CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

WILLIAM L. KOVACS
SENIOR VICE PRESIDENT
ENVIRONMENT, TECHNOLOGY &
REGULATORY AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062
(202) 463-5457

August 5, 2014

VIA ELECTRONIC FILING

Attn: Privacy RFC 2014
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230

Re: ***Big Data and Consumer Privacy in the Internet Economy*** **[Docket No. 140514424–4424–01]**

Dear Sir/Madam:

The U.S. Chamber of Commerce ("Chamber")[1] is pleased to submit these comments to the National Telecommunications and Information Administration ("NTIA") in response to its Request for Public Comment ("RFC") on "Big Data and Consumer Privacy in the Internet Economy."[2] These comments incorporate by reference the Chamber's response[3] earlier this year to the White House Office of Science and Technology's Request for Information regarding big data.[4] Given the benefits of big data, the Chamber urges NTIA to use caution and restraint as it examines this issue.

I. Data is a Key Driver of U.S. Innovation and Economic Growth

To help our economy continue to recover, the Chamber believes that big data will be a key component in the creation of jobs and innovation. Data is used in many beneficial ways in our economy and by our society, including but certainly not limited to: improving healthcare, enabling businesses to better understand and serve their customers, increasing access to credit, detecting and preventing fraud as well as authenticating individual identities, and refining the

---

[1] The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system.
[2] *Request for Comment Regarding Big Data and Consumer Privacy in the Internet Economy*, 79 Fed. Reg, 32714 (June 6, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-06-06/pdf/2014-13195.pdf. ("RFC").
[3] *U.S. Chamber Comment Letter to the White House Office of Science and Technology Regarding its Big Data Study* (filed Mar. 31, 2014), *available at* https://www.uschamber.com/comment/comment-letter-big-data-study.
[4] *Request for Information Regarding Government "Big Data,"* 79 Fed. Reg. 12251 (Mar. 4, 2014), *available at* http://www.gpo.gov/fdsys/pkg/FR-2014-03-04/pdf/2014-04660.pdf. ("*RFI*").

manufacturing of products.[5] As White House Counselor John Podesta said at the March 3, 2014, White House/Massachusetts Institute of Technology (MIT) big data workshop:

> 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.[6]

For example, the efficient use of big data allows manufacturers to reduce the cost of product development and assembly by up to 50 percent, and decrease the amount of required working capital by up to 7 percent.[7] Additionally, financial institutions may be able to better assess the creditworthiness of consumers and potentially grant credit to those who have been unable to obtain it (including those who have not yet established credit) by using big data analytics and not relying solely on credit scores.[8]

II. The Current Multi-Layered Privacy Approach to Privacy in the United States Protects Consumers While Enabling Innovation

The RFC requests comment on ‘‘big data" developments and how they impact the Consumer Privacy Bill of Rights that was proposed in the Administration's 2012 white paper on "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." In the United States, consumer privacy is protected by a flexible, multi-layered framework. Recognizing that the use of some sensitive types of data have a unique risk of harm, there are a variety of sector-specific federal laws (e.g., the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and the Health Insurance Portability and Accountability Act (HIPAA)) designed to protect certain types of information that if misused or accessed without authorization could result in real harm to consumers. Additionally, the Federal Trade Commission (FTC) has been aggressively asserting its authority under Section 5 of the FTC Act to prohibit unfair or deceptive acts or practices

---

[5] *See also*, Jeff Lundy, PhD, *Data for Good* (Jan. 17, 2014), *available at* http://www.uschamberfoundation.org/blog/post/data-good/31581; Rich Cooper, S*afer Cities through Data-Driven Crime Prevention* (Mar. 25, 2014), *available at* http://www.uschamberfoundation.org/blog/post/safer-cities-through-data-driven-crime-prevention/34326; and Rich Cooper, *The Promise and Challenges of Data-Driven Healthcare* (May 6, 2014), *available at* http://www.uschamberfoundation.org/blog/post/promise-and-challenges-data-driven-healthcare/34398.

[6] *Remarks as Delivered by Counselor John Podesta at The White House/MIT "Big Data" Privacy Workshop* at 2 (Mar. 3, 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/030414_remarks_john_podesta_big_data.pdf.

[7] McKinsey Global Institute, *Big Data – The Next Frontier for Innovation, Competition, and Productivity*, at 8, May 2011, *available at* http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx (*McKinsey Report)*.

[8] Comments of the Financial Services Roundtable to OSTP regarding Big Data at 3 (filed Mar. 31, 2014), *available at* http://fsroundtable.org/letter-re-big-data-request-information.

related to privacy. As a complement to these consumer protection laws, a variety of effective self-regulatory initiatives exist.

The White House acknowledged in its 2012 Consumer Privacy Bill of Rights proposal that:

> The consumer data privacy framework in the United States is, in fact, strong. This framework rests on fundamental privacy values, flexible and adaptable common law protections and consumer protection statutes, Federal Trade Commission (FTC) enforcement, and policy development that involve a broad array of stakeholders. This framework has encouraged not only social and economic innovations based on the Internet but also vibrant discussions of how to protect privacy in a networked society involving civil society, industry, academia, and the government.[9]

As it examines big data, NTIA should fully study the benefits of data and focus on how to enable more and better use of data.[10] Without fully understanding the capabilities and benefits of data, it will be impossible to understand the opportunity costs associated with limiting the use of data.[11] Beyond harnessing big data to answer specific questions, big data analysis allows "insights that could not be anticipated empirically or theoretically before the analysis took place….Instead, the data 'speak' and tell scientists something they did not know before."[12] Therefore, in addition to looking at data use, NTIA should also examine the implications to innovation and economic growth if this data is not allowed to be used. It is also worth noting that many of the benefits derived from data will come from business and scientific applications that do not involve the use of personal information.[13]

The RFC asks in Question 12 for comment on the White House Big Data Report's conclusion that big data could cause discrimination against individuals or groups. This concern needs to be considered in view of our nation's existing legal framework. The laws that prohibit unfair discrimination for credit, employment, housing and education are not subverted or rendered void by a person or an organization using its own big data or the big data of a third party to unfairly discriminate against a protected class. These

---

[9] *The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* at i (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[10] *See,* Comments of the Center for Data Innovation to OSTP Regarding Big Data at 2 (filed Mar. 31, 2014), *available at* http://www2.datainnovation.org/2014-ostp-big-data-cdi.pdf; and Comments of the Information Technology Industry Council to OSTP Regarding Big Data at 4 (filed Mar. 27, 2014), *available at* http://www.itic.org/dotAsset/bcae1b74-eb8e-4f01-a02d-7e8aa8bdaf0f.pdf.

[11] *Id.*

[12] Software & Information Industry Association Comments to OSTP Regarding Big Data at 2 (filed Mar. 31, 2014), *available at* http://www.siia.net/index.php?option=com_docman&task=doc_view&gid=5062&Itemid=318.

[13] *See,* Center for Data Innovation Comments at 2 and Information Technology Industry Council Comments at 4.

anti-discrimination laws are still in effect and all covered entities are still required to follow them. The use of big data does not change any of this.[14]

Businesses comply with the myriad of existing laws and regulations governing the use of information collected about consumers. Therefore, policymakers should restrain from acting unless there are specific, identified harms that cannot be addressed adequately by the current multi-layered approach toward privacy in the United States.

III. Focusing on Improper Uses of Big Data and the Harms Created, Rather than Focusing Heavily On Collection, Provides a Balanced and Scalable Approach Toward Big Data

Federal policy should recognize that differing risks of harm are caused by different types of data collection and usage. For example, there are fewer risks associated with non-personally identifiable data, especially when anonymized or aggregated, than with data that identifies a user. Similarly, encrypted data also results in reduced risk. Therefore, any federal policies in this area need to be flexible and adaptive to accommodate different uses of data along with rapidly developing technology.

The Chamber agrees with the recommendation in the President's Council of Advisors on Science and Technology's (PCAST) recent report on big data that "policy attention should focus more on the actual uses of big data and less on its collection and analysis."[15] Specifically, PCAST goes on to say:

> By actual uses, we mean the specific events where something happens that can cause an adverse consequence or harm to an individual or class of individuals….By contrast, PCAST judges that policies focused on the regulation of data collection, storage, retention, a priori limitations on applications, and analysis…are unlikely to yield effective strategies for improving privacy. Such policies would be unlikely to be scalable over time, or to be enforceable by other than severe and economically damaging measures.[16]

Additionally, societal benefits should be taken into account and certain uses, such as fraud prevention, may warrant fewer restrictions. For example, using big data to detect and prevent fraudulent activity can help protect financial institutions and their customers.[17] In 2012, attempted fraud against bank deposit accounts reached $14.8

---

[14] *See also,* Michael Hendrix, *Does Big Data Discriminate?* (June 26, 2014), *available at* http://www.uschamberfoundation.org/blog/post/does-big-data-discriminate/41553.

[15] President's Council of Advisors on Science and Technology, *Report to the President, Big Data and Privacy: A Technological Perspective* at xiii *(*May 2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[16] *Id.*

[17] *See*, Financial Services Roundtable Comments at 2.

billion; however, through the use of data analytics and other loss prevention measures, banks stopped $13 billion in fraudulent transactions.[18]

The Chamber believes that privacy protective technologies and practices will develop more rapidly in the marketplace as consumers look to protect their privacy through increasing interactions in the digital environment. As we see with the rapid increase in encrypted messaging, the market for companies selling easy to use privacy tools will grow organically in response to consumer demands. Cybersecurity professionals are continuously devising new and improved ways to protect data and combat threats from criminals and, sometimes, governments. Data scientists are working on new and improved means of disguising or de-identifying personally identifiable information.

IV. Conclusion

Thank you for the opportunity to provide comments on this important matter. The Chamber looks forward to working with NTIA as it considers the need for changes to U.S. privacy law.

Sincerely,

William L. Kovacs

[18] American Bankers Association, *Banks Stop $13 Billion in Fraud Attempts in 2012*, *available at* http://www.aba.com/Press/Pages/121213DepositAccountFraud.aspx.