Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

PUBLIC KNOWLEDGE, CENTER FOR DIGITAL DEMOCRACY, AND BENTON FOUNDATION'S OPPOSITION TO PETITIONS FOR RECONSIDERATION

Dallas Harris
Policy Fellow
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

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

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

March 6, 2017

TABLE OF CONTENTS

I. Introduction

Public Knowledge, Center for Digital Democracy and the Benton Foundation[1] ("Opponents") submit this Opposition to the Petitions for Reconsideration regarding the Commission's *Broadband Privacy Order*.[2] Specifically, the Petitions for Reconsideration filed are repetitious of arguments that petitioners and several other commenters presented to the Commission through the course of the above captioned proceeding. The Commission adequately addressed these arguments, and failed to agree with petitioners. Absent presenting new facts or identifying a material omission, reconsideration of repetitious petitions is wholly unwarranted. Petitioners are simply asking a more favorable Commission to reverse the determinations of a previous Commission without any additional facts presented. Petitions for Reconsideration are designed to correct material errors or present new facts unavailable at the time of a final order, not to function as a political tool to change rules passed by a previous Commission.

II. Arguments Fully Considered and Rejected by the Commission Plainly do not Warrant Reconsideration.

As described in detail below, a majority of petitioners arguments were presented to the Commission throughout this proceeding. The Commission carefully examined these arguments and rejected them based on evidence in the record. It is well settled "that the Commission will not consider a petition for reconsideration that merely repeats arguments that the Commission

[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

[2] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, FCC 16-148, (rel. Nov. 2, 2016) ("*Broadband Privacy Order*"). This Opposition is in response to the Petitions for Reconsideration filed by the American Cable Association (ACA), Consumer Technology Association (CTA), CTIA, Joint Petition of Association of National Advertisers, American Association of Advertising Agencies, American Advertising Federation, Data & Marketing Association, Interactive Advertising Bureau, and Network Advertising Initiative (DMA et. al), ITTA, NCTA – The Internet and Television Association, Oracle, United States Telecom Association (USTA), and the Wireless Internet Service Providers Association (WISPA) (Jointly referred to as "petitioners").

has previously rejected."[3] Indeed, the Commission's rules expressly identify petitions for reconsideration that "[r]ely on facts or arguments that have been fully considered and rejected by the Commission within the same proceeding" as a type of petition that "plainly do[es] not warrant consideration by Commission," and therefore may be "dismissed or denied by the relevant bureau(s) or office(s)."[4] There is no justification for the Commission to deviate from its practice now.

For several different reasons, it would be inappropriate and unwise for the Commission to break with its longstanding rejection of petitions for reconsideration where the Commission has already deliberated and spoken.[6] As the Commission has recognized, considering petitions for reconsideration that are merely repetitious is inefficient.[7] For ease of administration, the Commission adjusted its rules to allow such petitions to be disposed of under delegated authority.[8] Further, if the Commission grants these petitions based on arguments previously adjudicated, the Commission risks encouraging other petitioners to merely repeat presented arguments in the future, leading to more unnecessary work for the Commission. There must be a time when the Commission's determinations are final. In addition, granting these petitions on the basis of any arguments previously presented would create a dangerous precedent, increase the

[3] *In the Matter of Promoting Diversification of Ownership in the Broad. Servs.*, 66 Communications Reg. (P&F) 67 (F.C.C. Jan. 4, 2017) (citing *Federal-State Joint Board on Universal Service*, Order, 19 FCC Rcd 22305, 22306, ¶ 4 (2004)); *In the Matter of Ensuring Continuity of 911 Commc'ns*, 31 F.C.C. Rcd. 10131 (2016) ("It is by now well settled that the Commission will not consider a petition for reconsideration that merely repeats arguments that the Commission has previously rejected."). *See, also In the Matter of Fed.-State Joint Bd. on Universal Serv. Bus. Serv. Ctr., Inc., Mobile Phone of Texas, Inc., & 3 Rivers Pcs, Inc.*, 19 F.C.C. Rcd. 22305, 22306 (2004); *Applications of Bennett Gilbert Gaines et al.*, Memorandum Opinion and Order, 8 FCC Rcd 3986, 3987 (Rev. Bd. 1993); *see, also, Metrocall, Inc. v. Southwestern Bell Tel. Co. et al.*, Order on Reconsideration, 17 FCC Rcd 4781, 4782-83, ¶ 5 (2002).

[4] 47 C.F.R. 1.429 (l)(3).

[6] *In re Application of Eagle Radio, Inc.*, FCC 97-47, 12 FCC Rcd. 5105 at ¶ 7 (1997) ("Reconsideration will not be granted for the purpose of debating matters on which we have already deliberated and spoken."); *Isis Broadcasting Group*, 8 FCC Rcd 24 (Rev. Bd. 1992).

[7] *Amendment of Certain of the Commission's Part 1 Rules of Practice and Procedure and Part 0 Rules of Commission Organization*, Report and Order, 26 FCC Rcd 1594, 1606 ¶¶ 27-28 (2011) (Revision of Recon Rules Order).

[8] *Id.*

partisanship that Chairman Pai has decried,[11] and create a new level of procedural uncertainty. The policy views of the current FCC majority with respect to the *Broadband Privacy Order* do not justify upsetting settled Commission practice.[12]

Further, petitioners have failed to identify a material omission or error. When the Commission comes to a determination at odds with petitioners' assertions, as long as that determination is reasonable and supported by the record, there is no material error.[13] Because petitioners' arguments are merely repetitious and do not identify a material error or omission in the original order nor raise additional facts not known or existing at petitioners' last opportunity to present such matters, the order should remain in place.[14]

III. The Commission Properly Classified Web Browsing and App Usage History as Sensitive Information.

A majority of petitioners disagree with the Commissions determination that web browsing and app usage history are sensitive information, arguing that the Commission should adopt the framework laid out by the Federal Trade Commission. However, it is clear that even with encryption, ISPs can glean information about political views, sexual orientation, and other types of sensitive information. As is true with call history and video viewing history, web browsing history is sensitive and should require affirmative consent before use by ISPs. This is consistent with the FTCs framework. In addition, commenters previously presented this

[11] Statement of Ajit Pai, Commissioner, Federal Communications Commission (rel. Jan 11, 2017), *available at https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0111/DOC-342990A1.pdf* (condeming the pursuit of partisan political agendas).
[12] *In re Application of Eagle Radio, Inc.*, FCC 97-47, 12 FCC Rcd. 5105 at ¶ 7 (1997) ("Reconsideration will not be granted for the purpose of debating matters on which we have already deliberated and spoken."); *Isis Broadcasting Group*, 8 FCC Rcd 24 (Rev. Bd. 1992).
[13] *See In the Matter of Promoting Diversification of Ownership in the Broad. Servs*., 66 Communications Reg. (P&F) 67 (F.C.C. Jan. 4, 2017).
[14] *In the Matter of Fed.-State Joint Bd. on Universal Serv. Bus. Serv. Ctr., Inc., Mobile Phone of Texas, Inc., & 3 Rivers Pcs, Inc.*, 19 F.C.C. Rcd. 22305, 22306 (2004); *Petition for Reconsideration by Acadiana Cellular General Partnership*, Order on Reconsideration, 20 FCC Rcd 8660, 8663 ¶ 8 (2006).

argument to the Commission in the proceeding and each argument was addressed in the *Broadband Privacy Order*.

A. Web browsing history and app usage history are sensitive information and classifying them as such is consistent with the FTC 2012 Privacy Report.

As the Commission explains in the *Broadband Privacy Order*, call detail information has long been considered sensitive by the Commission, regardless of whether a customer called their bank, a hospital, or a service that reports movie times.[15] Web browsing and app usage history are the digital equivalent to call history. Similar to call history and video viewing history, a comprehensive view of every site a customer visits can lead to sensitive information such as political beliefs, gender, age, race, income range, and employment status.[16] Web browsing history can also reveal reading history, another category of information well established as sensitive.[17] Web browsing history is so comprehensive that researchers have made detailed conclusions about human behavior based solely on the information ISPs can see.[18] Given the inferences ISPs can make with collection of even just the top-level domain of every website a customer visits, web browsing history is properly classified as sensitive.

---

[15] *See Broadband Privacy Order* at ¶ 181.

[16] *See e.g.*, New America's Open Technology Institute, The FCC's Role in Protecting Online Privacy, 5 (2016) (OTI White Paper); Julie Brill, Comm'r, Fed. Trade Comm'n, Net Neutrality and Privacy: Challenges and Opportunities, Keynote Address at Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality at 6 (Nov. 19, 2015), *available at* https://www.ftc.gov/publicstatements/2015/11/net-neutrality-privacy-challenges- opportunities ("Even if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits—as well as those of all members of your household.").

[17] *See* Paul Ohm Ex Parte Presentation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 4-5 (July 28, 2016); Future of Privacy Forum Reply Comments, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, 6-7 (July 6, 2016) (explaining that "sensitive data would include the content of detailed browsing histories"); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. Sup. Ct. 2002) (en banc) (protecting privacy in book purchases).

[18] Letter from Nick Feamster, Professor, Princeton University, to Tom Wheeler, Chairman, FCC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 at 1 (March 3, 2016), *available at* http://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf ("We can learn so much from this traffic that we've written papers with conclusions about human behavior solely based on our analysis of the traffic that ISPs can see.").

Video history, which is also analogous to web browsing and app usage history, has also long been classified by Congress as sensitive because it can reveal the same types of information web browsing history can reveal.[19] Congress specifically pointed to shopping habits and political views as justification for protecting video history.[20] As described above, web browsing history reveals the exact same information about customer habits, if not more. Thus, to properly protect sensitive details about consumers, the Commission correctly classified web browsing and app usage history as sensitive.

A majority of petitioners also argue classification of web browsing and app usage history as sensitive is inconsistent with the previous regulatory scheme established by the Federal Trade Commission.[21] This misinterprets both the FTCs framework and the broadband privacy rules. In 2012, the Federal Trade Commission released a report outlining a privacy framework that would apply to the entities under its jurisdiction.[22] This framework was the result of work by the FTC that began as early as 2009.[23] At that time, the pervasiveness of smartphones and internet access were on the rise, but data mining practices were not nearly as sophisticated as they are today. While the report considered whether both online and offline data should be protected, this discussion was limited to entities that collect data in both contexts, such as retailers and other

[19] The cable and satellite privacy provisions of the Act were created in significant part to protect the privacy of video viewing habits. 47 U.S.C. § 551; 47 U.S.C. § 338(i). Video rental records have also been recognized by Congress as worthy of particular privacy protection. VPPA, 18 U.S.C. § 2710 *et seq*.

[20] *See* H.R. Rep. No. 934, 98th Cong., 2d Sess. 29 (1984) ("Subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions.").

[21] *See, e.g.,* United State Telecom Association Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 1 (May 27, 2016) (USTA Petition").

[22] *See Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report (March 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 ("*2012 FTC Privacy Report*").

[23] *See* FTC, FTC Privacy Report, *available* at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report (The press release on this page highlights the FTCs efforts in developing its privacy framework.).

traditional commercial entities.[24] In classifying certain information as sensitive, the FTC focused its discussion mainly on web sites that might collect and market based on sensitive information.[25]

Notably, the only time the FTC mentions Internet Service Providers (ISPs) was to highlight that they raise " heightened privacy concerns."[26] The FCC's broadband privacy rules simply recognized that fact, while remaining consistent with the FTCs tested notice and choice, sensitivity-based framework. The broadband privacy rules implement the principles contained in the *2012 FTC Privacy Report*, but apply those principles to ISPs. Therefore, the *2012 FTC Privacy Report* is insufficient basis for any argument that all web browsing and app usage history is non-sensitive, and classifying that information as sensitive is in now way inconsistent with the FTC's framework.

B. The Commission previously considered and rejected the argument that web browsing and app usage history are not sensitive.

Throughout the above captioned proceeding, many of the petitioners and other commenters attempted to persuade the Commission that it should adopt the FTC's sensitivity based framework.[28] In response to those comments, the Commission adjusted its proposal to require opt-in consent for sensitive information and opt-out for non-sensitive information, which aligned the consumer choice mechanism with the FTC framework as described in the *2012 FTC*

[24] *2012 FTC Privacy Report* at 17-18.
[25] *See, e.g. 2012 FTC Privacy Report* at 60 (discussing whether information collected from teens should be sensitive); *Id* at 48 (determining a website that collects and markets health information should obtain opt-in consent.)
[26] *2012 FTC Privacy Report* at 73.
[28] *See, e.g.*, Comments of the American Cable Association, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 39-42 (May 27, 2016) ("ACA Comments"); Comments of the Competitive Carriers Association, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 5-8 (May 27, 2016) ("CCA Comments"); Comments of ITTA, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 13 (May 27, 2016) ("ITTA Comments").

Privacy Report.[29] Despite the Commission's willingness to adopt the FTC's sensitivity based framework, several petitioners insist the broadband privacy rules are not in line with the FTC framework because web browsing and app usage history should not be classified as sensitive information.[30]

As is true with many of the arguments presented in the petitions for reconsideration, the claim that web browsing and app usage history should be considered non-sensitive information was presented to the Commission during the proceeding.[31] In response to this this argument, the Commission provided a well-reasoned response, explaining why the Commission was persuaded by other evidence in the record.[32] Similarly to how the Commission treats all call history as sensitive, regardless of who a customer is calling, the Commission correctly declined to define a subset of non-sensitive web browsing history. Not only is this in line with the Commission's goal to harmonize the broadband privacy rules with the phone privacy regime, it is also good policy, given the amount of sensitive information ISPs can determine based on web history alone.[33]

---

[29] *See 2012 FTC Privacy Report*; *See, also, Broadband Privacy Order* at ¶ 172.

[30] *See, e.g.,* Consumer Technology Association Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 13 (May 27, 2016) (CTA Petition").

[31] *See, e.g.*, AT&T Ex Parte Presentation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 3 (Oct 17, 2016); Google Ex Parte Presentation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 1 (Oct 3, 2016); American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, Network Advertising Initiative Joint Ex Parte Presentation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 4 (Oct. 10, 2016).

[32] *Broadband Privacy Order* at ¶ 181- 190.

[33] *See, e.g.*, Comments of Electronic Frontier Foundation, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 4 (May 27, 2016) ("EFF Comments"); *see, also* 18MillionRising.Org Petition and Comments at 1 ("The tracking and cataloguing of consumers' online habits are especially harmful to marginalized communities, for whom information regarding immigration status, mental health, race, and religion can be particularly sensitive."); Julie Brill, Comm'r, Fed. Trade Comm'n, Net Neutrality and Privacy: Challenges and Opportunities, Keynote Address at Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality at 6 (Nov. 19, 2015), *available at* https://www.ftc.gov/publicstatements/2015/11/net-neutrality-privacy-challenges-opportunities ("Even if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits—as well as those of all members of your household.").

Petitioners fail to present any new facts, arguments, or identify a material error or omission explaining why the Commission should reconsider this finding.

IV. Section 222 gives the Commission the Requisite Authority to Impose Privacy and Data Security Obligations on Internet Service Providers (ISPs).

As explained in detail below, Section 222 gives the Commission authority to promulgate the broadband privacy rules. There is no reasonable interpretation of Section 222(a) that would suggest it does not apply to all telecommunications carriers. Nor is there any argument that ISPs are not telecommunications carriers under the Act. Further, petitioners previously argued this exact point to the Commission throughout the proceeding. The Commission properly considered and rejected those arguments.

A. Section 222 gives the Commission the requisite authority to impose privacy and data security obligations on Internet Service Providers (ISPs).

A plain reading of Section 222 makes it clear that the Commission has the authority to impose privacy and data security obligations on ISPs. Section 222(a) reads in full: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."[34] In the *2015 Open Internet Order*, the Commission classified ISPs as telecommunications carriers, placing them squarely under the jurisdiction of Section 222.[35] Notably, while the Commission elected to forbear from certain provisions in Title II, it chose to leave in place the obligations under Section 222.

[34] 47 U.S.C. § 222(a).
[35] *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5736-42, at ¶ 141, *aff'd United States Telecom Ass'n v. F.C.C.*, 825 F.3d 674 (D.C. Cir. 2016) (*2015 Open Internet Order*).

Moreover, some commenters and petitioners asserted telephone specific references in 47 U.S.C. §§ 222(e), 222(g), 222(h)(1) indicate that Section 222 was only meant to apply to telephony.[37] However, the Commission properly determined references to telephone in other parts of Section 222 do not limit the Commission's authority to telephone services under 222(a). Telephone specific references throughout Section 222 show the use of the term telecommunications carrier in Section 222(a) was meant to reach beyond telephony. If Congress intended for Section 222(a) to apply specifically to telephone services, it would have referred to telephone services instead of telecommunications carriers in general as it did throughout the statute when it intended to limit the scope of a provision. Lastly, specific references to Internet in Section 203 do not limit the Commission's ability to apply Section 222(a) to all telecommunications carriers. This question has been litigated and settled.[38]

B. The Commission Has Already Addressed Arguments that Section 222 Provides Insufficient Authority for the Rules Adopted in the Broadband Privacy Order.

Many petitioners argue Section 222 does not give the Commission the requisite authority to impose privacy and data security obligations on Internet Service Providers (ISPs).[39] Petitioners, in their comments and reply comments, repeatedly presented this argument to the

[37] *See, e.g.* Comments of Comcast, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 67 (May 27, 2017) ("Comcast Comments"); American Cable Association Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 4 (Jan 3, 2017) ("ACA Petition").
[38] *See USTA v. FCC,* 825 F.3d at 702-03 (rejecting petitioners' Section 230-based argument against reclassification of BIAS as a telecommunications service).
[39] *See, e.g.*, ACA Petition at 4; Association of National Advertisers, American Association of Advertising Agencies, American Advertising Federation, Data & Marketing Association, Interactive Advertising Bureau, Network Advertising Initiative Joint Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 6 (Jan 3, 2017) ("DMA Joint Petition"); CTIA Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 2 (Jan 3, 2017) ("CTIA Petition").

Commission.[40] In fact, some petitioners cite their comments and the comments of other petitioners to support the position that Section 222 was only meant to apply to voice services and cannot be extended to ISPs.[41] However, the Commission clearly addressed this claim in the *Broadband Privacy Order*.[42] Primarily, the Commission reaffirmed its decision in the *2015 Open Internet Order*, which reclassified ISPs as telecommunications providers.[43] The Commission then correctly stated Section 222(a) imposes a general duty on "every telecommunications carrier" to protect personal information.[44] The Commission also addressed the claim that the scope of Section 222 is not limited to voice telephony or related services.[45] Although petitioners may disagree with the Commission's findings, this argument was presented to the Commission and addressed in the *Broadband Privacy Order*.

Further, petitioners claim the only type of information the Commission is authorized to protect under Section 222(a) is customer proprietary network information (CPNI).[46] Here again, these arguments were presented to the Commission multiple times throughout the proceeding and directly addressed in the *Broadband Privacy Order*.[47] One of many specific examples is CTIA's reply comments, in which it explicitly argued "Section 222 does not permit the

[40] *See, e.g.*, ACA Comments at 11-13; Comments of the National Cable & Telecommunications Association, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 7-13 (May 27, 2016) ("NCTA Comments"); Comments of CTIA, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 16-23 (May 26, 2016) ("CTIA Comments").
[41] ACA Petition at 7.
[42] *See Broadband Privacy Order* at ¶ 334-342.
[43] *Id.* at ¶ 334; *2015 Open Internet Order* at ¶ 141.
[44] *Broadband Privacy Order* at ¶ 334 (citing 47 U.S.C. § 222(a)).
[45] *Id* at ¶ 336.
[46] ACA Petition at 6; CTIA Petition at 3; NCTA Petition for Reconsideration, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 6 (Jan 3, 2017)("NCTA Petition").
[47] *See e.g.*, CTIA Comments at 4; NCTA Comments at 14; *Broadband Privacy Order* at ¶ 359-60 (finding no reason that the basic scheme set forth in Section 222(c) to govern individually identifiable CPNI cannot not be replicated under Section 222(a) to govern customer PI more broadly); CCA Comments at 10-15.

Commission to protect information beyond CPNI."[48] After examining arguments presented in the record, the Commission determined "Section 222 imposes an enforceable duty on telecommunications carriers that is more expansive than the combination of duties set forth subsections (b) and (c)."[49]

V. The Commission Fully Considered and Rejected Claims that Sections 201 and 202 do not Provide Additional Authority.

Petitioners also assert that the Commission does not have authority under Sections 201 and 202 to impose the privacy and data security rules adopted in the *Broadband Privacy Order*.[50] Similar to the other arguments discussed in this opposition, several petitioners and other commenters presented this argument to the Commission throughout the course of the proceeding.[51] To demonstrate this point, one only needs to look at the CTIA Petition, where CTIA frequently cites to its own comments and reply comments.[52] The Commission also adequately addressed this argument in the *Broadband Privacy Order*.[53]

In the *2015 Open Internet Order*, the Commission determined that "practices that fail to protect the confidentiality of end users' proprietary information" are among the potential carrier practices that are "unlawful if they unreasonably interfere with or disadvantage end-user consumers' ability to select, access, or use broadband services, applications, or content."[54] As the Commission explains, because of the common carrier exemption in the Federal Trade Commission (FTC) implementing statute, the FTC has no authority to regulate telecommunications carriers, therefore Sections 201(a) and 202(b) provide an important backstop

[48] Reply Comments of CTIA, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 15 (July 6, 2016) ("CTIA Reply Comments").
[49] *Broadband Privacy Order* at ¶ 343.
[50] *See e.g.*, ACA Petition at 10; CTIA Petition at 22.
[51] *See e.g.* ACA Comments at 15; CTIA Comments at 59; CTIA Reply Comments at 26-29.
[52] *See* CTIA Petition at n.9.
[53] *Broadband Privacy Order* at ¶ 368.
[54] *See 2015 Open Internet Order* at ¶ 141.

to ensure there are no gaps in consumer protection.[55] Moreover, both the Commission and the FTC have long recognized that insufficient protection of consumer data would tend to run afoul of Section 201(b) and of Section 5 of the FTC Act.[56] Petitioners fail to present any new facts or identify a material error in the Commission's determination that Section 201 and 202 provides additional authority for the broadband privacy rules.

VI. Conclusion

For the foregoing reasons, Opponents urge the Commission to deny the petitions for reconsideration filed by ACA, CTA, CTIA, DMA et al., ITTA, NCTA, Oracle, USTA, and WISPA.

Respectfully submitted,

/s/ Dallas Harris

Dallas Harris
Policy Fellow
Public Knowledge
1818 N Street NW, Suite 410
Washington, DC 20036

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

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

[55] *Broadband Privacy Order* at ¶ 369.
[56] *See* FCC and FTC, Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, 65 Fed. Reg. 44053-02, 44054 (July 17, 2000).