TECHNOLOGY POLICY INSTITUTE

October 17, 2016

Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street SW
Washington, DC 20554

RE: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

I would like to submit the attached commentary for the record regarding the "Protecting the Privacy of Broadband and other Telecommunications Services" Order and the corresponding fact sheet released by the Chairman's office.

Sincerely,
Scott Wallsten
President
Technology Policy Institute

409 12th Street SW • Suite 700 • Washington, DC 20024
Tel: (202) 828-4405 • Email: info@techpolicyinstitute.org • www.techpolicyinstitute.org

TECHNOLOGY POLICY INSTITUTE

Comments on Chairman Wheeler's October 2016 Privacy Fact Sheet

Scott Wallsten

In March, 2016 the Federal Communications Commission (FCC) issued a Notice of Proposed Rulemaking (NPRM) on privacy rules for Internet Service Providers (ISPs)[1] given their recent reclassification under Title II of the Communications Act.[2] On October 6, 2016, Chairman Wheeler released a "fact sheet" describing the Order, which is on the agenda for a vote at the FCC's October Open Meeting.[3]

Based on the fact sheet, the Order still seems to have at least two fundamental problems. First, the FCC continues to argue that ISPs should be subject to stricter privacy regulations than other industries not within the FCC's purview despite the lack of evidence supporting that argument and the potential effects on competition. Second, the Order does not seem to recognize that the use of data has large benefits and that an analysis of rules restricting its use must take into account not just the costs of potential data breaches but also the societal and personal benefits generated from using and innovating with data. The fact sheet implies that any rule restricting the collection and use of data is costless to the economy, which, by any accounting, is false.

Setting aside those issues, which have been discussed extensively in comments on the NPRM,[4] the fact sheet suggests some positive changes. One apparent improvement includes recognizing that not all data are equally sensitive. The Commission, however, giveth with one hand and taketh away with the other. The fact sheet does not take seriously its recognition of levels of data sensitivity by classifying almost all information as sensitive, and therefore subject to opt-in rather than opt-out.

Another apparent improvement is the Commission's decision not to ban broadband plans that include financial incentives related to privacy. However, the fact sheet seems to imply that ISPs may need approval from the Commission to use such plans.[5] Requiring regulatory approval for new business models is likely to reduce experimentation, and reducing the number of potential methods of paying for service is likely to harm consumers.

---

[1] The FCC and others have taken to calling ISPs Broadband Internet Access Service (BIAS) providers, but I choose to stick with the more colloquial "ISP." Just because.

[2] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," Notice of Proposed Rulemaking, (March 31, 2016).

[3] Tom Wheeler, "Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information," Fact Sheet, (October 6, 2016), http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1006/DOC-341633A1.pdf.

[4] See, generally, Thomas M. Lenard and Scott Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking" (Technology Policy Institute Working Paper, May 25, 2016), https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf.

[5] Specifically, the fact sheet says "The Commission would determine on a case-by-case basis the legitimacy of programs that relate service price to privacy protections."

I make these observations tentatively, however, because the text of the Order is not public. With regulations, details matter. While the fact sheet is about three-and-a-half pages long, the NPRM is 317 paragraphs and the entire NPRM document, including appendices and commissioner comments, is 147 pages long. Without the text of the actual order it is not possible for anyone outside the Commission—regardless of their general views on privacy—to have a fully-formed opinion of the Order on the basis of a fact sheet that has no legal significance. As Goldfarb, Tucker, and Wagman (2016) noted in responding to the NPRM,

> … we want to emphasize that the precise nature of the rules will matter a great deal. Extensive efforts should be taken to collect data that illuminate the burden that any new rules will impose on customers hoping to switch providers and the burden any new rules will impose on advertisers, whether incumbent or entrant.[6]

We do not yet know whether the Commission has gathered or analyzed any new data to evaluate the effects of the rules. Nevertheless, we can glean some insights from the fact sheet, including areas that appear to have improved and others that have not since the NPRM was published. The remainder of this note discusses those glimpses into the Order.

"Sensitive Data" and Opt-In

The NPRM proposed three data protocols by type of data: No approval required to collect the data necessary to provide broadband service, opt-out approval for data used to market communications-related services, and opt-in approval for all other data.[7] All available research suggests that opt-in consent dramatically reduces participation.[8] Any data classified under opt-in is less likely to be available to support services, innovation, and competition, as we and others discussed in previous filings.[9]

The underlying problem with the classification proposed in the NPRM was that it appeared to be ad hoc—a classification proposed without any justification of the reasons behind it. According to the new fact sheet, the Order will keep the three-tier system (opt-in, opt-out, and no consent required), but now recognizes that the most restrictive tier should be reserved for the most sensitive data. As the fact sheet puts it, ISPs would have to obtain opt-in consent from consumers to use "sensitive information," use "non-sensitive information" unless consumers opt out, while "customer consent is inferred for certain purposes spelled out in the statute."[10]

---

[6] This quote was in the context of a discussion of the potential effects of the rules on the advertising market. I am quoting it in a broader context here, but I believe it is appropriate given the entirety of their remarks. Avi Goldfarb, Catherine E. Tucker, and Liad Wagman, "Comments on 'Notice of Proposed RuleMaking: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'" (Comments Submitted to the FCC, May 20, 2016), https://ecfsapi.fcc.gov/file/60001996372.pdf#viewer.action=download.

[7] Federal Communications Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," para. 18.

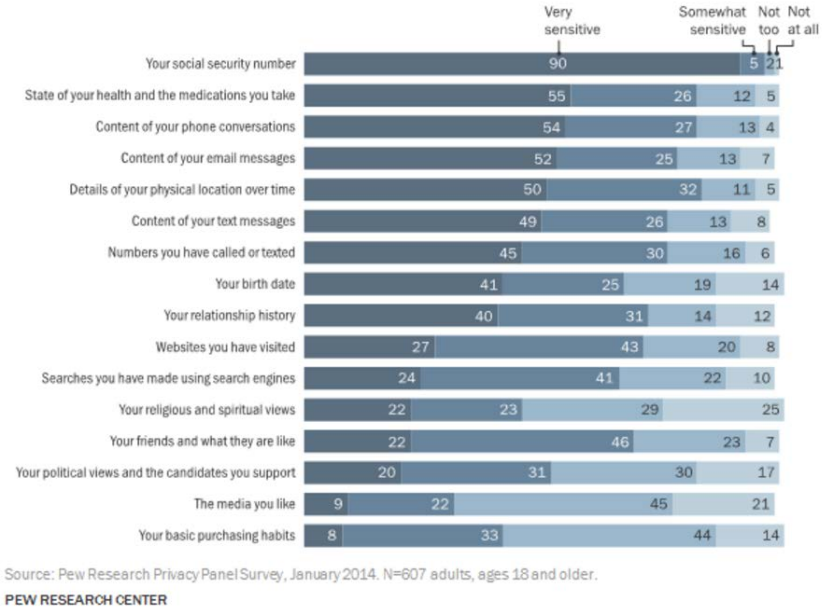
[8] Tom Lenard and I discussed the evidence in detail in our NPRM comments. Lenard and Wallsten, "An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking."

[9] Ibid.; Goldfarb, Tucker, and Wagman, "Comments on 'Notice of Proposed RuleMaking: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services.'"

[10] Wheeler, "Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information."

Categorizing data protocols by data sensitivity seems sensible. Presumably, any harms resulting from breaches of sensitive data are higher than the harms from breaches of non-sensitive data. And surveys show that people do not consider all their data to be similarly sensitive. For example, a 2014 Pew Survey showed that adults tend to believe different types of their information have different levels of sensitivity (Figure 1). By a wide margin, people were most concerned about their social security numbers with 90 percent reporting it to be "very sensitive" information. Health was a distant second, with 55 percent of respondents calling it "very sensitive."

Figure 1: Share of Adults Who Report Varying Levels of Sensitivity About Certain Types of Info[11]



However, the fact sheet suggests that the FCC has still not conducted any thoughtful analysis of what constitutes sensitive data. Instead, the Order appears to classify almost everything as sensitive data requiring opt-in, effectively annulling any benefits of the classification system.

The FCC includes social security numbers, financial information, and health information on its list of "sensitive" data requiring special attention. It also classifies children's data as sensitive, which, nearly everyone agrees, is appropriate and consistent with FTC rules. But the FCC's list also includes geo-location, web browsing history, app usage history, and the contents of communications. Web browsing and app usage history seem especially broad. The fact sheet does not provide the FCC's rationale for how it classified particular activities or why it would require opt-in consent for data consumers routinely trade for services elsewhere on the Internet.

[11] http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others

Deciding how to classify consumer information by sensitivity is not simple. Yet, if regulations are to be based on the classification, then the framework for classifying data should be a fundamental part of the analysis underlying the rule. Ideally, this analysis would take into account research on consumers' real-world behavior and, even better, would include experiments designed specifically to explore the effects of rules the Commission proposes.

The FCC, however, does not appear to have even tried to construct a coherent framework for categorizing or have studied how other agencies have gone about this task. Its broad definition would take it far beyond what the FTC or the European Union seem to consider sensitive.

The FTC has not explicitly defined what data should be considered "sensitive," *per se*, but has focused generally on financial and other information related to identity theft.[12] One careful summary of the EU's General Data Protection Regulation notes that it defines "sensitive personal data" as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data."[13] The FCC appears to consider sensitive personal data to be far more inclusive than the public as evidenced by surveys, the FTC, or the EU.

Conclusion

As a society we have benefited tremendously from the FTC's resistance to imposing opt-in across the board for uses of consumer data. It is impossible to know the counterfactual, but consider the possible outcomes if the FTC had headed down the path the FCC is now considering. In 2004, the Electronic Privacy Information Center objected to Google's then-new Gmail service largely because it did not take an opt-in approach, and called on consumers to avoid the email service and not even respond to people with @gmail.com addresses.[14] Suppose the FTC had responded to these objections by adopting a general opt-in approach to privacy. It is unlikely that we would have seen the virtuous circle created by new services supported by advertising, which created more demand for broadband services, which in turn, created additional incentives promoting online innovation along with more data available for analysis. The privacy rules described in the FCC's fact sheet could similarly disrupt this virtuous circle of innovation and demand.

It is not possible to know the source of new innovation. But creating a separate and more restrictive privacy regime for one industry without regard to the costs can only harm competition, innovation, and ultimately consumer welfare.

---

[12] For example, the FTC notes that in cases it has brought against companies it has considered to be sensitive data "bank account and credit card numbers, birth dates, contact information, employers' names, and information about debts the consumers allegedly owed," as well as usernames and passwords. https://www.ftc.gov/reports/privacy-data-security-update-2015.

[13] The quote is from the summary, not the GDPR. http://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

[14] https://epic.org/privacy/gmail/faq.html. Note that I do not intend to malign EPIC with this example—the organization has done a great deal of good and important work.