Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

Reply to Oppositions to Petition for Reconsideration

Matthew M. Polka
President and CEO
American Cable Association
875 Greentree Road
Seven Parkway Center, Suite 755
Pittsburgh, Pennsylvania 15220
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

Barbara S. Esbin
Cinnamon Mueller
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 872-6811

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW
Suite 400
Washington, DC 20007
(202) 342-8518

Counsel to the American Cable Association

March 16, 2017

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

Reply to Oppositions to Petition for Reconsideration

I. INTRODUCTION

The American Cable Association ("ACA") hereby replies to Oppositions to Petitions for Reconsideration of the Commission's October 27, 2016 *Privacy Order*.[1] Opponents have failed to undermine the compelling case for reconsideration articulated by ACA, other Petitioners and a broad spectrum of commenters filing in support of reconsideration.[2] This Reply focuses on why the Commission should reconsider and

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, 31 FCC Rcd 13911 (2016) ("Privacy Order" or "Order"). ACA's Reply is principally directed to the Oppositions filed by Center for Democracy & Technology, Free Press, Public Knowledge et al. and New America Foundation's Open Technology Institute. *See* Opposition of the Center for Democracy & Technology (filed Mar. 6, 2017) ("CDT Opposition"); Opposition of Free Press (filed Mar. 6, 2017) ("Free Press Opposition"); Opposition of Access Humboldt et al. (filed Mar. 6, 2017) ("Public Interest Commenters Opposition"); Opposition of Public Knowledge et al. (filed Mar. 6, 2017) ("Public Knowledge et al. Opposition") (collectively, "Oppositions").

[2] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Petition of American Cable Association for Reconsideration

rescind its broadband privacy rules in light of FCC Chairman Pai and Acting Federal Trade Commission ("FTC") Chairman Ohlhausen's pledge to work together on a new, "comprehensive and consistent framework" for protecting American's online privacy.[3]

A. Reconsideration Is Warranted Based on Numerous Material Omissions and Errors in the *Privacy Order*.

Reconsideration is permitted under Commission rules to allow the Commission to correct material errors and omissions in its decision-making.[4] ACA's Petition demonstrates that reconsideration of the *Privacy Order* is warranted in three principal areas.[5] First, the *Privacy Order* contains material errors regarding the Commission's legal authority to adopt the sweeping, prescriptive broadband privacy rules set forth in the Order or to apply its rules to categories of data beyond customer proprietary network information ("CPNI") as defined in the Communications Act.[6] Second, even if the Commission has legal authority to adopt the rules contained in the Order, it fails, in several respects, to provide an evidentiary basis for its rules, including its failure to properly weigh record evidence and meet its obligations under the Regulatory Flexibility

(filed Jan. 3, 2017) ("ACA Petition"). Eleven parties, representing nearly the entire ISP industry and other Internet companies, have filed petitions requesting reconsideration.

[3] *See* Joint Statement of FCC Chairman Ajit Pai and Acting FTC Chairman Maureen K. Ohlhausen On Protecting Americans' Online Privacy (rel. Mar. 1, 2017) ("FCC/FTC Joint Statement").

[4] 47 C.F.R. § 1.429(b).

[5] ACA's positions are shared by a broad array of industry petitioners and commenters. *See, e.g.*, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Petition of NCTA – The Internet & Television Association for Reconsideration at 22-23 (filed Jan. 3, 2017); Petition of the United States Telecom Association for Reconsideration at 2-3 (filed Jan. 3, 2017). *See also* Petition of Oracle for Reconsideration at 7 (filed Dec. 21, 2016) ("Oracle Petition").

[6] ACA Petition at 4-13.

Act ("RFA"), resulting in disproportionate burdens placed on small providers.[7] Importantly, the Commission's failure to conduct an adequate economic analysis in crafting its rules prevented it from providing a quantifiable description of their costs and considering means to mitigate disproportionate harms to small providers of broadband Internet access service ("BIAS") providers (i.e., Internet service providers or "ISPs").[8] Third, in adopting the data breach notification rules, the Commission failed to consider, address or appropriately balance arguments in the public interest, as it is required to do, resulting in rules that are overreaching in key respects, overly burdensome and out of sync with other federal and state policies and practices.[9]

Agency errors and omissions that violate the Communications Act, the source of the Commission's authority, as well as the RFA and the Administrative Procedure Act, cannot be characterized as anything but "material," and reconsideration is fully justified on these grounds alone. Opponents of reconsideration largely rely on unavailing procedural arguments, asking that the Petitions be dismissed because they present arguments already considered and rejected by the Commission.[10]

The standard for dismissal of Petitions for Reconsideration is discretionary, rather than mandatory. In its recent *Data Security Stay Order*, the Commission rejected arguments that Petitioners were unlikely to succeed on the merits, and stayed the data security rules based on its conclusion that Petitioners "are *uniquely* likely to succeed on

[7] *Id.* at 13-21. No Opponent of reconsideration even attempts to address or rebut this material omission.

[8] *Id.* at 19-20.

[9] *Id*.

[10] *See, e.g.*, Free Press Opposition at 6-9; Public Knowledge et al. Opposition at 8-11; Public Interest Commenters Opposition at 3-5.

the merits of their claim on reconsideration with respect to these requirements."[11] In doing so, the Commission specifically rejected assertions that its authority to grant reconsideration "is limited to [petitions] which rely on facts or arguments which have not been previously presented to the Commission," noting that the rules "simply permit the dismissal or denial of a petition" in such cases.[12] Most importantly, it observes that "the Commission *as it is currently constituted has not considered and rejected any arguments pertaining to the data security rule raised in the Petitions for Reconsideration.*"[13] The same, perforce, is true of Petitioners arguments with respect to *all* the broadband privacy and data breach notification rules, providing more than sufficient reason for reconsideration. Given the magnitude of the problems with the *Privacy Order*, it would be an abuse of discretion to dismiss the Petitions in this case.

B. Reconsideration Is Warranted in the Public Interest.

Reconsideration of the Commission's *2016 Privacy Order* is not only permitted, it is imperative if consumer online privacy expectations and desires are to be properly protected. ACA's characterization of the *Privacy Order* as a "train wreck" that cannot be patched up and placed back on the track is not, as Free Press suggests, "name calling" borne of "frustration" with the Commission's reclassification decision and application of the privacy provision of Title II to broadband ISPs.[14] It is, rather, an accurate

[11] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Order Granting Stay Petition in Part, WC Docket No. 16-106, ¶ 8 (rel. Mar. 1, 2017) ("Data Security Stay Order") (emphasis supplied). Significantly, the Commission further explained that "a majority of the current Commission dissented from the *2016 Privacy Order* because it did not agree with" an approach that "would subject ISPs to more burdensome regulation that other participants in the Internet ecosystem are subjected to by the FTC." *Id.*, ¶¶ 9-10.

[12] *Id.*, ¶11.

[13] *Id.*, ¶¶ 10-11.

[14] Free Press Opposition at 7. *See* ACA Petition at 3.

characterization of a flawed rulemaking launched on a set of false premises and assumptions. These include the scope of the Commission's legal authority – which informed the scope of the rules proposed, the purportedly unique visibility broadband ISPs have regarding customer online activity and their unique ability to develop highly detailed and comprehensive profiles of their customers.[15] These shortcomings led the Commission to propose and, with minor modifications, adopt an overly expansive set of controlling definitions of the customer proprietary information to be protected by cumbersome notice and opt-in requirements and a set of burdensome data breach notification requirements at odds with existing federal and state law.[16]

ACA has no quarrel with Opponents' position that subscribers must be able to protect the privacy of their sensitive online information, including information they must disclose to their ISPs to access the Internet,[17] but that right of privacy is not unlimited. The question on reconsideration is one of means, rather than ends. The NPRM's fundamental failure to correctly identify the key threats to online consumer privacy,

---

[15] *See, e.g.*, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, ¶ 4 (2016) ("NPRM"). The NPRM's reference to the 2012 FTC Privacy Report in its opening paragraphs selectively presents only those observations that comport to the Commission's preconceived notion of the omniscience of the broadband ISP in contrast to other Internet players. *See id.*; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* at 56 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Left out, for example, is the FTC's observation that ISPs serve only "as *a* major gateway to the Internet" (rather than a "gatekeeper"), that "[l]ike ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles," and its agreement with the concept that "any privacy framework should be technology neutral," concepts at odds with the Commission's ISP-centric, technology-specific privacy regime. *Id.* at 56.

[16] ACA Petition at 16-19.

[17] *See, e.g.*, CDT Opposition at 7-8, 10-12.

assess the degree to which traffic handled by ISPs is encrypted, correctly define the scope of information requiring opt-in protection, and conform its proposals to statutory constraints on the Commission's legal authority were compounded by the Commission's failure, in adopting the *Privacy Order*, to perform a sufficiently rigorous economic analysis of the impact of the proposals[18] and its failure to consider appropriately tailored, less-burdensome alternatives.

The correct definition of the information that is to be protected by providers is the foundational element of any successful privacy regime. Here, the rulemaking went off the rails from the outset by massively expanding the type of customer information subject to FCC privacy regulation[19] in derogation of cost-benefit considerations and in contravention of both the statute and consumer expectations regarding the privacy of their online activity.[20] Cumbersome opt-in protections for sensitive information that vary

[18] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Comments of Thomas Lenard and Scott Wallsten, Technology Policy Institute, at 4-5 (filed Mar. 3, 2017) (the *Privacy Order* fails to acknowledge that the rules would have any costs and implies no tradeoff exists between access to information and privacy, a recognition that is a necessary first step towards determining whether the new rules would lead to any incremental benefits beyond the rules that to apply to other companies).

[19] In its Petition, ACA demonstrated that the Commission exceeded its statutory authority by utilizing Section 222 to regulate BIAS providers and by creating an entirely new and overly expansive category of customer information to regulate. ACA Petition at 9-10. It then, contrary to established FTC precedent, includes within the category of "sensitive" PII web browsing and application usage history, and, by doing so, uniquely constrains the ability of ISPs, but not Internet edge providers, to use such information for marketing purposes without obtaining consent. This will only cause customer confusion and unfairly limit the ability of ISPs to use customer data for marketing purposes, while cementing the online advertising hegemony of Internet giants such as Google. *See id.* at 20-21. *See also* Oracle Petition at 1-2 ("The Order correctly recognizes that protecting consumer privacy online is 'fundamental,' but completely undermines that goal by handing Google the market to the obvious detriment of consumers; ISP-specific privacy rules that depart from the privacy approach of the [FTC] (which remains applicable to ISPs' edge provider competitors) will hurt competition.").

[20] Consumers understand that Internet companies have access to a great deal of information about them, and surveys show they want consistent protections for their online information from all players in the Internet ecosystem. *See Protecting the Privacy of Customers of Broadband*

according to *who* is holding the data and target only broadband ISPs will only serve to confuse consumers, fail to meet their online privacy expectations and skew the online marketplace.[21] The *Privacy Order*'s burdensome notice-and-choice rules magnify the problem by targeting only ISPs for particular burdens and limiting only ISPs' use of customer data to develop new and innovative products consumers may value, thus harming their competitive position vis-à-vis Internet edge providers unencumbered by similar constraints, results squarely contrary to the public interest.[22]

CDT attempts to defend the *Privacy Order* by pointing to how much more reasonable the only slightly less radical and burdensome rules adopted are than the NPRM's original proposals.[23] This illustrates rather than addresses the problem of a set of rules conceived to address a misconception about consumer privacy expectations and implemented through misapplication of a statutory provision intended for a far

---

and Other Telecommunications Services, WC Docket No. 16-106, Letter from Will Marshall, President, Progressive Policy Institute, to Marlene H. Dortch, Secretary, FCC, at 1 (filed May 26, 2016).

[21] Several Opponents counter by arguing that the Commission has already considered and rejected Petitioner's claims of customer confusion arising from opt-in requirements that apply only to ISPs and not edge providers; OTI notes that such sector-specific regulation of online privacy is "inevitable under current U.S. law." *See, e.g.*, CDT Opposition at 8; Public Interest Commenters Opposition at 3; OTI Opposition at 6-7, 9-10. These arguments fail for at least two reasons. First, the Commission "as currently constituted" has not considered and rejected Petitioners' claims concerning customer confusion and should take this opportunity to reconsider. Second, even if U.S. law provides for sector-specific privacy regulation, that does not mean that separate regimes, such as those administered by the FTC and FCC, cannot be better aligned to meet customer expectations and avoid skewing marketplace competition than the rules contained in the *Privacy Order*.

[22] *See, e.g.*, Oracle Petition at 2.

[23] *See* CDT Opposition at 13-14 (the FCC exercised "restraint" by declining to be prescriptive about either the format or specific content of privacy policy notices; the original NPRM proposal was revised in the Order to incorporate greater flexibility for opt-in consent only for use and sharing of sensitive information); *id.* at 21 (the FCC abandoned its original proposal to require enumerated data security requirements, further harmonizing with the FTC regime's flexible standard).

different service in a far different time. Nothing good could come from an NPRM as misguided as this, and nothing did. The *Privacy Order* creates significant compliance burdens without addressing consumers' expectations of consistent treatment regarding the privacy of their personal information online.[24] And, it bears noting, customer expectations of online privacy are rapidly evolving,[25] strongly suggesting that the FTC's more flexible framework for privacy and data security and *ex post* approach to privacy enforcement is better suited to meeting consumer expectations than the *Privacy Order*'s overly prescriptive broad and cumbersome opt-in regime.

The answer to the problem created by the *Privacy Order* is clear. The Commission should reconsider and retract the *Privacy Order*'s broadband privacy and data security rules. This will clear the path for the FCC Chairman Pai and Acting FTC Chairman Ohlhausen, who have pledged to work together, to harmonize the two agencies' approaches to privacy to the greatest degree possible to better meet consumer expectations of consistent treatment of their information across the Internet ecosystem.[26] The Commission should allow that process to play out.

---

[24] *See, e.g.,* FCC/FTC Joint Statement ("It does not serve consumers' interests to create two distinct frameworks—one for Internet service providers and one for all other online companies.").

[25] *See, e.g.*, Leah Burrows, *To be let alone: Brandeis foresaw privacy problems*, BRANDEIS NOW (July 24, 2013), *available at* http://www.brandeis.edu/now/2013/july/privacy.html (the expectation of privacy has changed since Brandeis' era thanks to Facebook, Foursquare, Twitter and other social media sites; "Today, many people voluntarily and actively give up their right 'to be let alone.'"); Doug Brake, Daniel Castro, and Alan McQuinn, *Broadband Privacy: The Folly of Sector-Specific Regulation*, ITIF at 6-7 (Mar. 2016), *available at* https://assets.documentcloud.org/documents/2730435/2016-Broadband-Privacy-Folly.pdf (showing a large percentage of customers trust ISPs more than the government with their data and find permitting tracking in exchange for lower prices an acceptable trade-off).

[26] *See* FCC/FTC Joint Statement ("All actors in the online space should be subject to the same rules, enforced by the same agency.").

Contrary to the claims of Opponents, broadband ISP consumer privacy will not be put at risk of a "privacy protection gap" during the Commission's deliberations on a new set of requirements.[27] The Commission has recognized that consumers have not been harmed by the lack of implementing regulations under Section 222 since its 2015 reclassification decision.[28] Nor is there reason to believe this will change. ACA members are committed to maintaining their excellent record of protecting subscriber privacy. BIAS providers are required to disclose their privacy policies as part of their Open Internet disclosures.[29] They remain subject to a variety of state and federal unfair and deceptive trade practices, data security and data breach laws, and have released a voluntary set of "ISP Privacy Principles" that cover transparency, consumer choice, data security and data breach notification and are consistent with the FTC's long-standing framework, and have committed to continue adhering to these obligations.[30] BIAS providers that also provide cable and VoIP services must comply, respectively, with the rigorous privacy mandates of Section 631 (cable subscriber privacy) and Section 222 (telecommunications carrier/interconnected VoIP CPNI privacy and data security

[27] *See, e.g.*, CDT Petition at 7-9 (the FCC is on the only agency with jurisdiction to protect the confidentiality of information possessed by ISPs as common carriers are exempt from the FTC's authority to protect against unfair and deceptive practices under Section 5); Public Interest Comments at 4.

[28] Data Security Stay Order, ¶ 17 ("While BIAS providers have not been subject to specific implementing rules for nearly two years now, they have been obligated to comply with Section 222 of the Communications Act of 1934, as amended; the Commission's interim guidance; and other applicable federal and state privacy, data security and data breach notification laws.").

[29] *Preserving the Open Internet, Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17905 (2010); *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015); 47 C.F.R. § 8.3.

[30] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Joint Associations Petition for Stay, Appendix, "ISP Privacy Principles" (filed Jan. 27, 2017); Data Security Stay Order, ¶ 17.

requirements). Collaborating with the FTC on a better approach than the overly prescriptive and burdensome regime created by the *Privacy Order* will not leave consumers with any less privacy protection than they enjoy today, while giving the currently constituted Commission the opportunity to chart a better course for ISP customer privacy for the future.

Respectfully submitted,

AMERICAN CABLE ASSOCIATION

By: 

Matthew M. Polka
President and CEO
American Cable Association
875 Greentree Road
Seven Parkway Center, Suite 755
Pittsburgh, Pennsylvania 15220
(412) 922-8300

Ross J. Lieberman
Senior Vice President of Government Affairs
American Cable Association
2415 39th Place, NW
Washington, DC 20007
(202) 494-5661

Barbara S. Esbin
Cinnamon Mueller
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 872-6811

Thomas Cohen
Jameson J. Dempsey
Kelley Drye & Warren LLP
3050 K Street, NW
Suite 400
Washington, DC 20007
(202) 342-8518

Counsel to the American Cable Association

March 16, 2017

Certificate of Service

I, Alma Hoxha, paralegal with the law firm of Cinnamon Mueller, hereby certify that a copy of the Reply was served via USPS on the 16th day of March, 2017 to the following:

Eric Null
New America's Open Technology Institute
740 15th St NW, Suite 900
Washington, D.C. 20005

Gaurav Larioa, Policy Counsel
Matthew F. Wood, Policy Director
Free Press
1025 Connecticut Ave, NW
Suite 1110
Washington, D.C. 20036

Natasha Duarte
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, D.C. 20005

Dallas Harris
Policy Fellow
Public Knowledge
1818 N Street NW, Suite 410
Washington, D.C. 20036

Angela J. Campbell
Chris Laughlin
Institute for Public Representation
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, D.C. 20001

Amina N. Fazlullah
Director of Policy
Benton Foundation
1875 K Street NW, Suite 400
Washington, D.C. 20006

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America
1601 I Street, NW, Suite 200
Washington, D.C. 20006

Katharina Kopp, Ph.D.
Deputy Director, Director of Policy
Center for Digital Democracy
1875 K Street NW, 4th Floor
Washington, D.C. 20036

Curtis J. Neeley, Jr.
380 W. 13th Street
Newark, AR 72562

Katie McInnis
Staff Attorney
Consumers Union
1101 17th Street, NW
Washington, D.C. 20036

Alma Hoxha
Paralegal