Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 140514424-4424-01**]**

RIN 0660-XC010

Big Data and Consumer Privacy in the Internet Economy

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Request for Public Comment.

SUMMARY: The National Telecommunications and Information Administration ("NTIA") is requesting comment on "big data" developments and how they impact the Consumer Privacy Bill of Rights.

DATES: Comments are due on or before 5 p.m. Eastern Time on [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Written comments may be submitted by email to privacyrfc2014@ntia.doc.gov. Comments submitted by email should be machine-searchable and should not be copy-protected. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue N.W., Room 4725, Attn: Privacy RFC 2014, Washington, DC 20230. Responders should include the name of the person or organization filing the comment, as well as a page number, on each page of their submissions. All comments received are a part of the public record and will generally be posted to http://www.ntia.doc.gov/category/internet-policy-task-force without change. All personal identifying information (for example, name, address) voluntarily submitted by the

commenter may be publicly accessible. Do not submit Confidential Business Information or otherwise sensitive or protected information. NTIA will accept anonymous comments.

FOR FURTHER INFORMATION CONTACT: John Morris, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4725, Washington, DC 20230; telephone (202) 482-1689; email jmorris@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482-7002.

SUPPLEMENTARY INFORMATION:

Background: In January 2014, President Obama asked Counselor to the President John Podesta to lead a team of advisors, including Secretary of Commerce Penny Pritzker, Secretary of Energy Ernest Moniz, Office of Science and Technology Policy Director John Holdren, and National Economic Council Director Jeffrey Zients, in conducting a 90-day study examining how "big data" will transform the way individuals live and work and impact the relationships among government, citizens, businesses, and consumers.

On May 1, 2014, the working group published its findings and recommendations as *Big Data: Seizing Opportunities, Preserving Values* (the "Big Data Report").[1] The Big Data Report notes that big data analysis can "become an historic driver of progress, helping our nation perpetuate the civic and economic dynamism that has long been its hallmark."[2] At the same time, big data "raises considerable questions about how our framework for privacy protection applies in a big data ecosystem" and has the potential to "eclipse longstanding civil rights

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

[2] Big Data Report, Letter to the President from John Podesta, Counselor to the President; Penny Pritzker, Secretary of Commerce; Ernest J. Moniz, Secretary of Energy; John Holdren, Director, Office of Science and Technology Policy; and Jeffrey Zients, Director, National Economic Council (May 1, 2014).

protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[3]

The Big Data Report specifically addresses privacy and the Administration's Consumer Privacy Bill of Rights.[4] The Big Data Report notes that:

> As President Obama made clear in February 2012, the Consumer Privacy Bill of Rights and the associated Blueprint for Consumer Privacy represent "a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies." The Consumer Privacy Bill of Rights is based on the Fair Information Practice Principles. Some privacy experts believe nuanced articulations of these principles are flexible enough to address and support new and emerging uses of data, including big data. Others, especially technologists, are less sure, as it is undeniable that big data challenges several of the key assumptions that underpin current privacy frameworks, especially around collection and use. These big data developments warrant consideration in the context of how to viably ensure privacy protection and what practical limits exist to the practice of notice and consent.[5]

The Big Data Report then includes a specific recommendation:

> The Department of Commerce should promptly seek public comment on how the Consumer Privacy Bill of Rights could support the innovations of big data while at the same time responding to its risks, and how a responsible use framework, as articulated in Chapter 5 [of the Big Data Report], could be embraced within the framework established by the Consumer Privacy Bill of Rights. Following the comment process, the Department of Commerce should work on draft legislative text for consideration by stakeholders and for submission by the President to Congress.[6]

Also, on May 1, 2014, the President's Council of Advisors on Science and Technology ("PCAST") released *Big Data and Privacy: A Technological Perspective* (the "PCAST

---

[3] *Id*.
[4] In February 2012, the White House released *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the "Privacy Blueprint"), *available at*: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Privacy Blueprint includes the Consumer Privacy Bill of Rights, which applies seven Fair Information Practice Principles to contemporary commercial data practices. The Blueprint also calls for Congress to pass baseline consumer privacy legislation.
[5] Big Data Report at 61.
[6] *Id*.

Report").[7] The PCAST Report "was developed to complement and inform the analysis of [the Big Data Report] … examining the nature of current technologies for managing and analyzing big data and for preserving privacy, [and] considering how those technologies are evolving."[8]

Request for Comment: NTIA, the Department of Commerce agency principally responsible for advising the President on telecommunications and information policy issues, seeks comment on the questions set out below. NTIA and the Department invite public comment on these issues from all stakeholders, including the commercial, academic, and public interest sectors, legislators, and from governmental consumer protection and enforcement agencies. As part of this effort, NTIA and the Department will consider the submissions to the White House Office of Science and Technology Policy's March 4, 2014 Request for Information regarding big data (the "Big Data RFI").[9] There is no need for any individual or organization to resubmit points made in that process, but anyone who filed comments there is welcome to supplement their prior submission with responses to the questions below.

The Big Data Report, the PCAST Report, the submissions responding to the Big Data RFI, and the three big data workshops conducted in coordination with the Big Data Working Group, taken together, produced a broad range of ideas about and possible approaches to big data, and NTIA and the Department seek comment about some of those ideas and proposals below.[10]

---

[7] Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President, Big Data and Privacy: A Technological Perspective* (the "PCAST Report") (May 1, 2014), *available at*: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[8] PCAST Report, Letter to the President from John P. Holdren, Co-Chair, PCAST, and Eric S. Lander, Co-Chair, PCAST (May 1, 2014).

[9] The Big Data RFI is available at: https://www.federalregister.gov/articles/2014/03/04/2014-04660/government-big-data-request-for-information. Responses to the RFI are available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/big_data_rfi_responses.pdf.

[10] More information regarding the Big Data Privacy Workshops is available at: www.whitehouse.gov/issues/technology/big-data-review.

Broad Questions Raised by the Big Data Report and the PCAST Report:

1. How can the Consumer Privacy Bill of Rights, which is based on the Fair Information Practice Principles, support the innovations of big data while at the same time responding to its risks?

2. Should any of the specific elements of the Consumer Privacy Bill of Rights be clarified or modified to accommodate the benefits of big data?[11] Should any of those elements be clarified or modified to address the risks posed by big data?

3. Should a responsible use framework, as articulated in Chapter 5 of the Big Data Report, be used to address some of the challenges posed by big data? If so, how might that framework be embraced within the Consumer Privacy Bill of Rights? Should it be? In what contexts would such a framework be most effective? Are there limits to the efficacy or appropriateness of a responsible use framework in some contexts? What added protections do usage limitations or rules against misuse provide to users?

4. What mechanisms should be used to address the practical limits to the "notice and consent" model noted in the Big Data Report? How can the Consumer Privacy Bill of Rights' "individual control" and "respect for context" principles be applied to big data? Should they be? How is the notice and consent model impacted by recent advances concerning "just in time" notices?

5. Is there existing research or other sources that quantify or otherwise substantiate the privacy risks, and/or frequency of such risks, associated with big data? Do existing resources quantify or substantiate the privacy risks, and/or frequency of such risks, that arise in non-big data ("small data") contexts? How might future research best quantify or substantiate these privacy risks?

6. The Privacy Blueprint stated:

> The Administration urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights … Congress should act to protect consumers from violations of the rights defined in the Administration's proposed Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data. The legislation should permit the FTC and State Attorneys General to enforce these rights directly … To provide greater legal certainty and to encourage the development and adoption of industry-specific codes of conduct, the Administration also supports legislation that authorizes the FTC to review codes of conduct and

[11] Big Data Report at 48, 61.

grant companies that commit to adhere—and do adhere—to such codes forbearance from enforcement of provisions of the legislation.[12]

How can potential legislation with respect to consumer privacy support the innovations of big data while responding to its risks?

Specific Questions Raised by the Big Data Report and the PCAST Report:

7. The PCAST Report states that in some cases "it is practically impossible" with any high degree of assurance for data holders to identify and delete "all the data about an individual" particularly in light of the distributed and redundant nature of data storage.[13] Do such challenges pose privacy risks? How significant are the privacy risks, and how might such challenges be addressed? Are there particular policy or technical solutions that would be useful to consider? Would concepts of "reasonableness" be useful in addressing data deletion?

8. The Big Data Report notes that the data services sector is regulated with respect to certain uses of data, such that consumers receive notice of some decisions based on brokered data, access to the data, and the opportunity to correct or delete inaccurate data. The Big Data Report also notes that other uses of data by data brokers "could have significant ramifications for targeted individuals."[14] How significant are such risks? How could they be addressed in the context of the Consumer Privacy Bill of Rights? Should they be? Should potential privacy legislation impose similar obligations with respect to uses of data that are not currently regulated?

9. How significant are the privacy risks posed by unindexed data backups and other "latent information about individuals?"[15] Do standard methods exist for determining whether data is sufficiently obfuscated and/or unavailable as to be irretrievable as a practical matter?

10. The PCAST Report notes that "data fusion occurs when data from different sources are brought into contact and new, often unexpected, phenomena emerge;" this process "frequently results in the identification of individual people," even when the underlying data sources were not linked to individuals' identities.[16] How significant are the privacy risks associated with this? How should entities performing big data analysis implement individuals' requests to delete personal data when previously unassociated information becomes associated with an individual at a subsequent date? Do existing systems enable entities to log and act on deletion requests on an ongoing basis?

---

[12] Privacy Blueprint at 35.
[13] PCAST Report at 39.
[14] Big Data Report at 45.
[15] PCAST Report at 39.
[16] *Id.* at 21.

11. As the PCAST Report explains, "it is increasingly easy to defeat [de-identification of personal data] by the very techniques that are being developed for many legitimate applications of big data."[17] However, de-identification may remain useful as an added safeguard in some contexts, particularly when employed in combination with policy safeguards.[18] How significant are the privacy risks posed by re-identification of de-identified data? How can de-identification be used to mitigate privacy risks in light of the analytical capabilities of big data? Can particular policy safeguards bolster the effectiveness of de-identification? Does the relative efficacy of de-identification depend on whether it is applied to public or private data sets? Can differential privacy mitigate risks in some cases? What steps could the government or private sector take to expand the capabilities and practical application of these techniques?

12. The Big Data Report concludes that "big data technologies can cause societal harms beyond damages to privacy, such as discrimination against individuals and groups" and warns "big data could enable new forms of discrimination and predatory practices."[19] The Report states that "it is the responsibility of government to ensure that transformative technologies are used fairly" and urges agencies to determine "how to protect citizens from new forms of discrimination that may be enabled by big data technologies."[20] Should the Consumer Privacy Bill of Rights address the risk of discriminatory effects resulting from automated decision processes using personal data, and if so, how? How could consumer privacy legislation (either alone or in combination with anti-discrimination laws) make a useful contribution to addressing this concern? Should big data analytics be accompanied by assessments of the potential discriminatory impacts on protected classes?

Possible Approaches to Big Data Suggested by the Reports and the Big Data Workshops:

13. Can accountability mechanisms play a useful role in promoting socially beneficial uses of big data while safeguarding privacy? Should ethics boards, privacy advisory committees, consumer advisory boards, or Institutional Review Boards (IRBs) be consulted when practical limits frustrate transparency and individuals' control over their personal information? How could such entities be structured? How might they be useful in the commercial context? Can privacy impact assessments and third-party audits complement the work of such entities? What kinds of parameters would be valuable for different kinds of big data analysts to consider, and what kinds of incentives might be most effective in promoting their consideration?

14. Would a system using "privacy preference profiles," as discussed in Section 4.5.1 of the PCAST Report, mitigate privacy risks regarding big data analysis?[21]

15. Related to the concept of "privacy preference profiles," some have urged that privacy

[17] *Id.* at 38.
[18] *Id.* at 39.
[19] Big Data Report at 51, 53.
[20] *Id.* at 49.
[21] PCAST Report at 40-41.

preferences could be attached to and travel with personal data (in the form of metadata), thereby enabling recipients of data to know how to handle the data.[22] Could such an approach mitigate privacy risks regarding big data analysis?

16. Would the development of a framework for privacy risk management be an effective mechanism for addressing challenges with big data?[23]

17. Can emerging privacy enhancing technologies mitigate privacy risks to individuals while preserving the benefits of robust aggregate data sets?

18. How can the approaches and issues addressed in Questions 14-17 be accommodated within the Consumer Privacy Bill of Rights?

19. What other approaches to big data could be considered to promote privacy?

20. What other questions should we be asking about big data and consumer privacy?

Dated: June 3, 2014.

Angela M. Simpson,
Deputy Assistant Secretary for Communications and Information.

[FR Doc. 2014-13195 Filed 06/05/2014 at 8:45 am; Publication Date: 06/06/2014]

[22] *Id.* at 41.
[23] *See* National Institute of Standards and Technology, Privacy Engineering Workshop (Apr. 9-10, 2014), *available at:* http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm.