Information Technology Industry Council

Submission to the White House Office of Science and Technology Policy

Response to the Big Data Request for Information

Comments of the Information Technology Industry Council

March 27, 2014

I. Introduction

The Information Technology Industry Council (ITI) appreciates this opportunity to provide comments to the Office of Science and Technology Policy (OSTP). ITI is a U.S.-based global trade association representing more than 50 of the world's most dynamic and innovative companies in the information and communications technology (ICT) sector.

Following months of revelations relating to the nation's surveillance programs, on January 17, 2014, President Obama delivered remarks outlining his plans for surveillance reform. Both prior to January 17, and since the President's remarks, ITI provided written comments to the administration, the President's Review Group on Intelligence and Communications Technologies (Review Group), and the Privacy and Civil Liberties Oversight Board (PCLOB).[1] In these comments, ITI outlined the significant negative economic impact that the revelations are having on the technology sector due to the erosion of public trust, as well as the potential long-term implications for innovation and Internet governance on the global economy. ITI recommended

[1] *See* letter to White House Chief of Staff and White House Counsel (August 20, 2013), *available at* http://www.itic.org/public-policy/TechLetteronWaystoProtectCivilLibertiesinGov%E2%80%99tDataCollection.pdf; comments to the Review Group (October 3, 2013) a*vailable at* http://www.itic.org/upload/ITISIIALettertoReviewGroup.pdf; and comments to PCLOB (October 24, 2013), *available at* http://www.itic.org/dotAsset/6/9/697dec86-0d33-448c-9798-960e172a6dc5.pdf.

specific steps that the U.S. government could take to restore public trust, including greater transparency and oversight. In recent testimony before the House Judiciary Committee, and PCLOB, ITI's President and CEO stressed the critical need for reforms.[2] ITI continues to urge the administration and Congress to work together to implement the necessary reforms to restore trust in the innovative products and services that ITI member companies provide, and to maintain the open and borderless Internet that benefits so many individuals, companies, and countries around the world.

In his January 17, 2014 remarks, President Obama also announced that he had appointed John Podesta to conduct a comprehensive review of big data. Recognizing that this review of big data is distinct from the issues in connection with surveillance reform, ITI's comments today relate specifically to this big data review. ITI appreciates the opportunity to provide input on this important topic.

II. Big data

Both the U.S. government and the private sector recognize the potential capabilities of large-scale data analytics. In 2012, the administration announced the National Big Data Research and Development Initiative to improve the "ability to extract knowledge and insights from large and complex collections of digital data."[3] That initiative is committed to helping "accelerate the pace of discovery in science and engineering, strengthen our national security, and transform teaching and learning."

---

[2] *See* testimony of Dean C. Garfield before the House Judiciary Committee (February 4, 2014) *available at* http://www.itic.org/media/news-releases/testimony-of-iti-president-dean-c-garfield-before-the-house-judiciary-committee-regarding-fisa-reform, and testimony of Dean C. Garfield before the PCLOB (March 19, 2014) *available at* http://www.itic.org/media/news-releases/testimony-of-iti-president-and-ceo-dean-garfield-before-the-privacy-and-civil-liberties-oversight-board.

[3] *See* Press Release, White House Office of Science and Technology, Obama Administration Unveils "Big Data" Initiative: Announces $200 Million in New R&D Investments (March 29, 2012) *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf.

Across the U.S. government, agencies are examining how to derive maximum benefit from data. Last month, the National Oceanic and Atmospheric Administration (NOAA) issued a request for information outlining its interest to "unleash the power of its data" and seeking assistance from the private sector to make NOAA's data available in a "rapid, scalable manner to the public."[4] We encourage the administration to continue its work on maximizing the greatest benefits from big data.

Innovation across sectors, including ICT, depends on the value derived from large-scale data analytics. Specific societal benefits of big data were highlighted in the March 3, 2014 conference at the Massachusetts Institute of Technology (MIT) convened as part of OSTP's big data review. Panelists discussed how big data is enabling tremendous benefits in areas such as medical care, transportation, and education. As acknowledged by John Podesta in his keynote address:

> *The value that can be generated by the use of big data is not hypothetical. The availability of large data sets, and the computing power to derive value from them, is creating new business models, enabling innovations to improve efficiency and performance in a variety of public and private sector settings, and making possible valuable data driven insights that are measurably improving outcomes in areas from education to healthcare.*[5]

[4] *See* Press Release, NOAA, NOAA announces RFI to unleash power of 'big data' Agency calls upon American companies to help solve 'big data' problem *available at* http://www.noaanews.noaa.gov/stories2014/20140224_bigdata.html.

[5] *See* Remarks as Delivered by Counselor John Podesta The White House/MIT "Big Data" Privacy Workshop (March 3, 2014) *available at* http://www.whitehouse.gov/sites/default/files/docs/030414_remarks_john_podesta_big_data.pdf.

While the benefits of big data are considerable, the question has been posed—by OSTP, as well as others—whether existing policy frameworks for protecting consumer privacy sufficiently address the privacy issues that could be implicated by big data. At the same time that this issue is examined, it is fundamentally important that we more fully consider and understand the significant and transformational benefits that big data can have on individuals: improvements in health care through application of personalized medicine; improved living conditions though enhanced urban planning and development; environmental advancements through enhanced sustainable consumption and more efficient use of energy; and countless other beneficial applications as well as innovative products and services.

As the White House conducts its examination of big data, there must be sufficient study of the beneficial applications as well as the potential risks. We encourage OSTP to fully examine the range of benefits and capabilities associated with big data. Without understanding the benefits, it is impossible to understand the possible opportunity cost of risk mitigation strategies. Only with a complete picture can policy approaches to big data be optimized. Because of the capabilities of large-scale data analytics, responsibility requires being mindful of how data is being used, but also what the implications are for not using it.

III. Policy Frameworks

As OSTP examines how existing privacy frameworks can address the issues raised in connection with big data, we agree that such analysis should begin with the privacy framework approach outlined in the 2012 White House report, which includes a "Consumer Privacy Bill of Rights" that incorporates elements of the Fair Information Practice Principles.[6]

[6] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), ("White House Report") *available at*

As recognized in the White House Report, the "existing consumer data privacy framework in the United States is flexible and effectively addresses some consumer data privacy challenges in the digital age."[7] This framework, which includes sector-specific laws enforced by a number of different U.S. agencies, Federal Trade Commission (FTC) enforcement under Section 5 of the FTC Act,[8] industry best practices, and self-regulatory initiatives, has shown a level of adaptability to technological innovation. We urge OSTP to identify the strengths of the existing privacy framework as it examines big data policy considerations and risks to privacy.

Below, ITI identifies a number of areas that OSTP can consider as it develops a road map of the policy issues to be considered in connection with big data.

A. Risk minimizing technologies and policies

As discussed at the MIT Workshop, big data encompasses predicated data analysis (uncovering results from what is known to be available in the data), to non-predicated analysis, where big data can reveal new insights or patterns not known to exist within the data prior to the analysis. To the extent certain protections as outlined in the Consumer Privacy Bill of Rights are challenged in these contexts, technological tools and policies may be useful in minimizing privacy risks.

---

http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Fair Information Practice Principles (FIPPs), which include the concepts of notice, choice, data minimization, purpose specification, and use limitation, serve as the foundation for both policy and regulatory frameworks for privacy. FIPPs are incorporated into the privacy frameworks developed by multilateral fora, such as the Organization for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation (APEC) forum. The FIPPs can also be seen in legislative frameworks, such as the European Union's privacy regulatory framework, as well as certain U.S. privacy laws.

[7] White House Report, at 6.

[8] 15 U.S.C §§ 41-58, as amended.

For example, technological tools that can render personal data pseudonymous, anonymous, or de-identified is one way of addressing privacy risks. Further technological research into the development of the robust tools in this area is necessary. When the analysis of data (whether it is the entirety of the data being examined, or a subset thereof) in an anonymous, pseudonymous or de-identified form can be achieved through technological means without adversely affecting the quality of the results derived from the analysis, privacy risks can be minimized. Such analysis would not implicate the privacy concerns that can be present when data is linked to individuals. We further note that the measures that an organization should take to anonymize, pseudonymize, or de-identify data will necessarily depend on the intended use of the data, as well as the available methodology and technology for such modifications. As recognized by the Federal Trade Commission, "the nature of the data at issue and the purposes for which it will be used are also relevant" in determining what would constitute an organization achieving a "reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[9] We further note that an organization's practices with respect to the data will inform the measures necessary to achieve that "reasonable level of justified confidence."

B. Risk-based approach to big data use and analysis

The development of a risk-based analysis approach to determine whether a proposed use or analysis of data is appropriate should be considered as a methodology to minimize the privacy impact on individuals, particularly where certain

[9] See FTC, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policy-makers, FTC Report ("FTC Privacy Report") (Mar. 2012), p. 21, *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

FIPPs protections are impractical. A risk assessment, that could be based on a common set of factors, might include the type of data, how the data was amassed, the public interest in the use of the data, the benefits of the use, the security measures in place, and the potential harmful impact to individuals resulting from the use. This risk assessment exercise could serve not only as a determination as to whether a particular use or analysis should go forward, but also to implement privacy-protecting safeguards. Through this risk assessment that considers privacy at the outset—essentially, a privacy impact assessment—data analyzers could determine a proper balance of risk minimization and maximum benefit from the data.

C. Accountability

The well-known concept of "accountability" in the privacy realm applies equally in the big data context, and would be useful in connection with both the risk-minimizing technologies and risk-based approach to big data use and analysis discussed earlier. Generally, accountability requires that organizations develop and put into place processes that foster compliance with their privacy-related commitments. Further, it requires organizations to describe how their processes comport with those commitments and be prepared to demonstrate them.

For example, accountability would require organizations to develop processes—and be able to describe such processes—to determine if and when anonymization, pseudonymization, de-identification and other privacy-protecting measures are appropriate. The accountability requirement would similarly apply in the risk assessments that data analyzers would conduct in connection with intended use of data. Organizations would need to develop processes—and be able to describe such processes—related to the conducting of risk assessments based on commonly understood use-based best practices that could be developed in connection with big data.

D. Consumer education

"Big data"—the term of art generally used to represent large-scale data analytics—is not easily understood by consumers. Improved consumer education on how data analytics are being used to provide benefits in a multitude of areas, such as health, transportation, and medicine should be developed. Long disclosures that are not easily understood may not be the most effective way to inform consumers about data practices. Research into the scope of information to be shared with consumers and how that information can be effectively imparted should be a priority, and we encourage the administration to support such research.

IV. International landscape

Big data magnifies the already challenging international environment where barriers to cross-border data flows impede the information that may be available to emerging big data services that can be provide benefits to individuals. Various types of global restrictions to data flows, from localization requirements to overly restrictive data protection requirements, may also interfere with the potential for big data. Data localization requirements limit the availability of data sets for uses based on geographic location and data protection requirements may constrain collection or use of information. While there are legitimate reasons for data protection regulations, they need not be written or implemented in a way that overly constrains collection or use of information for legitimate purposes.

We urge the administration to resist efforts by other jurisdictions to impose data localization restrictions, overly restrictive data protection regimes, and barriers to cross-border data flows. We further encourage the administration to support mechanisms that enable and facilitate cross-border data flows. For example, the U.S.-EU Safe Harbor enables the transfer of data from the U.S. to the EU and the continued

availability of this mechanism is critical across industry sectors—we urge the administration to ensure the continued availability of this mechanism.

Other international efforts to develop interoperable data protection and cross-border data flow regimes should also be supported by the administration. For example, the administration should continue its important work within the Asia Pacific Economic Cooperation forum (APEC) to promote APEC's Cross-Border Privacy Rules (CBPRs).[10] The APEC CBPRs are a set of privacy rules that are consistent with the APEC Privacy Framework, and CBPRs were developed to provide a flexible way for companies to demonstrate their trustworthiness and accountability for personal information. The ultimate goal is for participating companies to be able to transfer data within the APEC region without impediments.

Such cross-border transfer facilitation mechanisms are critical in the big data context in that they allow for the availability of data across jurisdictions and enable large-scale data analytics. The continued development of these transfer mechanisms should be a priority for the administration. A recent collaborative effort involving APEC CBPR's and one of the EU's data transfer mechanisms—Binding Corporate Rules—demonstrates progress in identifying the compatible elements of differing privacy systems.[11] More work needs to be done in this area—and should be supported by the administration—to identify common ground among differing systems in efforts to

[10] *See* APEC, APEC Cross-Border Privacy Rules System, Policies, Guidelines and Procedures, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

[11] *See* Joint Work between experts from the Article 29 Working Party and from APEC Economies, on A referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, (March 6, 2014) *available at* http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

promote interoperability.

* * *

ITI appreciates the opportunity to submit these comments to OSTP. 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.