. Indeed, in question 13 of the RFC, NTIA inquires what role accountability mechanisms can play in the big data context to promote socially beneficial uses of big data while safeguarding privacy.

Accountability is one of the principles of the Consumer Privacy Bill of Rights, and a principle of fair information practices articulated in several of the seminal international privacy instruments, including the Organisation for Economic Cooperation and Development's Privacy Guidelines (1980), and the Asia Pacific Economic Cooperation's Privacy Framework, (2005). Both of these instruments state that entities "should be accountable for complying with measures that give effect" to the principles in the applicable instrument. Generally, accountability requires that organizations develop and implement processes that foster compliance with their privacy-related commitments. The nature of these commitments will differ, depending on a number of factors including the regulatory requirements to which a company is subject, self-

[9] "Big Data: Seizing Opportunities, Preserving Values," *Executive Office of the President*, May 2014, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

regulatory mechanisms in which a company participates, and the policies that a company develops, which in some cases may include elements of external criteria such as the fair information practice principles (FIPPs). As noted below, however, implementation of certain of the FIPPs can be challenging in the big data context.

Accountability requires that organizations describe how their processes comport with the commitments they have made and demonstrate how they are meeting their commitments. The tools that a company uses to evaluate its processes will depend on various factors, including the size, complexity and nature of an organization's business. Assessments can include internal or external audits, as well as other systems for ongoing oversight, assurance reviews and verification.

Robust accountability is particularly important in the context of big data and a responsible use framework and risk-based approach to privacy where there may be a lesser reliance on certain of the fair information practice principles. In the RFC, NTIA seeks input on the Consumer Privacy Bill of Rights and whether its elements accommodate big data. One limitation of the Consumer Privacy Bill of Rights in the big data context is the "individual control" principle, which may not be practical in an environment with connected devices and sensors, where user interfaces are not feasible. For example, the collection of data relating to energy consumption through smart grid technologies may not include user interfaces. The responsible use framework would, as articulated in the Big Data Report "shift the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data."[10] Thus, a robust responsible use framework and a risk-based approach with accountability mechanisms is a practical alternative to a framework that relies on principles such as "individual control" which may not be feasible in certain circumstances.

C. Data security and breach notification

While the NTIA RFC largely focuses on privacy-related considerations, we urge the conversation to include the importance of data security. The Consumer Privacy Bill of Rights includes "security" as one of its principles, and the importance of security is paramount in the big data context where large amounts of data are collected and processed, often in real time. In addition, certain decisions are made—based on data—about the functioning of devices that impact all facets of our lives. These "devices" include vehicles, alarm systems, medical devices, and countless other ICT-enabled products. We note that the measures that an organization employs to secure data will depend on a number of factors, including the nature of the data and its sensitivity, as well as the size and complexity of the organization.

In addition, the large amounts of data that can be amassed in the big data context highlights the need for federal data breach notification legislation, as recommended in the Big Data Report, to replace the current patchwork of state breach notification laws. ITI supports a federal standard that would require data breach notification when the unauthorized acquisition of sensitive personal data could result in a significant risk of fraud. Such legislation would preempt existing states laws, would be

[10] "Report to the President: Big Data and Privacy: A Technological Perspective," *Executive Office of the President: President's Council of Advisors on Science and Technology*, May 18, 2014, accessed July 31, 2014, http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

technology neutral, and would set forth reasonable time periods for breach notification.

* * *

ITI appreciates the opportunity to submit these comments to NTIA. If you have any questions about these comments, please contact Yael Weinman, VP, Global Privacy Policy and General Counsel, Information Technology Industry Council, at 202-626-5751, yweinman@itic.org.