

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of

Protecting the Privacy of Customers of
Broadband and Other
Telecommunications Services

WC Docket No. 16-106

OPPOSITION TO PETITIONS FOR RECONSIDERATION

Filed by

Access Humboldt
Access Now
Access Sonoma Broadband
American Civil Liberties Union
Benton Foundation
California Center for Rural Policy
Campaign for a Commercial-Free Childhood
Center for Democracy and Technology
Center for Digital Democracy
Center for Economic Integrity
Chicago Consumer Coalition
Color of Change
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Consumers Union
Electronic Frontier Foundation
Massachusetts Consumers Council, Inc.
National Consumer Law Center
National Consumers League
National Digital Inclusion Alliance
New America's Open Technology Institute
Online Trust Alliance
Oregon Consumer League
Privacy Rights Clearinghouse
Public Knowledge
X-Lab

March 6, 2017

Public Interest Commenters, comprised of Access Humboldt, Access Now, Access Sonoma Broadband, American Civil Liberties Union, Benton Foundation,¹ California Center for Rural Policy, Campaign for a Commercial-Free Childhood, Center for Democracy and Technology, Center for Digital Democracy, Center for Economic Integrity, Chicago Consumer Coalition, Color of Change, Consumer Action, Consumer Federation of America, Consumer Federation of California, Consumer Watchdog, Consumers Union, Electronic Frontier Foundation, Massachusetts Consumers Council, Inc., National Consumer Law Center, National Consumers League, National Digital Inclusion Alliance, New America’s Open Technology Institute, Online Trust Alliance, Oregon Consumer League, Privacy Rights Clearinghouse, Public Knowledge, and X-Lab submit this opposition to the petitions for reconsideration of the FCC’s broadband privacy *Order*. In particular, these organizations oppose the petitions for reconsideration that argue the FCC should fully repeal the *Order*. On the contrary, the record shows that the FCC should retain the *Order* in its entirety.

I. The *Order* will provide vital consumer privacy protections.

The FCC enacted a thorough, consumer-protective privacy regime that focuses on ensuring that consumers have real choice, transparency, and security regarding the use and disclosure of information collected by their Internet service providers (“ISPs” or “BIAS providers”). The *Order* requires ISPs to obtain their customers’ affirmative consent before using and disclosing their web browsing history, application usage data, health data, finance data, and other sensitive information for marketing purposes and with third parties. In addition, ISPs must

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

be transparent about their privacy practices in a clear and comprehensible way. Further, the rule creates a breach notification regime that informs consumers when their information has been accessed by unauthorized parties and could cause harm.

These privacy protections are vital because consumers greatly value their privacy. Consumers often take steps to protect themselves against collection, use, and disclosure of their data. Consumers have also altered their online activity based on fears that their data may be compromised.² And most importantly, consumers wish that they had more privacy protections by default and wish the government would help ensure those protections are met.³ This rule provides those protections for ISP customers.

Further, the FCC's rule reflects common practices of ISPs. The record showed that ISPs can develop highly detailed and comprehensive profiles of their customers without those customers knowing about the practice.⁴ Nearly every unencrypted web page visited, app used, and message sent is likely collected and stored by the consumer's ISP. And worse, customers cannot reasonably avoid this collection. Some argue that ISPs do not collect comprehensive information from their customers because of the existence and use of encryption technology.⁵ But even with encryption (implemented at the discretion of the website operator, not the consumer), the ISP can still see the top-level and second-level domains accessed by its

² Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities>.

³ OTI Reply Comments at 21-27 (explaining how consumers have grown skeptical of their privacy and desire more protections).

⁴ See generally Center for Digital Democracy Comments, *Big Data Is Watching* (Mar. 2016), [https://ecfsapi.fcc.gov/file/1021752328610/ispbigdatamarch2016\(12\).pdf](https://ecfsapi.fcc.gov/file/1021752328610/ispbigdatamarch2016(12).pdf).

⁵ NCTA Petition at 14; USTA Petition at 9.

customers. Many Petitioners cite to a paper by Peter Swire that claims ISPs have a very narrow window into their customers' activities. But the record refuted Swire's paper extensively.⁶

Petitioners also rehash the argument that consumers will be confused by being provided more information and choice about the privacy practices of their ISPs.⁷ But privacy is contextual, and consumers know that different websites and services provide different levels of privacy.⁸ That said, whether consumers actually understand the privacy practices of their ISPs depends on the level of clarity with which privacy policies are drafted. Because privacy policies are often dense, unclear, and confusing, the default rules are important for protecting consumers against practices that may be obscured or not explained well. Opt-in protection for certain uses and disclosure of customer information will better protect consumers against those harmful practices.

The *Order* provides vital consumer privacy protections and the FCC should deny reconsideration.

II. The petitions for reconsideration merely relitigate issues already decided in the underlying proceeding and should be dismissed.

The FCC should not grant petitions for reconsideration that present issues already decided in the underlying proceeding. The Commission has consistently rejected petitions for reconsideration because “[r]econsideration will not be granted for the purpose of debating matters on which [the Commission has] already deliberated and spoken.”⁹ Further, “[r]econsideration is generally appropriate only where the petitioner...raises additional facts not

⁶ Upturn, *What ISPs Can See* (Mar. 2016); Paul Ohm Testimony at 3; EFF Comments at 1.

⁷ *E.g.*, NCTA Petition at 20-21; ACA Petition at 16-17.

⁸ *See* OTI Comments, at 7-9.

⁹ *In re Application of Eagle Radio, Inc.*, 12 FCC Rcd. 5105 at ¶7 (1997).

known or not existing until after the petitioner’s last opportunity to respond.”¹⁰ Most, if not all, of the petitions for reconsideration filed in this proceeding simply relitigate issues that were already decided in this proceeding and that were fully supported by the record.¹¹

The FCC should again reject arguments based on the petitioners’ policy disagreement over the proper classification of BIAS. While these parties may prefer that BIAS not be classified as a Title II service, the *Open Internet Order* is settled law¹² and their disagreement is irrelevant in this proceeding. Whether petitioners like it or not, BIAS providers are “telecommunications carriers” under the law. Thus, the FCC properly relied on its *Open Internet Order* and Title II reclassification to apply Section 222 of the 1996 Telecommunications Act to BIAS providers.

As Title II “telecommunications carriers,” BIAS providers are “common carriers” and therefore exempt from Section 5 of the FTC Act. This means the FTC’s privacy regime no longer applies to BIAS providers. Instead, Congress gave the FCC the authority, through Section 222 and other sections, to protect the privacy and security of customers of telecommunications services, which now includes broadband services. The FCC has, in this *Order*, ensured the continued protection of consumer privacy and ensured there will not be a gap left by the common carrier exemption.

However, the FCC is not obligated to, nor should it, enact the exact same privacy regime as the FTC. First, the record reflected consumer skepticism of current privacy regimes. For

¹⁰ Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers and Other Providers of Mobile Data Services, 29 FCC Rcd. 7515, 7518 ¶7.

¹¹ Indeed, petitioners make frequent reference to their own comments, letters, and notices of ex parte. For instance, CTIA references its own filings at least 43 times in its petition, in addition to many references to other industry comments.

¹² *USTA v. FCC*, 825 F.3d 674 (DC Cir 2016). En banc review or Supreme Court review is extremely unlikely.

instance, even under the FTC’s privacy regime, consumers still modified their behavior online to prevent losing control of data, and expressed a desire for more privacy protections enforced by government entities.¹³ Thus, it is simply incorrect to claim, as so many petitioners do, that the FTC’s regime is successful.¹⁴

Second, Section 222 of the Telecom Act is a substantively different source of authority for privacy protections than Section 5 of the FTC Act. Section 222 specifically applies to telecommunications carriers and specifically addresses “privacy of customer information.”¹⁵ It also takes into account certain aspects of owning and maintaining a network, including that a network provider has access to a vast amount of customer information to ensure the proper functioning of the network. Section 222 also has the general mandate of subsection (a), giving the FCC flexibility to protect customer information of all telecommunications carriers, not just phone customers. The FCC has the expertise over communications networks, so it is appropriate for the FCC to ensure customer privacy over such networks. Section 5 of the FTC Act, however, is broadly applicable to all interstate commerce. Privacy protections under Section 5 must fit the mold of essentially all sectors of the economy. Targeted privacy protections, such as those under Section 222, are more appropriate for the unique circumstances of broadband services, as Congress envisioned.

For these reasons, the FCC should reject the petitions for reconsideration and uphold the rule in its entirety.

¹³ *See supra*, footnotes 2-3.

¹⁴ *See, e.g.*, NCTA Petition at 16; US Telecom Petition at 4.

¹⁵ 47 USC §222.

III. Conclusion

The *Order* will provide vital consumer privacy protections that will help ensure consumers have choice, transparency, and security. There is no persuasive reason to reconsider the *Order*. In fact, there are many reasons, fully discussed in the record, that the FCC should retain the rule in its entirety. If the FCC repeals the rule, it will only ensure that consumers will have no privacy protections despite a clear Congressional directive and the pressing need for consumer protections.

Respectfully submitted,

/s/

Eric Null

New America's Open Technology Institute

740 15th St NW, Suite 900

Washington, DC 20005

CERTIFICATE OF SERVICE

I, Eric Null, hereby certify that on March 6, 2017, a copy of the foregoing Opposition to Petitions for Reconsideration was served by first-class mail, postage prepaid, upon the following:

Jonathan Banks
B. Lynn Follansbee
USTelecom
607 14th Street, NW, Suite 400
Washington, D.C. 20005

Steven K. Berry
Rebecca Murphy Thompson
Elizabeth Barket
Competitive Carriers Association
805 15th Street NW, Suite 401
Washington, DC 20005

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, DC 20007

Stephen E. Coran
S. Jenell Trigg
Paul A. Cicelski
Lerman Senter PLLC
2001 L Street, NW, Suite 400
Washington, DC 20036

Kenneth Glueck
Oracle Corporation
1015 15th St. NW, Suite 200
Washington, DC 20005

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris, Glovsky &
Popeo, P.C.
701 Pennsylvania Avenue, N.W., Suite 900
Washington, D.C. 20004

Stuart P. Ingis
Michael Signorelli
Robert Hartwell
Venable LLP
575 7th Street, NW
Washington, D.C. 20004

Julie M. Kearney
Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

Genevieve Morelli
Michael J. Jacobs
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, D.C. 20005

Thomas C. Power
Maria Kirby
Scott K. Bergmann
CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036

Brita D. Strandberg
Adrienne E. Fowler
Elizabeth B. Uzelac
Harris, Wiltshire & Grannis Llp
1919 M Street, N.W., 8th Floor
Washington, DC 20036

/s/ Eric Null
Eric Null