Public Knowledge
1818 N St, NW
Suite 410
Washington, DC 20036

August 5, 2014

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

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

Dear Mr. Morris:

Public Knowledge, Benton Foundation,[1] Center for Digital Democracy, Common Cause, Consumer Federation of America, Consumer Watchdog, Free Press, New America Foundation's Open Technology Institute, U.S. PIRG, and World Privacy Forum ("Commenters") respectfully respond to your office's June 6 request for comments regarding the implications of the White House working group report *Big Data: Seizing Opportunities, Preserving Values* ("Big Data Report") on the Administration's Consumer Privacy Bill of Rights.

Commenters write in particular regarding the section of the Big Data Report that addresses "Data and Metadata."[2] In light of the Report's recognition that metadata merit robust privacy protections, we urge the Administration to clarify a section of its Consumer Privacy Bill of Rights framework that addresses existing legal protections for metadata under the Communications Act.[3] That section, titled "Amend Laws that Create

[1] The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.
[2] Exec. Office of the President, Big Data: Seizing Opportunities, Preserving Values 34 (2014) [hereinafter *Big Data Report*], *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[3] 47 U.S.C. §§ 222, 338, and 551.

Inconsistent or Confusing Requirements," could be read as support for a legislative proposal that eliminates privacy protections written into the Communications Act. The Administration should clarify the continuing importance and applicability of 47 U.S.C. §§ 222, 338, and 551.

Metadata Reveal an Enormous Amount of Sensitive Information About Individuals

Top privacy researchers have described the disturbing amount of information that can be derived from metadata, and in particular telecommunications metadata. For example, as Ed Felten explained in testimony before the Senate Judiciary Committee last year,

> [C]ertain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence and rape. Similarly, numerous hotlines exist for people considering suicide, including specific services for first responders, veterans, and gay and lesbian teenagers. Hotlines exist for sufferers of various forms of addiction, such as alcohol, drugs, and gambling.
>
> Similarly, inspectors general at practically every federal agency—including the NSA—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud. Hotlines have also been established to report hate crimes, arson, illegal firearms and child abuse. In all these cases, the metadata alone conveys a great deal about the content of the call, even without any further information.
>
> . . . .
>
> . . . . Today, wireless subscribers can use text messages to donate to churches, to support breast cancer research, and to support organizations such as Planned Parenthood. Similarly, after a policy change in 2012 by the Federal Election Commission, political candidates such as Barack Obama and Mitt Romney were able to raise money directly via text message.
>
> . . . .

> Metadata can expose an extraordinary amount about our habits and activities. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations.[4]

Felten went on to explain how metadata collected and aggregated over time can be used to construct even more information about an individual,[5] and how data mining of metadata across many individuals is even more revealing.[6]

And in a proceeding earlier this year under the section of the Communications Act that governs telecommunications customer proprietary network information ("CPNI"), computer scientist Vitaly Shmatikov explained to the Federal Communications Commission:

> By linking calls made by [an] individual and the locations of the corresponding cell towers obtained from the [call detail records ("CDRs")], it is very easy to reconstruct the entire "trajectory" taken by this individual throughout the day. These trajectories, also known as "mobility traces" or "mobility patterns," include, for example, the route of the person's highway commute and the path taken when walking his or her children to school. Mobility traces are even easier to re-identify than simple home/work location pairs, especially with the additional information such as the time of each call and the knowledge of other important locations in the person's life, such as their gym, favorite restaurant, or place of worship, which . . . can also be deduced from the anonymized CDRs. With just a

---

[4] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing before the S. Comm. on the Judiciary,* 113th Cong. 8-10 (2013) (statement of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University) *available at* http://www.judiciary.senate.gov/meetings/continued-oversight-of-the-foreign-intelligence-surveillance-act.

[5] *Id.* at 11 ("[A]ggregated telephony metadata allows the NSA to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, or the social dynamics of a group of associates.").

[6] *Id.* at 11-12 ("The work of . . . researchers suggests that the power of metadata analysis and its potential impact on the privacy of individuals increases with the scale of the data collected and analyzes.").

> little bit of additional information, an average mobility trace (i.e., a sequence of CDRs belonging to the same individual but taken at different locations) can be re-identified with high confidence.[7]

The White House Big Data Review team agrees:

> The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals. What protections this material and the information derived from it merit is now a pressing question.
>
> An equally profound question is whether certain types of data—specifically the "metadata" or transactions records about communications and documents, versus the content of those communications and documents—should be accorded stronger privacy protections than they are currently. "Metadata" is a term describing the character of the data itself. The classic example comes from telecommunications. The phone numbers originating and terminating a call, as metadata, are considered less revealing than the conversation itself and have been accorded different privacy protections. Today, with the advent of big data, both the premise and policy may not always be so straightforward.[8]

Metadata Should Be Accorded Stronger Privacy Protections Than They Are Currently

The Big Data Report raises the question of whether "the 'metadata' or transactions records about communications and documents . . . should be accorded stronger privacy protections than they are currently."[9] Commenters—and the American public—agree, with a resounding yes. For the reasons cited by experts such as Ed Felten and Vitaly Shmatikov—and

---

[7] Comments of Vitaly Shmatikov to the *Public Knowledge Petition for Declaratory Ruling,* WC Docket No. 13-306 at 2-3 (March 2, 2014), *available at* http://apps.fcc.gov/ecfs/document/view?id=7521087284.

[8] *Big Data Report* at 34.

[9] *Id.*

even the White House itself—the release of metadata raises substantial privacy concerns, and must be afforded vigorous protection.

Thus, there have been numerous recent legislative efforts to place limits on the surveillance authorities that the government has used to collect Americans' telecommunications metadata. Some Commenters have supported such proposals. Indeed, there is broad public support for such efforts, and a general consensus among the American public that reform is necessary.

Protection of Telecommunications' Metadata Must Include Limitations on Both Compelled and Voluntary Disclosure of That Information

Several of the below-signed groups support current legislative proposals to limit the circumstances under which the government can compel disclosure of telecommunications metadata, but such proposals would be meaningless without corresponding limitations on voluntary disclosure. Without limitations on voluntary disclosure, the government could easily circumvent safeguards by merely purchasing the information that it cannot compel.

The Communications Act Already Contains the Necessary Limitations on Voluntary Disclosure of Telecommunications Metadata

Appropriately, where telecommunications metadata is concerned, the Communications Act already includes some of the strongest protections on the books. 47 U.S.C. § 222, "Privacy of Customer Information," accomplishes the following regarding customer proprietary network information ("CPNI"):

- Greatly restricts the circumstances in which a carrier may use CPNI for marketing purposes
- Requires opt-in consent before carriers may use, disclose, or permit access to CPNI
- Affords customers the right to inspect their own information
- Grants the Federal Communications Commission rulemaking authority over CPNI

And the rules promulgated by the FCC regarding CPNI detail:

- When carriers may use CPNI without customer consent
- What type of consent is sufficient when consent is required
- Standards for maintenance of CPNI (including an annual compliance certificate)
- Standards for disclosure of CPNI, when it is allowed
- What to do in the event of a CPNI security breach

The statute and the rules are remarkably comprehensive, constituting an important limitation on the carriers' ability to voluntarily disclose customers' private metadata with others.

The Communications Act Likewise Protects Satellite and Cable Subscribers' Metadata

Just as 47 U.S.C. § 222 protects telecommunications subscribers' metadata, 47 U.S.C. §§ 338 and 551 protect satellite subscribers' and cable subscribers' metadata, respectively. Together, 47 U.S.C. §§ 222, 338, and 551 represent Congress's determination that where consumers have limited options for service providers and have no choice but to share deeply private information with whomever their service provider is, the default privacy policy should be highly protective.

The Administration Should Clarify Its Recommendation Regarding the Privacy-Protecting Provisions of the Communications Act

According to the White House's Consumer Privacy Bill of Rights framework issued in February 2012,

> Because existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for

> enforcing the Consumer Privacy Bill of Rights against communications providers.[10]

A footnote following this sentence cites 47 U.S.C. §§ 222, 338, and 551, and therefore could be read to support implicitly the elimination of those sections.[11]

But given the privacy implications of metadata, which the White House has recognized, it cannot be the case that the Administration supports eliminating the provisions of the Communications Act that protect metadata—indeed, among the strongest and most comprehensive privacy laws we have. It would not make sense to replace these provisions with the Consumer Privacy Bill of Rights, which constitutes weaker regulation in a number of ways, including that it does not grant rulemaking authority and does not appear to include opt-in consent by default.

Thus the Administration should clarify that it does not support eliminating 47 U.S.C. §§ 222, 338, and 551 or rolling the protections codified therein into the proposed Consumer Privacy Bill of Rights. Rather, any new jurisdiction over telecommunications privacy that is granted to the Federal Trade Commission should coexist with the FCC's jurisdiction.

Respectfully submitted,

Public Knowledge
Benton Foundation
Center for Digital Democracy
Common Cause
Consumer Federation of America
Consumer Watchdog
Free Press
New America Foundation's Open Technology Institute
U.S. PIRG
World Privacy Forum

By: _____

Laura M. Moy
Public Knowledge
1818 N St, NW
Suite 410
Washington, DC 20036
(202) 861-0020 ext. 106

[10] Exec. Office of the President, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digtial Economy* at 39 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[11] *Id.* at n.49.