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	**)**	

Reply Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

Joshua Seidemann
Vice President of Policy
NTCA-The Rural Broadband Association
4121 Wilson Boulevard, Suite 1000
Arlington, VA 22203
703/351-2000

July 6, 2016

TABLE OF CONTENTS

SUMMARY

In initial comments, NTCA–The Rural Broadband Association (NTCA) examined the Commission's proposals in the above-captioned docket and urged the Commission to avoid implementing a regulatory regime that would have the effect of imposing intentional marketplace disparities and distortions. In these reply comments, NTCA offers a composite image of others parties' statements and responds in order to demonstrate that many of the Commission's proposals regarding the creation of Section 222-sourced requirements for providers of broadband Internet access service are not consistent with marketplace expectations, technological conditions, or legal authority.

NTCA also explains herein the need for a suitable review in accordance with the Regulatory Flexibility Act. NTCA describes the impact of the various proposals on small ISPs, and explains how unnecessary costs will limit small ISP abilities to deploy and maintain networks.

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	**)**	

Reply Comments of

NTCA–THE RURAL BROADBAND ASSOCIATION

To the Commission:

I. INTRODUCTION

NTCA–The Rural Broadband Association (NTCA) hereby submits these reply comments in the above-captioned proceeding. The record reflects that numerous parties representing a spectrum of providers, academic experts, and equipment providers who agree that the Commission's proposals to rewrite existing, time-tested CPNI processes and implement new far-reaching detailed and prescriptive requirements for ISPs will visit adverse impacts on the industry and its customers. The Commission's proposals, if adopted, would foist costly and unnecessary obligations upon providers that would be especially challenging for small firms, and would inject a chilling measure of regulatory disparity into the marketplace. Moreover, the Commission's proposals are hard-pressed for justification on the basis of marketplace realities, technical standards, and legal authority. Small providers would bear disproportionate impacts that would inure to the disfavor of their customers. These adverse outcomes would have the effect of increasing provider costs that would necessarily be passed along to customers,

creating disincentives to adoption even as the Commission continues to champion the need to extend broadband further throughout the Nation. For these reasons, NTCA reiterates the positions it established in initial comments, and elucidates aspects of them here in response to other filed comments.

II. DISCUSSION

A. THE COMMISSION'S PRIVACY PROPOSALS ARE INCONSISTENT WITH MARKETPLACE, TECHNOLOGICAL, AND LEGAL CONDITIONS.

1. The Commission's Proposals are Neither Consistent with Marketplace Realities nor the Commission's Prior Pronouncements.

The breadth of interests represented in filed comments evidences the expanse of the so-called "broadband ecosphere." It is notable that among those industry participants, ranging from large and small providers providing service by varied technologies, there is virtually no support for the Commission's recommendations. One could suppose that "the devil can cite Scripture for his purpose,"[1] and that industry's descriptions of marketplace, technological, and legal conditions have been presented in a manner solely to support their positions. And, yet, academic experts (both before the Commission and Congress) also roundly criticized the Commission's proposals, citing substantial difficulties reconciling the Commission's intent with the realities of the marketplace or statutory authority.[2] Toward those ends, a cynic might conjecture that even an

[1] William Shakespeare, "The Merchant of Venice," Scene III.

[2] *See, e.g.*, Letter to Thomas Wheeler, Chairman, FCC, from J. Howard Beales III, Professor, Strategic Management and Business Policy, George Washington School of Business (May 27, 2016) (" . . . "the FCC should forbear from creating a new regulatory framework for privacy practices, and defer to the successful FTC regime. . . . The Commission should not risk undermining . . . .numerous benefits without clear evidence of a problem that needs to be solved) (Letter at 3); Testimony of Jon Leibowitz, Co-Chairman, 21st Century Coalition before the

objective academic's opinion may be swayed by industrial preference. But, added upon industry expertise and professorial product are the comments of the Federal Trade Commission (FTC), which leave no doubt as to the robust usefulness of existing safeguards. Even non-providers characterized the proposals as "out of step with any current federal or state regulations for privacy and data security," threatening to "stifle innovative business models and deprive consumers of choice."[3] The Commission's proposals are inconsistent with the realities of the marketplace, technology, and the law. The adverse impacts of these inconsistencies will be especially burdensome for small ISPs and their customers.

In initial comments, NTCA explained that general principles consistent with Section 5 of the FTC Act have provided an expanding body of guidance to the market. "Unfair and deceptive" practices are to be avoided by service, applications, and edge providers. American consumers have learned to navigate a consistent field of privacy expectations in the broadband space. This consistency also benefits consumers by creating a level field across which many firms can compete. No sector of the industry is hampered unduly by costly, burdensome and unnecessary regulations. Consumers and providers enjoy a three-way confluence of the industry's keen interest in protecting its customers; the competitive nature of the industry that leads to best practices; and the technological conditions that require a flexible, evolving

---

House Energy and Commerce Subcommittee on Communications and Technology (June 14, 2016) (". . . the FCC proposal amounts to a *de facto* rejection of the FTC's determination that ISPs should not and need not be governed by a different set of standards with regard to how they handle broadband consumer data. . . . .The breadth of data covered by the proposal, and the highly restrictive nature of the permissions regime employed by the FCC, creates a serious risk of unforeseen consequences that could adversely affect Internet capabilities and operations and disrupt consumer expectations." (Testimony at 5); Comments of International Center for Law and Economics at 2 ("The proposed rules instead dig in the heels of the Commission against the irresistible tide of progress, attempting to maintain arbitrary industry firewalls between firms.").

[3] Computing Technology Industry Association at 1.

discipline within which privacy and security can be addressed. Chairman Wheeler has recognized a similar construct, explaining, "[T]here is a new regulatory paradigm where the Commission relies on industry and market first while preserving other options if that approach is unsuccessful."[4] And, yet, there is no evidence that the FTC has been "unsuccessful" or that the industry has failed to create a comprehensive menu of best practices (in fact, proposals to promulgate rules based on various voluntary industry standards evidences their strength and suitability). As noted by American Cable Association, "A 20-year run free of major incidents simply does not support the argument that prescriptive privacy and data security regulations are needed to promote broadband usage and deployment."[5]

The success of the current regulatory environment, in which consumers and providers enjoy consistent expectations that are based upon the *substance* of the data rather than on the *holder* of the data support recommendations that the Commission stand down from implementing a system that enforces a disparate set of standards and expectations. Marketplace realities also argue against the proposed rules.

As noted by the United States Chamber of Commerce, the Commission's "decision to regulate broadband providers under two different regulatory regimes is entirely arbitrary."[6] The Commission's claim that ISPs enjoy unique incentives and opportunities is not borne out by actual practices. As noted by CenturyLink, a BIAS provider obtains information about the

[4] Chairman Wheeler, June 12, 2014, speech to the American Enterprise Institute, https://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc (last viewed July 6, 2016, 9:45).

[5] Comments of American Cable Association at 21 (ACA).

[6] U.S. Chamber of Commerce at 5.

customer only when the customer is using the service. By contrast, firms that are capable of "cross network" and "cross device" monitoring can paint a more comprehensive image of the user that is fed by more data. And, of the firms that extract the largest values from consumer information, none are ISPs.[7] Accordingly, the proposition that ISPs enjoy special incentives is incorrect.

It is not only providers who aver these absences of motive and opportunities. Academics, as well, agree that there is insufficient basis to differentiate among ISPs and application or edge providers. A working paper from Georgia Tech explains, "First, ISP access to user data is not comprehensive – technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs."[8]

Even public interest organizations, often at odds with private industry, offer supportive conclusions. The Electronic Privacy Information Center states,

> The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the on-line communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services.[9]

[7] CenturyLink at 9.

[8] Peter Swire, Justin Hemmings and Alana Kirkland, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others, Working Paper of the Institute for Information Security and Privacy at Georgia Tech, Feb 29 2016. *See, also,* International Center for Law and Economics at 9 (" . . . non-ISP information practices are frequently far more robust than those of ISPs.").

[9] Electronic Privacy Information Center at 16 (EPIC).

EPIC explains that when the limited potential activities of ISPs are compared to edge and application providers, "it is obvious that the more substantial privacy threats for consumers are not the ISPs."[10] Accordingly, the Commission's attempts to weave a complicated web of regulation for ISPs, while others in the market take guidance from clear and straight-forth FTC principles, cannot be justified.

As USTelecom notes, the FTC has "knowledge gained through robust enforcement."[11] A growing body of case law has emerged that provides guidance to all participants in the on-line market.[12] The Commission's proposals to single-out ISPs for regulations that in the first instance are not contemplated by the governing statute are unnecessary, and should be rejected. As noted by the U.S. Chamber of Commerce, the Commission's proposals threaten to expand "a regulatory divide between edge and telecommunications providers, and . . . stifl[e] the already thriving Internet ecosystem."[13] This result would be not only contrary to the calls of industry and market experience, but would conflict as well with the Chairman's views on these matters: "The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking . . . We cannot hope to keep up if we adopt a prescriptive regulatory approach. We must harness the dynamism and innovation of competitive markets to fulfil our policy and

[10] EPIC at 16. To the extent EPIC calls for rules that extend beyond either FTC requirements or narrowly tailored obligations arising out of Section 222, NTCA disagrees with EPIC's conclusion that "privacy rules for ISPs are important and necessary."

[11] USTelecom at 2.

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

[13] U.S. Chamber of Commerce at 1.

develop solutions."[14] Disparate regulations applied to participants who hold the same information, however, will undermine the "dynamism and innovation of competitive markets"[15] by littering the playing field with regulatory hurdles and obstacles. Or, as American Cable Association expresses, "[T]he proposed rules are more likely to shove a stick in the spokes of the virtuous circle than to perpetuate it."[16]

By way of example, the Commission proposes that MAC addresses be considered protected information. In initial comments, NTCA explained why MAC addresses do not disclose the sort of information that consumers would consider private.[17] And, as noted by other commenters, MAC addresses are available to operating system providers, device manufacturers, app providers, and others.[18] Accordingly, regulating some who hold that information, but not others, would tilt the playing field and insert disadvantages into the market.

The imposition of burdensome, disparate regulations is not supported by marketplace conditions. The approach of the Commission in this proceeding conflicts with the sensible principles articulated by the Chairman previously. The Commission should accordingly reject the proposals and enable a level playing field in the market.

---

[14] Chairman Wheeler, June 12, 2014, speech to the American Enterprise Institute, https://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc (last viewed July 6, 2016, 9:45).

[15] *Id.*

[16] ACA at 21.

[17] NTCA at 21.

[18] CenturyLink at 15.

2. The Privacy Proposals are Not Supported by the Actual Technological Abilities of ISPs.

The Commission's proposals are premised on the misplaced assumptions that ISPs can monitor their customers' traffic and obtain unique access to valuable information. CenturyLink observes, "This view is incorrect, and has resulted in a deeply flawed proposal."[19] The universe of information to which ISPs have access is decreasing.[20]

In the first instance, encryption is employed at increasing rates. ISPs are shifting from basis HTTP to HTTPS protocol, which "prevents BIAS providers from being able to see customer content and detailed URLs."[21] Encryption ameliorates against many Commission concerns, and it is predicted that by the end of this year, more than 70 percent of global Internet traffic will be encrypted, with some networks approaching an 80 percent encryption threshold.[22] Moreover, as noted by USTelecom "consumers are increasingly accessing the Internet through virtual private networks (VPNs), which encrypt a user's connection to the Internet, and therefore block an ISPs ability to know what the customer is viewing."[23] The Commission should enable the industry to continue to develop solutions to market needs, and to pivot when new developments are necessary. EPIC's recommendation that "service providers offer robust, end-

[19] CenturyLink at 5.

[20] CenturyLink at 6.

[21] CenturyLink at 7.

[22] Sandvine at 9.

[23] USTelecom at 5.

to-end encryption for all consumers free of charge"[24] should be rejected. The focus should remain fastened on the FTC principles of "unfair and deceptive" practices.

Sandvine elucidates this principle as it addresses the Commission proposal to ban DPI. Sandvine compares this to a single lens reflex camera, which can be used for both legal and unlawful purposes. Rather than ban the technology, the use should be the actionable offense.[25] Above all, the notion that "perfect security" can be obtained must be relinquished: as Consumer Technology Association states, "'[p]erfect' security simply does not exist."[26]

Toward these ends, the Commission's proposals to implement prescriptive solutions should be rejected. The industry-driven practice formulated by industry should remain voluntary, with adherence to them encouraged by the watchful eye of the FTC. In light of the evolving nature of technology and markets, NTCA supports the USTelecom observation that security is best addressed through a "comprehensive and multi-stakeholder fashion" that fosters "collaboration across the ecosystem."[27] As CTA notes, "frozen prescriptive broadband privacy rules, as proposed by the Commission, will restrict ISPs' ability to innovate and adjust to consumer demands of both today and tomorrow."[28]

[24] EPIC at 23.

[25] Sandvine at 3.

[26] CTA at 12.

[27] USTelecom at 21.

[28] CTA at 8.

3. The Commission's Proposals are Unsupported by the Law.

As noted in NTCA's initial comments, the Commission's proposals are not supported by the law. Section 222 offers a limited scope of authority. And, reliance on other provisions, including Section 706, evinces what seems a troublesome effort to shoehorn unnecessary regulation into place, regardless of whether either technological or market conditions warrant such action.

If the broadband market were an entirely unregulated environment, then the need for expansive Commission involvement might warrant some justification (notwithstanding the fact that the particular *strain* of involvement as proposed would as yet remain inappropriate). But, as Consumer Technology Association characterizes correctly "the FTC's time-tested and principles-based privacy and data security framework" has supported the market and its users.[29] The Commission's proposals to expand the scope of regulatory activity beyond a narrow data set that is analogous to CPNI in the telephone environment (and that would be consistent with the statute) should be rejected.

As CTA notes, Section 222 provides specific reference only to "proprietary information," and does not reference the quite more expansive field of "personal information" as the Commission proposes to capture.[30] The Commission's proposals are a "radical departure"[31] from both the statute and prior policy.

[29] Consumer Technology Association f/k/a Consumer Electronics Association (CTA) at 4.

[30] CTA at 6.

[31] USTelecom at 2.

Numerous comments deconstruct the Commission's legal authority. As the U.S. Chamber of Commerce notes, other sections of the Act refer to the Internet, but Section 222 does not; this indicates the Congress had no intention of capturing Internet access within the narrow and discrete protections accorded by Section 222.[32] The U.S. Chamber of Commerce warns against invoking Section 706 to support widespread regulation of BIAS activities, observing a chilling proposition that "the Commission is essentially claiming that it has the authority, *independent of Title II*, to regulate entities so long as it is doing so in the name of the timely deployment of broadband."[33] Indeed, the potential impact of a 706-based regime can be discerned from the extent to which some commenters desire the Commission to exert authority. EPIC, for example, "urges the Commission to investigate and regulate the practices of companies other than ISPs that collect and use consumer data generated by communications services."[34] The Commission's approach to privacy is inconsistent with assurances offered at the time of the *Open Internet Order* that regulation would be imposed thoughtfully and in a limited fashion. The instant rulemaking threatens to break open the gates of regulatory overreach, and such proposals therein that suggest gratuitous expansion into areas already covered by the FTC should be rejected. Section 222 is clear, and is limited by Congress to address only certain discrete data that arise out of the service itself. The Commission's efforts in these instant regards are best reserved to limited sets of information that are directly analogous to CPNI. Other data, such as so-called

[32] *See,* U.S. Chamber of Commerce at 4.

[33] U.S. Chamber of Commerce at 7.

[34] EPIC at 1, 2.

"PII" or information that is gathered by and accessible to app and edge providers, should remain within the purview of the able FTC.

B. SMALL PROVIDERS MUST BE EXEMPTED FROM BURDENSOME RULES.

1. The Costs of Implementation will Affect Small Providers Disproportionately.

In a related proceeding, NTCA noted that small ISPs do not serve markets or customer bases that are large enough to trigger concerns implicated by third-party interest in certain data.[35] Other representatives of small ISPs agree that there is "virtually no demand for most RLECs and their ISP affiliates to monitor the Internet browsing histories or online contacts of their customers to create detailed profiles for individually targeted or customized advertising purposes."[36] And, yet, the Commission could impose "tremendous burdens" on small providers if it were to adopt sweeping requirements that would govern activities in which small ISPs do not engage.

Of particular concern is the potential impact to operations and expenses for small providers. American Cable Association identifies nearly a score of costly impacts that would accrue to small providers, including, but not limited to: attorney and consultant costs associated with regulatory analysis, contract negotiation, risk management analysis, and preparing required policies, forms, training and audits; personnel costs associated with dedicated privacy and data security staff; third-party costs associated with modifying contracts and ensuring compliance for call centers, billing software, and others that interface with customer proprietary information.

---

[35] *See, i.e., Protecting and Promoting the Open Internet: Comments of NTCA–The Rural Broadband Association, Docket No. 14-28,* at 9 (Aug. 5, 2015).

[36] WTA at 2.

Most critically, however, these expenditures would sap resources otherwise directed toward network deployment and development.[37] Others from across the industry agree.

CTA warns that data security obligations as proposed by the Commission could "be a death knell for smaller ISPs."[38] Small providers have more limited customer bases and smaller staff. WISPA notes that "[f]or small providers, the costs of compliance are no lower, and, in fact, probably higher, than they are for large companies."[39] On average, NTCA provider member companies have a staff of 33 people. These include office staff responsible for customer account management; network operations personnel; sales and billing personnel; linemen and other construction personnel; regulatory managers responsible for local, state and Federal obligations; and bookkeepers/accountants. USTelecom observes, "small providers would have unique challenges and an even greater burden attempting to implement the FCC's proposed rules."[40] By way of example, in initial comments, NTCA opposed Commission recommendations that dedicated personnel with defined credentials be retained to serve as certifying compliance officers. This, plus additional data security requirements as proposed by the Commission, would "supersize the responsibility of the designated point of contact . . . [and] effectively require a full-time staff member to manage privacy and data security compliance, which is well beyond the means of small providers."[41] NTCA members already devote resources to network security,

[37] ACA at iii.

[38] CTA at 10.

[39] WISPA at 26.

[40] USTelecom at 19.

[41] ACA at 25.

but the proposed rules would supplant voluntary industry-designed practices with mandates to protect an unnecessarily expansive range of data. These would necessitate either the addition of new personnel, the costs of which would either be borne by customers or result in less resources for infrastructure deployment and maintenance, or the diversion of existing personnel from tasks that are critical to operations of the normal and ordinary course of business. Attempts to mitigate costs by hiring part-time network security personnel would not be feasible in rural areas served by NTCA members, as those skill sets on that basis do not generally exist in rural employment markets.[42] CTA characterizes the Commission approach as "an unforgiving and unrefined standard" that could "force an ISP to spend scare resources on efforts to encrypt large swathes of non-sensitive data . . . ." The allocation of additional costs on a per-customer basis would be higher for small ISPs than for large ISPs. The Internet Commerce Coalition, which includes both ISPs and edge providers, warns that the proposed "onerous audit trail, access control, and breach notification requirements for non-sensitive customer information . . . would divert ISP security resources from protecting their networks (which are critical infrastructure) and truly sensitive information."[43]

NTCA proposes that to the extent *any* new and burdensome regulations are adopted, the Commission exempt small providers. In the alternative, if no exemption is provided, NTCA urges the Commission to provide a delayed implementation schedule that will accommodate a sufficient period of at least 12-to-18 months to gather information about the impact of the rules

[42] In preparing these comments, NTCA polled a portion of its membership. One response noted that average staff size of operating companies in its state is ten. Another noted that rate increases to cover additional security costs, as opposed to those implemented for network improvement, would not engender favorable reactions among rate payers. The consensus supported the proposition that proposals would visit disproportionate costs among small providers.

[43] Internet Commerce Coalition at 8 (internal citation omitted).

on the operations of larger providers. After such a data gathering is completed, if the Commission concludes tentatively that the requirements should be imposed on small providers, then the Commission should issue a Further Notice of Proposed to explore the meaning of the data and how it may justify continuing the exemption or modifying requirements for small providers. Other commenters echo this proposition: ACA submits that compliance deadlines for small providers, if adopted at all, should be extended for at least one year to study impact and then implement notice-and-comment.[44] WISPA similarly calls upon the Commission to allow additional time for small provider compliance, noting that this has been done many times. [45]

2. The Commission Must Execute a Suitable Expression of the Regulatory Flexibility Act.

Section 603 of the RFA requires the Commission to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect impact on small entities was rejected."[46] The "factual" reasons include a quantification of the potential impacts.[47] Where quantification is not possible or practicable, the agency may present a qualitative assessment of the projected impacts.[48] In the instant matter, neither task has been completed. This requirement

[44] *See,* ACA at 46-49.

[45] WISPA at 27-29.

[46] 5 U.S.C. § 604(a)(6).

[47] 5 U.S.C. § 607.

[48] *Id.*

cannot be satisfied by simply seeking comment on the impact of proposed regulations on small businesses. Moreover, the RFA requires the agency to consider reasonable alternatives. To be sure, the Commission sought comment on the specific impact on small providers more than a half-dozen times in the NPRM. And, comments filed by many parties, including, but not limited to, ACA, NTCA, USTelecom and WISPA indeed identified significant potential impacts that attend the imposition of the proposed regulations on small providers, as described in Section B.1 of these Reply Comments, above. Even if the threshold questions regarding the legal sustainability of the Section 222 proposals are addressed, RFA obligations to provide a meaningful analysis of less-burdensome alternatives for small providers must be completed.[49]

III. CONCULSION

NTCA reiterates its commitment to protecting sensitive customer data and providing network security. As NTCA noted at the Commission's April 2015 Privacy Workshop and expressed in its initial comments in this docket, it looks toward the principles of notice, choice and transparency. Moreover, NTCA has been an active participant in numerous industry working groups that are formulating voluntary standards aimed at implementing network security measures in ways that are both strong and evolutionary to meet developing demands. NTCA, however, opposes measures that would inject a formidable dose of regulatory disparity into the marketplace. This would not only effect a steeply tilted imbalance among ISPs and edge and application providers, but also set the stage for damaging customer confusion.[50] Moreover, these

[49] 5 U.S.C. § 604.

[50] These concerns are noted by academic from Massachusetts Institute of Technology (MIT) and University of California, San Diego (USC-SD). *See*, Comments of William Lehr (MIT), Steve Bauer (MIT), and Erin Kenneally (USC SD) at 7 ("In summary, we are cautiously supportive of the FCC's efforts to redefine Section 222 in order to address BIAS, but are concerned about ways in which this asymmetric regulation may inappropriately distort market protection and add

measures would implicate costly and burdensome requirements for carriers, especially small providers.

Accordingly, NTCA recommends the Commission to limit the application of Section 222 to data that arises uniquely from the provision of BIAS, and to enable continued FTC oversight of all other data. NTCA further recommends the Commission to promote the implementation of voluntary, industry-designed security practices that balance strength and the ability to react quickly to evolving technology and potential threats.

Respectfully submitted,

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

July 6, 2016

costs, without significantly enhancing the federal framework for protecting consumer PI."). *See, also,* ADTRAN at 7 (". . . customers are likely to be confused by the different treatment of their confidential information, depending on the classification of a service provider as a telecommunications carrier or not.").