September 7, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20553

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

Dear Chairman Wheeler:

The undersigned 37 organizations file this letter in response to some of the arguments made recently in the above-referenced proceeding. In particular, the Commission should resist some parties' requests for the creation of a special carve-out for "de-identified" customer information. Further, the FCC should resist calls to require opt-in consent only for sensitive information, as Congress did not intend for the Commission to make such a distinction. We also strongly encourage the Commission to prohibit mandatory arbitration clauses, which often leave consumers without any reasonable means of recourse.

De-identified Data

We urge the Commission to resist some parties' request for the creation of a special carve-out for "de-identified" customer information. There is no room in the statute to accommodate that request. Even if there were, it would be harmful to consumers to allow ISPs to make an end-run around privacy rules simply by removing certain identifiers from data, while leaving vast swaths of customer details largely intact.

Section 222 creates a dichotomy between "individually identifiable" customer proprietary network information and "aggregate customer information." Opponents of the broadband privacy proposal argue that the final rule should recognize a third, completely unmentioned and unregulated category of customer information, so-called "de-identified" customer PI. But as a number of consumer and privacy organizations have explained in the past, the statute cannot reasonably be read to accommodate ISPs' preferred exception for de-identified data.[1]

[1] "If Congress had wanted to create an exception to Section 222 for de-identified information it would have done so, just as it created other exceptions." In addition, under ISPs' formulation, "carriers would face more restrictions with respect to aggregate de-identified information than information that is de-identified but not aggregate—an absurd result." *Petition of Public Knowledge et al. for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent*, Reply Comments of Public

Not only does the statute not permit a carve-out for de-identified information, but such a carve-out would be extremely harmful to consumers. It is often trivial to re-identify data that has supposedly been de-identified. For example, researchers have been able to re-identify individuals based on web browsing history;[2] telephone metadata;[3] location history, such as where one works and lives;[4] and Genome Project data.[5] These examples illustrate the type of problem Congress was attempting to address in 1996 when it declined to create a statutory exception to Section 222 for disaggregated de-identified data.

Nor have ISPs presented any compelling arguments that such an exception would benefit consumers. The information that customers must share with their providers in order to obtain service rightfully belongs to the customers, not to the ISPs. The burden is on ISPs to demonstrate what information it wishes to de-identify, how it would go about conducting that de-identification, and how consumers would benefit as a consequence. But ISPs have not met that burden, and the FCC must therefore greet with extreme skepticism ISPs' vague claims of consumer benefits from de-identified data. If ISPs manage to make a convincing case to consumers in the future that consumers would benefit from non-service-related uses of de-identified information, they should have no problem obtaining the requisite affirmative consent to make those desired uses.

The FCC should also be skeptical of ISPs' desired de-identification carve-out because this category would easily become the exception that swallows the rule. Under the framework ISPs desire, ISPs would simply "de-identify" all their data to sell or use it for any purpose, despite how easy it is to re-identify that data to the detriment of consumers. This would undermine the purpose of the rule, which is to give consumers true choice through opt-in consent, and would present an attractive way for BIAS providers to circumvent the vital consumer protections that will be put in place by this rule.

Knowledge, Benton Foundation, Center for Digital Democracy, Center for Media Justice, Common Cause, Consumer Action, Electronic Frontier Foundation, Electronic Privacy Information Center, Free Press, New America Foundation's Open Technology Institute, and U.S. PIRG at 6 (Mar. 4, 2014), WC Docket No. 13-306.

[2] Steven Englehardt *et al*., *Cookies That Give You Away: The Surveillance Implications of Web Tracking* (2015), http://dl.acm.org/citation.cfm?id=2741679; Jonathan R. Mayer, *Third-Party Web Tracking: Policy and Technology* (2012), http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6234427. Re-identification based on web browsing history is particularly apt in the BIAS provider context.

[3] Jonathan Mayer *et al*., *Evaluating the Privacy Properties of Telephone Metadata*, Nat'l Academy of Sciences (2015), http://www.pnas.org/content/113/20/5536.full.

[4] Philippe Golle & Kurt Partridge, *On the Anonymity of Home/Work Location Pairs*, Seventh International Conference on Pervasive Computing (2009), http://link.springer.com/chapter/10.1007%2F978-3-642-01516-8_26.

[5] Latanya Sweeney *et al*., *Identifying Participants in the Personal Genome Project by Name*, Harv. U. Data Priv. Lab (2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257732.

The statute leaves no room for the de-identification category of data ISPs desire, and consumers would not benefit from it. The FCC should reject creating a carve-out for de-identified data and leave it up to ISPs to explain to their customers through the notice-and-opt-in-consent framework why de-identification is trustworthy and why customers should allow ISPs to use de-identified data for non-service-related purposes.

Distinguishing Sensitive Information from Non-Sensitive Information

The FCC should also resist calls to require opt-in consent only for sensitive information, as Congress did not intend for the Commission to make such a distinction. When Congress enacts a specific privacy law such as Section 222 of the Communications Act (like HIPAA, the Wiretap Act, and FERPA), passage of the law reflects Congress' determination that the information covered by the statute is intrinsically sensitive. For example, HIPAA protects medical records, regardless of sensitivity.[6] The Wiretap Act applies to all private communications, not just those that are deemed sensitive. No one would suggest that the Wiretap Act protects medical and financial conversations, and not others. And FERPA protects education records. This stands in contrast to the statutory framework of the general privacy regime enforced by the Federal Trade Commission (FTC), which carries out the broad and general mandate of Section 5 of the Federal Trade Commission Act across a number of different sectors. Distinguishing between sensitive and non-sensitive data may make sense within the context of the FTC's general and broad approach to privacy, but here Congress has given the FCC a direct and specific obligation to protect telecommunications customers' proprietary information, regardless of sensitivity.

Moreover, it is difficult, maybe impossible, for carriers to distinguish between sensitive and non-sensitive without actually looking at and assessing a customer's information to make that distinction—and it would be administratively difficult for the FCC to oversee any such distinction. The difficulty in distinguishing between sensitive and non-sensitive information is exacerbated by the fact that the sensitivity of information depends on context. As noted privacy scholar Paul Ohm has pointed out, some subset of consumers may consider sensitive a category of information that the majority of consumers do not. For example, many people do not consider individual movie ratings (on sites such as Netflix) to be sensitive.[7] But in a class-action privacy lawsuit against Netflix, the class representative was a person who felt that her sexual orientation could be deduced from her Netflix viewing record. The complaint alleged, "were her sexual orientation public

[6] Specifically, HIPAA covers "protected health information" (PHI), which is defined as individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium, with a few narrow exceptions. 45 CFR § 160.103. There are parallels between the information covered as PHI and CPNI.

[7] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

knowledge, it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's ability to live peaceful lives."[8]

Furthermore, as with ISPs' call for a de-identification carve-out, there is no demonstrated need for the FCC to water down privacy protections afforded to information some parties consider to be less sensitive. The Commission's proposed rule doesn't ban any activity; it only requires opt-in consent. As recent evidence suggests, companies have had no trouble successfully obtaining consumer consent under similar rules.[9] If the benefits to consumers are as good as ISPs have claimed, consumers will consent to allowing their ISPs access even to sensitive information. Thus, not only is protecting information based on sensitivity not in line with congressional intent, it is also difficult to implement and ultimately unnecessary.

Mandatory Arbitration

The FCC should not only adopt strong broadband privacy rules, but also adopt procedural safeguards to ensure that ISPs cannot violate the rules with impunity. The FCC should prohibit mandatory arbitration in privacy disputes. A majority of ISPs insert forced arbitration terms into their terms of service that require customers to forfeit their right to seek redress in court and initiate a private arbitration proceeding instead. The terms of service are take-it-or-leave it, where the consumer has no bargaining power and, in many cases, doesn't have the choice to opt out of the arbitration clause.

In a case involving a telecommunications provider, the U.S. Supreme Court broadly interpreted the Federal Arbitration Act of 1925 to allow companies to prohibit customers from joining together to seek redress in court as a class. In that case, *AT&T Mobility v. Concepcion*, the provider hid a prohibition on class actions in its cell phone contracts, forcing customers to arbitrate their claims on an individual basis.[10] AT&T customers alleged that they were charged a hidden $30 fee when they purchased phones advertised as free. The $30 charge, while a small amount relative to an individual customer, multiplied across millions of customers would amount to millions of dollars in ill-gotten gains. Yet, due to the class action ban, customers were prohibited from coming together as a class to seek redress.

This is now a common story. Justice Ruth Bader Ginsburg correctly stated that *Concepcion* and its progeny "have predictably resulted in the deprivation of consumers' rights to seek redress for losses, and turning the coin, they have insulated powerful

[8] *Doe v. Netflix*, Class Action Complaint, Case No. C09-05903, at 21 (Dec. 17, 2009), *available at* http://www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf.
[9] Reply Comments of Professor Lauren E. Willis to Federal Communications Commission (June 27, 2016), WC Docket No. 16-106, https://www.fcc.gov/ecfs/filing/1070776478772.
[10] 563 U.S. 333 (2011).

economic interests from liability for violations of consumer protection laws."[11] The Commission must take affirmative steps in this proceeding to ensure consumers are able to enforce their privacy rights in court, and prohibit these harmful arbitration clauses.

Pay for Privacy

Pay-for-privacy plans are very concerning because of their overall reduction in privacy and their potential to coerce consumers, particularly low-income consumers, to give away their privacy by charging a substantial sum unrelated to the actual value of the data. Plans that protect consumer privacy can cost up to $800 more per year.[12] Consumers should not have to choose between broadband and their right to privacy.

We appreciate the Commission's attention to these important issues and look forward to the passage of strong, enforceable consumer privacy rules.

Sincerely,

Access Humboldt
Access Now
Access Sonomo Broadband
American Civil Liberties Union
Appalshop, Inc.
Ashbury Senior Computer Community Center
Benton Foundation[13]
California Center for Rural Policy
Campaign for a Commercial-Free Childhood
Center for Digital Democracy
Center for Media Justice
Chicago Consumer Coalition
Color Of Change
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog

---

[11] DirecTV v. Imburgia, 577 U.S. ___, 136 S.Ct. 463, 477 (2015) (Ginsburg, J., dissenting).
[12] *See, e.g.*, Karl Bode, *Think Tank Argues that Giving Up Privacy Is Good for the Poor*, Techdirt (Aug. 18, 2016), https://www.techdirt.com/articles/20160816/07164935254/think-tank-argues-that-giving-up-privacy-is-good-poor.shtml.
[13] "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."

Demand Progress
Electronic Frontier Foundation
EPIC
Free Press
Greenlining Institute
Maryland Consumer Rights Coalition
Massachusetts Consumer Council
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
National Consumers League
National Digital Inclusion Alliance
Open Technology Institute at New America
Privacy Rights Clearinghouse
Public Health Advocacy Institute at Northeastern University School of Law
Public Knowledge
Southern California Tribal Digital Village
TURN
U.S. PIRG
Virginia Citizens Consumer Council
World Privacy Forum
X-Lab

cc: Commissioner Mignon Clyburn
Commissioner Jessica Rosenworcel
Commissioner Michael O'Reilly
Commissioner Ajit Pai