Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

REPLY OF

NTCA–THE RURAL BROADBAND ASSOCIATION

TO OPPOSITIONS TO PETITIONS FOR RECONSIDERATON

To the Commission:

NTCA–The Rural Broadband Association (NTCA)[1] hereby files this Reply to Oppositions to Petitions for Reconsideration in the above-captioned proceeding.[2] NTCA submits that the fundamental infirmities of the new privacy rules are (a) the disparate treatment of broadband Internet access service (BIAS) providers and other broadband market participants and (b) the inaccurate factual analysis which conjectured that BIAS providers have a uniquely broader and deeper hold on user data than application and edge providers. NTCA submits that the petitions for reconsideration demonstrate the need to reconsider the rules and replace them with a reasoned and rational approach that ensures consumer protection while avoiding

[1] NTCA represents more than 800 independent, community-based telecommunications companies. All NTCA members are full service local exchange carriers and broadband providers, and many of its members provide wireless, cable, satellite, and long distance and other competitive services to their communities.

[2] NTCA has been an active participant in the instant proceeding, filing comments (May 27, 2016), reply comments (July 6, 2016), meeting with Commission staff) (*ex parte* appearances in September and October 2016), and most recently replying to the Paperwork Reduction Act notice (*see,* 82 Fed. Reg. 3313, Jan. 11, 2017) (March 13, 2017).

unnecessary marketplace confusion and costs. NTCA urges the Commission to be guided by Federal Trade Commission (FTC) policies that govern edge and application providers. That approach will ensure a consistent standard of care across the broadband marketplace. Consumers and providers will benefit from a uniform approach to privacy matters. The new rules that created regulations that apply to only one segment of the industry should be reconsidered and amended.

Numerous parties filed for petitions for reconsideration of the new rules. The petitions address numerous issues, including, but not limited to, the definition of "harm" and "customer proprietary information;" notification requirements pertaining to date breaches or changes to policy privacy; opt-in requirements for use of customer data; and whether the rules were adopted properly under Section 222. These are issues upon which NTCA commented throughout the course of the proceeding. These instant comments are intended to highlight but two fundamental matters that underpin the Commission action in this proceeding.

BIAS Provider Access to Customer Information

In the first instance, the rules are premised in large measure upon the incorrect assumption that ISP's have uniquely broad and pervasive insight into and knowledge of user information that exceeds that of app or edge providers. Public Interest Commenters[3] argue, "ISPs can develop highly detailed and comprehensive profiles of their customers without those customers knowing about the practice."[4] Indeed, the FTC recognized that ISPs are "in a position

[3] "Public Interest Commenters" is the self-designated title of a group of 26 parties that joined in an Opposition to the Petitions for Reconsideration. The pleading may also be identified by the first party listed on the pleading, Access Humboldt (filed Mar. 6, 2017).

[4] Public Interest Commenters at 2 (internal citation omitted).

to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible."[5] And, the Center for Democracy & Technology avers that "customers have no choice but to disclose large amounts of personal information, including browsing history and location, to their ISPs."[6] Those observations, however, must be weighed against others actors in the broadband marketplace. And, once measured, it is clear that the disparate treatment of BIAS providers must be rejected.

By way of example, unless disabled, mobile Google maps can track a user's physical location and store that information over a period of years.[7] Google, Amazon, Facebook, WhatsApp and Apple can tap artificial intelligence (AI) software to analyze the content of text messages and photos in order to recommend responses and to "learn" user preferences in order to provide tailored responses to inquiries.[8] Even the Washington Post uses cookies, web beacons and "other technologies" for online tracking and advertising.[9] App and edge providers have the

[5] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Notice of Proposed Rulemaking*, Docket No. 16-106, FCC 16-39, at para. 4 (2016) (NPRM).

[6] Center for Democracy & Technology at 10 (filed Mar. 6, 2017).

[7] "Where to Find the Map that Shows Google is Tracking Your Location," Matt Elliott, c|net (Nov. 5, 2015) (http://www.cnet.com/how-to/how-to-delete-and-disable-your-google-location-history) (last viewed May 19, 2016, 17:49).

[8] "Google's New Products Reflect Push Into Machine Learning," Jack Nicas, Wall Street Journal (May 18, 2016) (https://www.wsj.com/articles/googles-new-products-reflect-push-into-machine-learning-1463598395) (last viewed Mar. 14, 2017) 17:13)).

[9] Privacy Policy, Washington Post (https://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html) (last viewed May 25, 2016, 10:50). The Post explains further that in addition to itself, "third-parties may collect or receive certain information about your use of Services, including through the use of cookies, beacons, and similar technologies, and this information may be combined in information collected across different websites and online services."

ability to develop more detailed and more comprehensive profiles of their users.[10] And, the ability of ISPs to develop similar data is becoming increasingly constricted as encryption increases.[11]

There is, therefore, no justification to subject BIAS providers to more onerous standards. While Public Knowledge, *et al.* aver that the Commission "has already deliberated and spoken,"[12] this aspect itself is a critical element that justifies reconsideration of the rules, as it speaks to an incorrect assessment of the factual circumstances that would tend to support the final rules. Public Knowledge, *et al.* imply that the adoption of the rules was "reasonable and supported by the record" and that "there is no material error."[13] And, yet, independent sources underscore the vast access to user data that edge and app providers enjoy and can utilize lawfully within the boundaries of the FTC posts.[14] The disparate treatment of actors with access to the same information cannot be supported.

The Commission Should Reconsider the Regulatory Disparity that Results from the New Rules

To be sure, the FTC lacks authority to regulate common carriers, [15] which BIAS providers are following reclassification of BIAS as a Title II service. Public Interest Commenters

---

[10] *See, e.g.*, Petition for Reconsideration of Oracle (filed Dec. 21, 2016).

[11] *See*, Reply Comments of NTCA, at 8, 9 (filed Jul. 6, 2016).

[12] Public Knowledge, Center for Digital Democracy, and Benton Foundation at 2 (filed Mar. 6, 2017) (internal citation omitted) (Public Knowledge, et al.)

[13] Public Knowledge, et al., at 3.

[14] *See, e.g.*, "The Price of Free: How Apple, Facebook, Microsoft and Google Sell You to Advertisers," Mark Hachman, PCWorld (Oct. 1, 2015) (http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html) (last viewed Mar. 16, 2107, 13:51).

[15] *See*, 15 U.S.C. § 45(a)(2).

propose that the Commission's Order ensures that "there will not be a gap left by the common carrier exemption" of the FTC rules. However, the Commission could have more effectively mirrored the FTC approach and fostered a seamless and level user experience across BIAS and other broadband market services, and no such gap would have formed. The Center for Democracy & Technology illuminates that the Commission could have relied upon Section 201(b), which confers upon the Commission the authority to act against "unjust and unreasonable practices."[16] Instead, the Commission created an expansive, overarching regulatory regime that affects more subjects, more data, and more costs.

The Commission now includes applicants for service within the definition of customer;[17] broadened the categories of information that is to be protected by creating a new category of "personal information;"[18] and imposed breach reporting requirements whose composition will likely compel carriers to issue unnecessary and confusing notifications.[19] As the Internet Commerce Coalition observes, the new rules veer from a rational FTC approach that "limits sensitive information to defined categories, such as financial information, health information, Social Security numbers" and other data.[20] The resulting set of bifurcated Federal policies will cause customer confusion. NTCA cautioned in initial comments in this proceeding that "[m]ost

[16] Center for Democracy and Technology at 9 (filed Mar. 6, 2017).

[17] *See*, 47 C.F.R. § 64.2002(e).

[18] *See*, 47 C.F.R. § 64.2002(f); *see, also, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Order,* Docket No. 16-106, FCC 16-148, at para. 46, *et seq.*

[19] *See*, 47 C.F.R. § 64.2006. For further discussion of this issue, *see, Protecting the Privacy of Customers of Broadband and Other Telecommunications Services: Comments of NTCA-The Rural Broadband Association,* OMB 3060-XXXX, Docket No. 16-106 (filed Mar. 13, 2017).

[20] Internet Commerce Coalition at 2 (filed Mar. 6, 2017).

users will be unaware that regulatory oversight could depend less upon the *nature* of the data and more upon the *holder* of the data," and urged the Commission that standards derived from FTC principles that apply to all players would be a sounder approach.[21]

The Center for Democracy & Technology notes correctly that Section 222 "does not provide specific guidance on the steps BIAS providers must take to comply with the law,"[22] and thereby justifies the Commission's unprecedented expansions. But, neither does Section 5 of the FTC Act provide a regulatory playbook of granularity. Rather, Section 5 prohibits "unfair or deceptive or practices in or affecting commerce." To be sure, the FTC Act defines its terms: "unfair or deceptive" is a material representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. "Practice" is an action that (a) causes or is likely to cause substantial injury to the consumer which is not (b) reasonably avoided by the consumer or (c) outweighed by countervailing benefits to the consumer or competition.[23] And, yet, the statute does not round of these definitions. Rather, these guideposts are informed by industry practice and, where necessary, direction from the courts.[24] They may contemplate retroactive policy changes, deceitful data collection, improper use of data, or unfair design. The FTC umbrella can cover obligations of providers to maintain

---

[21] Comments on NTCA at 11 (filed May 27, 2016) (emphasis in original).

[22] Center for Democracy & Technology at 8 (filed Mar. 8, 2017).

[23] *See*, 15 U.S.C. § 45(n). This standard is also incorporated in the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, *codified at* 12 U.S.C. § 5511 (2011). This three-prong approach was first articulated in the FTC's "Policy Statement on Unfairness," and later incorporated into the FTC Act. *See*, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last viewed May 26, 2016, 12:27).

[24] *See, generally*, Solove, Daniel J., and Hartzog, Woodrow, "The FTC and the New Common Law of Privacy," 114 Columbia Law Review 583 (2014).

confidentiality; to collect data only in a manner consistent with stated policies; and, to protect that data.[25] These standards provide sufficient guidance to edge and app providers, and would be fully sufficient to protect the BIAS sector of the broadband market sector.

There is no justification to enact a wholly different set of standards for ISPs. Public Interest Commenters propose that "privacy is contextual, and consumers know that different websites and services provide different levels of privacy."[26] NTCA submits, however, that a consistent standard of privacy practices and expectations across the spectrum of a user's broadband experience would reduce opportunities for misplaced reliance upon non-existent or inapplicable protections. BIAS subscribers would be protected fully and sufficiently under FTC-type standards that would provide those users with a level field of expectations and practices when "going on-line."

The disparity is even more evident when certain of the Commission rules are compared to state regulation. State Privacy and Security Coalition observe that new rules "adopt an asymmetrical definition of sensitive data . . . [that] differs not only from the FTC privacy framework, but also from all the state privacy and security statutes."[27] NTCA submits that this outcome will create customer confusion. NTCA does not propose Federal preemption of state regulations to create a single, universally-applicable standard. Rather, NTCA submits that user ease and understanding will be facilitated by a uniform Federal standard that in many instances

---

[25] *See, FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015) (failure to use readily available technology such as firewalls; storage of information in plain text; failure to implement adequate policies; failure to remedy known vulnerabilities; failure to use adequate protocols and passwords; failure to restrict access to network; and failure to follow incident response procedures, taken together, constitute unreasonable behavior).

[26] Public Interest Commenters at 3 (internal citation omitted).

[27] State Privacy and Security Coalition at 3 (filed Mar. 6, 2017).

will complement the respective state standards to which users and operators are subject. As stated succinctly by the Internet Commerce Coalition, the new rules "invent a very different regulatory paradigm for ISPs than the regime that applies to the rest of the Internet ecosystem."[28]

To the extent the Commission endeavors to identify BIAS data that is analogous to CPNI, it should be guided by the discrete limitations of those rules arising out of Section 222 to address those aspects of BIAS that arise specifically out BIAS. Other data sets that are common to both BIAS and other firms, include edge and app providers, should be governed by a uniform standard articulated in the FTC Act, and which can be rooted in Section 201. This will ensure that consumers enjoy a uniform expectation of privacy, and that regulatory parity among market players will enable a level field of competition.

Respectfully submitted,

By:
/s/ Joshua Seidemann
Joshua Seidemann
Vice President of Policy
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
jseidemann@ntca@ntca.org
703-351-2000 (Tel)

March 16, 2017

[28] Internet Commerce Coalition at 3.