

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554**

In the Matter of)
)
Protecting The Privacy of Customers of Broadband) **WC Docket No. 16-106**
And Other Communications Services)

Comments of the Electronic Transactions Association

The Electronic Transactions Association (“ETA”) hereby submits its comments in response to the Commission’s above-captioned Notice of Proposed Rulemaking (“NPRM”).¹ ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services. ETA’s members include mobile broadband service providers that may be affected by the Commission’s proposed privacy and data security rules. In formulating rules to govern privacy and data security obligations of broadband Internet access service (“BIAS”) providers, the Commission must take care to ensure that such providers are not put at a competitive disadvantage by being subject to stricter or different regulation than other operators in the Internet ecosystem. Rather than reinvent the wheel for BIAS providers, ETA urges the Commission to follow the lead taken by the Federal Trade Commission (“FTC”) in protecting consumer privacy and data security and not to duplicate privacy obligations already imposed by other provisions of federal law, including the Electronic Communications Privacy Act (“ECPA”).²

¹ *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, FCC 16-39 (rel. Apr. 1, 2016).

² 18 U.S.C. §§ 2510-2522, 2701-2712.

Protecting customer privacy and security is an obligation that broadband providers take very seriously.³ Broadband providers have links to their privacy policies on their websites that allow visitors to review what information they collect, how they use it, with whom they share it, instructions for giving opt-in and/or opt-out approval for the use of certain information, the processes they have in place to protect the information from unauthorized access, and the manner in which customers are informed when changes to the policies are made. These privacy principles reflect industry best practices and are consistent with the FTC’s Privacy Framework and the Administration’s Consumer Privacy Bill of Rights,⁴ which apply to the collection and commercial use of consumer data that can be reasonably linked to a specific individual by *all* entities operating in the Internet economy.⁵ Contrary to the Commission’s assumption that “absent legally-binding principles,” broadband networks have the “commercial motivation to use and share extensive and personal information about their customers,”⁶ broadband providers have adopted and adhered to these policies of transparency, choice and security in the absence of any Commission requirements or “legally-binding principles,” demonstrating the efficacy of voluntary self-regulation in the data privacy and security context.

³ NPRM at ¶10 (all of the nation’s largest broadband providers have publicly available privacy policies describing their use and sharing of confidential customer information); *see also*, e.g., Verizon Privacy Policy, available at <http://www.verizon.com/about/privacy/privacy-policy-summary>; T-Mobile Privacy Policy, available at <http://www.t-mobile.com/company/website/privacypolicy.aspx>

⁴ FTC Report, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (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> (“FTC Privacy Report”); The White House, Consumer Digital Privacy In A Networked World: A Framework For Protecting Privacy and Promoting Innovation In the Global Digital Economy at 1 (Feb. 2012), available at <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

⁵ FTC Report at vii; Consumer Digital Privacy at 10.

⁶ NPRM at ¶3.

As the FTC has found, businesses frequently acknowledge how important consumer trust is to the growth of digital commerce.⁷ For this reason, and others, broadband providers have strong economic incentives to zealously guard their customers' privacy and it appears they have been successful in engendering consumer trust. According to a study reported in the Harvard Business Review, 73 percent of consumers surveyed said that telecommunications carriers were "trustworthy" or "completely trustworthy" when it came to making sure that personal data was never misused."⁸ In contrast, only 66 percent of consumers felt the same way about the government.

I. Self-Regulation Is A Better Alternative Than Burdensome New Rules

Adherence to a common set of privacy principles ensures that all entities doing business in the Internet economy are operating on a level playing field and that consumers have a common understanding with respect to what they can expect from those who may obtain access to their personal information in a commercial context without regard to the type of entity that collects or maintains the information or the manner in which it was obtained. Because the Internet economy is intensely competitive, the Commission must carefully weigh the impact that subjecting broadband providers to stricter regulation than other entities operating in the Internet economy would have on competition and innovation.

The Administration has appropriately recognized that the "Internet's complexity, global reach, and constant evolution require timely, scalable, and innovation-enabling policies" and has called upon stakeholders to "develop voluntary, enforceable codes of conduct that specify how

⁷ FTC Report at 8-9.

⁸ Timothy Morey, Theodore "Theo" Forbath, Allison Schoop, "Customer Data: Designing for Transparency and Trust," Harvard Business Review (May 2015), available at <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>

the Consumer Privacy Bill of Rights applies in specific business contexts.”⁹ The existing privacy policies of broadband providers are consistent with the self-regulatory regime the Administration envisioned and protect consumers while supporting innovation. Until the Commission’s reclassification of broadband service as a telecommunications service, the FTC had jurisdiction to enforce the privacy rights of broadband consumers pursuant to Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts and practices affecting commerce.¹⁰ This self-regulatory framework with the FTC as the chief privacy enforcer has proven effective in protecting consumers while at the same time allowing broadband providers the flexibility to craft their privacy policies based on the services they offer, the customer information they collect and the use they make of the information.

Consistent with the Administration’s preference for voluntary self-regulation, the Commission should follow the FTC’s approach rather than adopt prescriptive new rules that will put broadband providers at a competitive disadvantage relative to other operators in the Internet ecosystem. The Commission’s existing transparency rule, 47 C.F.R. § 8.3, already requires broadband providers to publicly disclose accurate information regarding the commercial terms of their broadband Internet access services, including their privacy policies, sufficient for consumers to make informed choices.¹¹ To the extent that the Commission believes that a

⁹ Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values at 20 (May 2014), available at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

¹⁰ 15 U.S.C. § 45.

¹¹ *In the Matter of Preserving The Open Internet*, GN Docket No. 09-191, Report and Order, 25 FCC Rcd 17905 at ¶ 56 (2010) (privacy policies are among the commercial terms of service that broadband providers must disclose pursuant to Section 8.3); *In the Matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling and Order, FCC 15-24, at ¶ 164 (rel. Mar. 12, 2015) (disclosure of commercial terms shall also include the provider’s privacy policies)

broadband provider collects, uses or discloses customer proprietary information in a manner contrary to its privacy policy, the Commission can bring an enforcement action for violation of the transparency rule.¹² In light of the safeguards that are already in place, the Commission does not need to adopt new rules to protect consumer privacy.

Asserting that “the current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration’s efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks,”¹³ the Commission asks whether consumers may be hesitant to apply for broadband service or apprehensive about changing service providers “without the privacy protections of Section 222.”¹⁴ The short answer is that there is no basis for such speculation because the very effective self-regulatory regime remains in place for broadband providers and there is no evidence that customers have been hesitant to apply for service or switch providers without regulations adopted pursuant to Section 222.

Although Section 222 itself has been applicable to broadband service since the reclassification went into effect on June 12, 2015,¹⁵ the Commission has forborne from applying

¹² See *In the Matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling and Order, FCC 15-24, at ¶¶182, 184 (broadband providers’ disclosures of commercial terms of service, including privacy policies, must be accurate and not misleading and if providers’ disclosures fail to meet the requirements of the transparency rule, they could be subject to investigation and forfeiture) (*Protecting and Promoting the Open Internet*); see also, *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, File No. EB-TCD-14-00017601, Order, DA 16-242 (Enforcement Bureau, rel. Mar. 7, 2016).

¹³ *Protecting and Promoting the Open Internet*, at ¶462; NPRM at ¶2.

¹⁴ NPRM at ¶¶ 32-33.

¹⁵ 80 Fed. Reg. 19737.

its implementing regulations pending the adoption of rules to govern broadband Internet access service in this rulemaking proceeding.¹⁶ As a result, to the extent that consumers are hesitant to apply for broadband service or to switch providers without the privacy protections of Section 222 regulations, one would have expected to see a decline in broadband Internet access service subscriptions after June 12, 2015. Instead, there was a net increase of 1.59 million wireline broadband subscribers in the third and fourth quarters of 2015.¹⁷ This is undoubtedly due, at least in part, to the fact that broadband providers' privacy policies have remained in place and the self-regulatory regime is effective in protecting consumers' privacy interests.¹⁸ Significantly, the Commission does not assert, nor could it, that broadband providers have failed to adequately safeguard their customers' privacy in the absence of Commission regulation.¹⁹

While the Commission seems to believe that broadband Internet access service providers are in a unique position to develop highly detailed and comprehensive profiles of their customers by following "the activities of every subscriber who surfs the web, sends an email or text, or even walks down the street carrying a mobile device,"²⁰ this is not necessarily the case and does not justify heightened regulation for this one industry segment. As discussed in a recent paper released by the Institute for Information Security & Privacy at Georgia Tech, there are

¹⁶ *Protecting and Promoting the Open Internet* at ¶¶ 463-467.

¹⁷ See <http://www.statista.com/statistics/217938/number-of-us-broadband-internet-subscribers/> and <http://www.statista.com/statistics/217941/number-of-us-broadband-net-adds/>

¹⁸ Moreover, as noted above, to the extent a broadband provider acts in a manner inconsistent with the commitments in its privacy policy, the Commission can bring an enforcement action for violation of Section 8.3 of the Commission's Rules.

¹⁹ It bears mentioning that the FTC did not find it necessary to bring an enforcement action against a broadband provider based on data privacy or security practices in the many years it had jurisdiction to do so.

²⁰ NPRM at ¶¶ 3-4.

significant technological limits on a broadband provider's visibility into its users' Internet activity.²¹ For example, it is estimated that 70 percent of Internet traffic will be encrypted by the end of this year. Encryption prevents a broadband provider from examining its users' content.²² The use of virtual private networks ("VPN") and third party proxy services further limit a broadband provider's visibility into its customers' Internet activity.²³ As for the user walking down the street carrying a mobile device, that user's Internet traffic is just as likely to be offloaded to a series of WiFi networks rather than carried on the user's broadband network.²⁴ This is not to downplay the access that Internet service providers have to their customers' online activity, but to challenge the characterization of that access as unique or comprehensive. Many other entities operating in the Internet economy have access to comparable online activity and personal data of their users, including search engines, operating systems, browsers, e-commerce sites and social networks such as Facebook, Twitter, and Pinterest.²⁵ Because the Commission's proposed privacy rules apply only to broadband Internet access providers, however, broadband providers alone will be held to different privacy standards than others operating in the Internet economy even though those others have access to the same, or similar, personally identifiable information about their users.

²¹ Peter Swire, *et al.*, Online Privacy and ISPs, a Working Paper of the Institute for Information Security & Privacy at Georgia Tech (Feb. 29, 2016), available at http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf

²² *Id.* at 3, 23.

²³ *Id.* at 25-35.

²⁴ *Id.* at 3, 10, 24-25.

²⁵ *Id.* at 43-48.

If the Commission is truly concerned about avoiding action that may inhibit competition and innovation in the Internet access space,²⁶ it should refrain from subjecting broadband providers to different or heightened privacy standards. So long as customers are advised about the collection and use of their information by their broadband providers and are able to exercise choice as they are today in the absence of Commission regulation, the Commission does not need to adopt prescriptive regulations to ensure consumer privacy continues to be properly protected.

II. The Commission Does Not Have Authority To Rewrite Section 222

If the Commission nonetheless deems it necessary to move forward with new rules, those rules should be based upon the Privacy Framework that the broadband industry has submitted for consideration.²⁷ The Privacy Framework is consistent with the approach the FTC successfully implemented before reclassification to ensure that the data privacy and security practices of broadband providers were transparent, fair and non-deceptive. That approach has proven successful in the past and should be the model for regulation in the future.

At the very least, the Commission must ensure that any rules it may adopt are consistent with Section 222 of the Communications Act. The Commission proposes to broadly define customer proprietary network information (“CPNI”) to include not only customer proprietary network information as defined by Section 222(h) of the Act but also a broad range of additional categories of information a broadband provider might acquire by virtue of providing service.²⁸

²⁶ See e.g., NPRM at ¶ 33.

²⁷ See March 1, 2016 letter to Chairman Tom Wheeler from the American Cable Association, the Competitive Carriers Association, CTIA, National Cable & Telecommunications Association and US Telecom, available at <http://sf8.colo.ctia.org/docs/default-source/fcc-filings/wheeler-letter-privacy-principles.pdf?sfvrsn=6>; NPRM at ¶¶ 280-282.

²⁸ Proposed Rule 64.7000(f), (g); NPRM at ¶¶ 38-55.

Section 222(h) defines CPNI as information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service to which a customer subscribes and that is made available to the carrier solely by virtue of the carrier-customer relationship and information contained in the bills pertaining to telephone exchange or toll service received by a customer. As the D.C. Circuit has made very clear, however, the Commission does not have the freedom to expand statutory definitions. *ACLU v. FCC*, 823 F.2d 1554, 1568-69 (D.C. Cir. 1987) (where Congress has not left gaps for the Commission to fill, the Commission’s redefinition of a statutory term is contrary to law); *Time Warner Entertainment Co., LLP v. FCC*, 56 F.3d 151, 189-90 (D.C. Cir. 1995) (the Commission does not have authority to rewrite a statutory definition enacted by Congress).

To the extent that the Commission believes that the definition of CPNI in Section 222(h) is too narrow and should be broadened to incorporate additional categories of information that broadband providers may collect, the solution is to seek a legislative change from Congress. In the meantime, the Commission cannot magnify the coverage of the existing statute by rewriting Congress’ definition of CPNI in Section 222(h).

The Commission also seeks to create a distinction between the “proprietary information” of customers referenced in Section 222(a) and the “customer proprietary network information” defined in Section 222(h). ETA submits that Section 222(a) merely articulates the duty all telecommunications carriers have to protect CPNI and the proprietary information of other carriers (and equipment manufacturers) as more fully detailed in Sections 222(b) and (c), and that it does not create a category of customer proprietary information separate and apart from CPNI. Section 222(a) provides that every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to (1) other telecommunications

carriers, (2) equipment manufacturers and (3) customers. The Commission asserts that “customer proprietary information,” although not separately defined in the statute, encompasses all information that can be linked to an individual and that CPNI is just a subset of the customer proprietary information that Section 222 protects.²⁹ It is hard to reconcile the Commission’s interpretation with the plain language of the statute, which does not distinguish between customer proprietary information and CPNI, and Congress’ failure to include a separate definition for customer proprietary information if in fact it is something different and much more encompassing than CPNI. The Commission’s interpretation also cannot be reconciled with its previous reading of Section 222 as not applying to information a carrier collects that does not meet the statutory definition of CPNI.³⁰

The Commission’s attempt to label all personally identifiable information that is linked or linkable to an individual as confidential and proprietary³¹ cannot withstand scrutiny. Among the personally identifiable information the Commission claims is confidential and proprietary are customer name and postal address and all information identifying personally owned property, including license plates.³² If the Commission’s assertion were correct, a broadband provider

²⁹ NPRM at ¶¶ 15, 59, 68.

³⁰ *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers; Use of Customer Proprietary Network Information and Other Customer Information*, 28 FCC Rcd 9609, Declaratory Ruling, at ¶ 24 (2013) (“[I]f the information a carrier collects in the future does not meet the statutory definition [of CPNI], then Section 222 will not apply. To reiterate, the Commission is clarifying only that information that meets the definition of CPNI is subject to Section 222. . .”).

³¹ NPRM at ¶¶ 60-61, 63 (a broadband customer’s name and postal address “are customer PI protected by Section 222(a)”).

³² NPRM at ¶¶ 61-64. It is difficult to understand how license plate information can be “confidential and proprietary” when license plates are publicly displayed on automobiles. It is also difficult to understand why a broadband provider would collect license plate information.

would violate Section 222(a) every time it sent a customer anything through the U.S. mail, including its privacy policy notices,³³ because the customer’s “confidential and proprietary” name and postal address would be publicly disclosed on the envelope. Although Section 222(d) provides that carriers are not prohibited from using or disclosing CPNI without customer notice or approval to bill and collect for telecommunications service, the statute contains no similar exemption for the customer proprietary information referenced in Section 222(a). The Commission proposes to fill the statutory gap by adopting a similar exemption for the use of customer proprietary information to bill and collect for broadband service,³⁴ but does not explain why Congress would have adopted the billing exemption for CPNI, but not for the Section 222(a) customer proprietary information. Again, the more reasonable reading of the statute is that Congress did not intend a distinction between the customer proprietary information referenced in Section 222(a) and the CPNI referenced throughout the rest of Section 222 so there was no need to create a separate exemption.

The Commission asks whether it should regulate access to the content of consumer communications carried over broadband networks pursuant to Section 222.³⁵ As the Commission acknowledges, ECPA³⁶ and Section 705 of the Communications Act³⁷ already provide strong protection for the content of communications carried over broadband networks.³⁸

³³ Proposed Rule 64.7001(c) would require broadband providers to disclose material changes to their privacy policies on customer bills for service; see also NPRM at ¶¶ 96, 99.

³⁴ NPRM at ¶ 115; Proposed Rule 64.7002(a)(2).

³⁵ NPRM at ¶¶ 20, 67.

³⁶ 18 U.S.C. §§ 2510, *et seq.*

³⁷ 47 U.S.C. §605.

³⁸ NPRM at ¶ 67.

There is no need for the Commission to adopt additional regulations pursuant to Section 222 of the Act or section 705 to cover the privacy of content. In fact, doing so would be contrary to the Administration's expressed preference to avoid duplicative and burdensome regulatory requirements on activities that are already subject to existing Federal data privacy laws.³⁹

ETA appreciates (and shares) the Commission's concern for protecting customer privacy. The Commission cannot, however, expand its jurisdiction to protect customer privacy beyond the specific obligations imposed on telecommunications carriers by Section 222. Unless and until the Commission is able to obtain a legislative fix, customer privacy would be far better protected by allowing broadband providers to maintain their existing self-regulatory privacy policies, which do cover personally identifiable information. As noted above, if the Commission were to suspect that a broadband provider was acting in a manner inconsistent with its privacy policy, it could investigate and, if necessary, sanction the provider for a violation of the transparency rule.

III. The Commission Should Not Hamstring Competition

The Commission's proposed rules would prohibit broadband providers from using, disclosing or accessing customer proprietary information without customer approval. Proposed rule 64.7002(a) and (b) would infer customer approval for broadband providers to use, disclose or grant access to customer proprietary information in order to provide and bill for service, market other broadband services to the customer, protect the rights and property of the provider and protect users and other broadband providers from fraudulent, abusive or unlawful use of the broadband service, to assist in the delivery of emergency services or as otherwise required by law. Proposed rule 64.7002(e) would require customer *opt-out approval* for broadband providers to use, or to disclose or permit access to customer proprietary information to their agents or affiliates, for the purpose of marketing communications-related services. Finally,

³⁹ Consumer Digital Privacy at 35, 38.

proposed rule 64.7002(f) would require broadband providers to obtain customer *opt-in approval* for any other use, disclosure or access to customer proprietary information.

ETA agrees with the Commission that informed choice is necessary to protect consumers' fundamental privacy interests.⁴⁰ Opt-in consent should definitely be required before a broadband provider uses or shares any very sensitive consumer personal information (*e.g.*, Social Security Number, financial information, credit card information, medical information, precise geo-location information or unique government identification numbers). However, it should be sufficient for broadband providers, like other companies operating in the Internet ecosystem, to obtain opt-out consent for the use of non-sensitive information. The Commission's proposed rules would put broadband providers at a competitive disadvantage and may deprive their customers of the opportunity to realize the potential upside of the beneficial use of customer data for targeted advertising or other purposes. So long as customers have notice and the ability to revoke their opt-out consent conveniently and at any time, there is no reason to subject broadband providers to disparate regulation.

⁴⁰ NPRM at ¶ 12.

Conclusion

For the foregoing reasons, ETA urges the Commission to follow the FTC's and the Administration's recommendations for a self-regulatory approach to the protection of consumer privacy rather than attempt to impose prescriptive regulations which, at least in some cases, are beyond its statutory authority to adopt.

Respectfully submitted,

Scott Talbott
Senior Vice President, Government Relations
Mary C. Albert
Director, Regulatory Affairs
Electronic Transactions Association
1101 16th Street N.W., Suite 402
Washington, D.C. 20036
(202) 677-7417

May 27, 2016