Before the

Federal Communications Commission

Washington, D.C. 20554

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

Comments of WTA – Advocates for Rural Broadband

WTA – Advocates for Rural Broadband
By: /s/ Derrick B. Owens
Derrick B. Owens
Vice President of Government Affairs
400 7th Street NW, Ste. 406
Washington, DC 20004
(202) 548-0202

By: /s/ Patricia Cave
Patricia Cave
Director of Government Affairs
400 7th Street NW, Ste. 406
Washington, DC 20004
(202) 548-0202

By: /s/ Gerard J. Duffy
Gerard J. Duffy, Regulatory Counsel
Blooston, Mordkofsky, Dickens, Duffy & Prendergast, LLP
2120 L Street NW, Suite 300
Washington, DC 20037
(202) 659-0830

Date: May 27, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As traditional voice telecommunications carriers, WTA's members have deep familiarity with the privacy structure adopted pursuant to Section 222 of the Communications Act for traditional telephone service. While some RLECs apply the same opt-out and opt-in standards applicable to voice customer proprietary network information ("CPNI") as for information relating to their broadband Internet access service ("BIAS") customers along with the corresponding opt-out and opt-in marketing approvals, others simply refrain from the use of CPNI for marketing purposes altogether. The Commission should refrain from ramping up requirements on providers serving 100,000 or fewer customers (and those who do not engage in use of CPNI for marketing) when the existing rules work for small BIAS providers and their customers. At a time when small rural providers are seeing decreasing federal and state universal service support while subject to increasing deployment obligations, overly restrictive privacy requirements that necessitate expensive compliance programs will only divert funds towards regulatory compliance and away from broadband buildout in rural areas where such investment is critically needed.

The Commission must also bear in mind that applying differing rules to BIAS providers than those applicable to participants in the online ecosystem for whom online behavior advertising is a critical component of their business models (such as social media, web browsers or search engines) will likely result in confusion for consumers regarding which entities are subject to heightened privacy and security requirements. Unlike these other online entities, small telecommunications providers to date do not engage in the creation of highly detailed profiles of individual consumers or online behavioral advertising or retain substantial amounts of sensitive customer information. Furthermore, with regards to data security and risk management policies,

the Commission must refrain from adopting "one-size-fits-all" policies or micromanaging the practices of telecommunications providers and should align and calibrate its rules with expectations already in place and enforced by the Federal Trade Commission ("FTC") to ensure parity in regulation and consumer expectations of entities in the online ecosystem.

The Commission must also bear in mind that certain practices that could be inappropriately used may actually benefit consumers when used appropriately and ethically, after full disclosure to consumers, or when used to improve network management and performance. Although small BIAS providers such as WTA's members have not explored targeted advertising to the extent that large providers have, the Commission should not altogether foreclose that revenue opportunity, particularly when small providers are subject to substantial and costly broadband buildout requirements. Any rules adopted by the Commission in this proceeding should retain the ability for carriers to expand their revenue sources so long as such expansions are transparent and consistent with consumer expectations.

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

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

Comments of WTA – Advocates for Rural Broadband

WTA-Advocates for Rural Broadband ("WTA")[1] hereby submits these comments in response to the Notice of Proposed Rulemaking ("NPRM")[2] seeking comment on a proposed privacy and data security regime specific to broadband Internet access service ("BIAS") and other telecommunications providers.

I. Introduction

WTA members and other small rural local exchange carriers ("RLECs") are familiar with the handling of customer proprietary network information ("CPNI") in the voice services context.[3] Depending upon the manner in which the Commission ultimately defines CPNI in the broadband context, they will likewise come into possession of service plan information, geo-

[1] WTA – Advocates for Rural Broadband is a national trade association representing more than 300 rural telecommunications providers offering voice, broadband and video-related services in rural America. WTA members serve some of the most rural and hard-to-serve communities in the country and are providers of last resort to those communities.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, FCC 16-39, MB Docket No. 16-106 (rel. April 1, 2016) ("*Broadband Privacy NPRM*").

[3] With respect to voice telecommunications services, CPNI is generally considered to encompass information such as: (a) the telephone numbers called by a customer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a customer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a customer. Although WTA has previously challenged the Commission's legal authority to adopt data security rules for BIAS providers pursuant to Section 222 of the Communications Act in the Lifeline context, WTA generally supports the goal of protecting customer data and telecommunications networks.

location data, source and destination information and other data that are likely to be considered as broadband CPNI. However, only a small minority of RLECs and their Internet service provider ("ISP") affiliates use voice or broadband CPNI for marketing or other advertising purposes, and virtually none provide it to third-parties for such use.

First, with only a few hundred or thousand broadband customers, 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. Moreover, given the sparsely populated rural markets they serve, RLECs and their ISP affiliates generally find it more effective and economical to market new services to all potential customers in their service areas (or portions thereof) rather than to use CPNI and opt-out and opt-in measures to target specific households or classes of customers. Over the past decade, the primary CPNI issues faced by most RLECs have entailed attempts by spouses, former spouses, boyfriends and girlfriends to find out if their significant others were calling or being called by other people. These matters can be handled by employee training and company procedures, and do not require complex and expensive information security systems and measures or notifications that distract law enforcement resources from critical public safety functions.

Hence, WTA supports exemptions from the proposed new customer approval requirements, customer data security requirements and data breach notification requirements for small RLECs and their ISP affiliates that do not collect and retain broadband usage information for marketing purposes or for sale to third-parties. Moreover, WTA believes that such exemptions should apply to RLECs and their ISP affiliates that serve 100,000 or fewer broadband customers, similar to the exemption provided to small providers from enhanced

transparency requirements under the *Open Internet Order*. Moreover, in light of increasing rural customer bandwidth needs, new Commission broadband build-out requirements and limited high-cost support,[4] costly new broadband CPNI customer approval and data security requirements should not be imposed upon small companies that need every available dollar at this time for broadband network and service improvements.

For the relatively few RLECs and ISP affiliates that use, or are considering the use of, broadband CPNI for marketing purposes, the Commission should make certain that its new broadband CPNI customer approval, security and notification rules correspond as much as practicable to its existing rules for voice and cable television service.[5] Substantially similar rules and procedures for the handling and use of confidential customer information both make it easier for customers to understand and enforce their rights and for RLEC and ISP employees to understand and comply with their obligations. It would also be useful for the Commission's CPNI requirements to be congruent with Federal Trade Commission ("FTC") privacy regulation of websites, edge providers and other non-Commission-regulated entities for whom data collection, consumer profiling and online behavior advertising are critical components of their business models,[6] particularly as RLECs are also subject to FTC requirements for their non-

[4] *See Connect America Fund, et al.*, WC Docket No. 10-90, *et al*., Report and Order, Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking (rel. March 30, 2016) ("*Rate-of-Return Reform Order*") (reforming the rate-of-return portion of the High-Cost Fund to support standalone broadband, imposing certain limitations on USF recovery and budgetary controls, and imposing ambitious build-out requirements).

[5] WTA members that apply the same treatment across the board for privacy purposes have expressed that consistency increases administrative efficiency and reduces the likelihood for a violation of the CPNI rules to occur.

[6] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 55-56 (2012), 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*") (nothing that operating systems and browsers "can access all traffic regardless of location and encryption" and "may be in a position to track all, or virtually all, of a consumer's online activity to create

common carrier activities.[7] Applying wholly different rules to BIAS providers than those applicable to other major Internet participants (including the non-common carrier activities of RLEC affiliates[8]) will likely only result in confusion for consumers regarding which entities are subject to heightened privacy and security requirements.

Likewise, with regard to data security and risk management policies, the Commission should refrain from adopting "one-size-fits-all" policies or micromanaging the practices of telecommunications providers, particularly as different rules will apply to different aspects of telecommunications providers' businesses and to different online entities. The Commission should calibrate to the extent possible its privacy and data security processes with those enforced by the FTC to which carriers must already answer for their non-common carrier activities.

II. The Commission Should Harmonize Privacy Requirements Among Telecommunications Services With Existing Rules and FTC Guidance to the Extent Feasible to Reduce Complexity and Associated Burdens on Small Providers.

WTA recognizes that the nature and scope of the information classified as broadband CPNI is likely to be more extensive than the originating call, terminating call and service information included in voice CPNI. However, there appears to be no reason why the privacy principles and protections that have been successful in protecting the voice CPNI of RLECs

---

highly detailed profiles" and that "the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues" as online tracking by ISPs).

[7] WTA realizes that the differences between RLECs and Google, Microsoft, Facebook and others who engage heavily in data collection, consumer profiling and behavioral advertising may be too great to accommodate precisely similar regulation.

[8] *See* FCC-FTC Consumer Protection Memorandum of Understanding at 2 (2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-336405A1.pdf ("FCC-FTC MOU") (stating that "the scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing the non-common carrier activities engaged in by common carriers"). For example, the websites of BIAS providers are subject to FTC, rather than FCC, jurisdiction. Consumers are likely to be confused as to whether the provider's privacy policy applies to its telephone and BIAS services or use of its website, and confusion is even more likely to the extent that the FCC and FTC requirement differ.

cannot be equally successful in protecting the broadband CPNI of their ISP operations or affiliates.[9]

Many RLECs forego use of CPNI for marketing purposes altogether. Cooperatives do not target member-customers with certain characteristics, but rather offer and advertise new and improved services to all members in the areas where they are being rolled out. In fact, cooperatives are under substantial pressure from their constituencies and directors to offer the same services to all members throughout their entire service areas. Likewise, many commercial companies serve sparsely populated areas and prefer to offer and advertise new and improved services to all local residents via newspapers, community bulletin boards, websites and general mailings. They find these general offers to be much more effective and economical than to use CPNI to target certain likely customers and to deal with opt-out and opt-in procedures and related CPNI compliance. These privacy practices and procedures work well, with the most common issues being customer frustration that results when customers forget account passwords and notification issues that result from failures in automated systems.

For those RLECs that use voice CPNI for marketing purposes, the existing opt-in and opt-out notices and procedures are familiar to their customers and employees and appear to be working effectively and to the satisfaction of the vast majority of customers.

RLECs generally protect and limit access to their voice CPNI via password systems. WTA knows of no significant security breaches affecting its members. As noted above, there may have been some isolated instances where a suspicious person sought call data regarding his or her significant other. In most cases, these situations involved requests by acquaintances to

[9] RLECs typically sell wholesale broadband capacity to an affiliated BIAS provider to offer broadband service to their rural customers.

RLEC employees. The most common customer complaints regarding the existing password systems involve loss or mistakes regarding the passwords.

Similarly, WTA knows of no members that have had data breaches of a nature or magnitude necessary to notify the Federal Bureau of Investigation or the Secret Service. In spousal cases, the persons whose call detail information was sought have generally been notified, but some instances may not have been reported to the Commission.

The Commission should refrain from ramping up privacy requirements when the existing rules work for small BIAS providers that affirmatively choose to use CPNI and their customers, as well as those providers that refrain from using CPNI altogether. At a time when small rural providers are seeing decreasing federal and state universal service support while subject to increasing deployment obligations, the Commission must also consider the impact that overly restrictive privacy requirements that require carriers to implement costly compliance programs will have on broadband buildout in rural areas where such investment is critically needed. Accordingly, the Commission should entirely exempt from proposed new customer approval requirements, customer data security requirements and data breach notification requirements small RLECs and their ISP affiliates serving 100,000 customers or fewer that do not collect and retain broadband usage information for marketing purposes or for sale to third-parties.

To further reduce the burdens on small and community-based providers that are least likely to engage in anti-consumer conduct, the Commission should seek to harmonize the number of rules already applicable to these providers, simultaneously streamlining compliance and reducing the likelihood of violations to occur, by allowing providers already subject to the Commission's CPNI rules to apply their existing and effective voice CPNI procedures and

policies to broadband CPNI and by exempting providers that entirely refrain from use of CPNI for marketing.

WTA acknowledges that while voice CPNI is already clearly defined in Section 222 and the Commission's implementing rules and orders, the Commission will need to define CPNI in the broadband context. The Commission will then be able to incorporate the existing voice and new broadband-specific definition of CPNI into the broader category of customer proprietary information ("CPI"). A specific list of what is included within the scope of Section 222's CPI and CPNI definitions will be necessary to provide a level of certainty, particularly for small providers. However, WTA has substantial concerns about the Commission's proposal to expand the list to include things that have never historically fallen within the scope of Section 222 until recent enforcement actions and, in fact, were entirely outside its scope by the statute's own terms, such as name, telephone number, and other non-network or otherwise publicly available information relating to customers.[10]

Similarly, WTA has concerns about the Commission's proposal to dramatically limit the scope of "communications-related services" to Commission-regulated services as applicable to first-party use and affiliate sharing for marketing purposes.[11] The proposal would entail the use of more difficult "opt-in" procedures as opposed to the current "opt-out" standard applicable to affiliate marketing for most services offered by traditional telecommunications providers. Many RLECs currently also provide non-voice services, and there is no evidence that the current

[10] *Id.* at ¶ 56 (noting the Commission's interpretation of customer proprietary information to include personally identifiable information); *id.* at ¶ 62 (proposing a long list of data points to be included within the definition of personally identifiable information). *See also* 47 U.S.C. § 222(h)(1) (excluding subscriber list information from the definition of CPNI). Some state laws also exclude from protected personal information any information that is publicly available.

[11] *Id.* at ¶ 71.

parameters of "communications-related services" are too broad so as to place consumer privacy in jeopardy.

Furthermore, as the online ecosystem converges, the Commission will struggle with determining the scope of its own jurisdiction. This tension is best illustrated in the context of online video services. Under the Commission's proposed more limited approach to defining "communications-related services," in the case of a BIAS provider seeking to launch a purely over-the-top video product, use of covered customer information to market the new service would be subject to an opt-in rather than opt-out customer approval despite the fact that the service offered is substantially similar to its existing FCC-regulated multichannel video programming distributor ("MVPD") service. This also leads to additional questions, such as which rules properly determine the scope of the provider's obligations given that the provider is subject to both Section 222 and the cable privacy requirements in Section 551? Furthermore, what role does FTC regulation play in this instance?

Additionally, premium technical and device support is an additional service that rural BIAS providers are increasingly being requested by some customers to provide. To that end, "services related to provision or maintenance of customer premises equipment" should also remain part of the definition of "communications-related services" offered by the BIAS provider or an affiliate, as it applies currently to voice providers and their affiliates.

Similarly, the Commission should retain the current definition of "breach" under Section 64.2011(e) of its rules that specifically includes an intent element to deal with mistakes by employees in good-faith that do not result in consumer harm.[12] This would ensure that customer notification is tied to meaningful and impactful breaches, rather than inadvertent or accidental

[12] *Id.* at ¶76.

access by employees, and does not lead to notice fatigue. This would also align with the vast majority of state privacy and data security laws that exempt good-faith mistakes that do not result in consumer harm as an impetus for customer notification.[13]

The Commission should also harmonize notice requirements for voice and broadband services[14] and permit—but not require—providers to offer a single notice for all services they provide.[15] Allowing providers to offer one notice would provide a comprehensive notice to customers if they take more than one service from affiliates operating under the same brand, ultimately leading to less confusion for customers, fewer burdens on providers and more efficient use of limited resources for providers for deployment of broadband rather than regulatory compliance. For example, under this approach a provider could offer a single privacy policy on its website to include policies applicable to all of the services it offers. Alternatively, a provider could, if it so chose, include a separate privacy policy applicable for each individual service.

As with any template, the usefulness of a standardized privacy notice for providers will depend on what the final product looks like. General guidelines that allow for flexibility are

---

[13] *See, e.g.,* Alaska Stat. §45.48.050; Ariz. Rev. Stat. Ann. §44-7501(L)(1); Ark. Code Ann. §4-110-103(1)(B); Cal. Civ. Code §1798.82(g); Colo. Rev. Stat. §6-1-716(1)(a); Del. Code Ann. Tit. 6, §12B-101(1); D.C. Off'l Code §28-3851(1); Fla. Stat. Ann. §501.171(1)(a); Ga. Code Ann. §10-1-911(1); Haw. Rev. Stat. §487N-1; Id. Code Ann. §28-51-104(2); 815 Ill. Comp. Stat. 530/5; Ind. Code §24-4.9-2-2; Iowa Code §715C.1(1); Kan. Stat. §50-7a01(h); Ky. Rev. Stat. Ann. §365.732(1)(a); La. Rev. Stat. Ann. §51:3073(2); Maine Rev. Stat. Ann. Tit. 10, §1347(1); Md. Code Ann., Com. Law §14-3504(a)(2); Mich. Comp. Laws §3(b); Minn. Stat. §325E.61, Subdiv.1(d); Mo. Rev. Stat. §407.1500.1(1); Mont. Code Ann. §30-14-1704(4)(a); Neb. Rev. Stat. §87-802(1); Nev. Rev. Stat. §603A.020; N.H. Rev. Stat. Ann. §359-C:19(V); N.J. Stat. Ann. §56:8-161; N.Y. Gen. Bus. Law §899-aa(1)(c); N.C. Gen. Stat. §75-61(14); N.D. Cent. Code §51-30-01(1); Ohio Rev. Code Ann §1349.19(A)(1)(b)(i); Okla. Stat. tit. 24 §162(1); Ore. Rev. Stat. §602(1)(b); 73 Pa. Stat. §2302; R.I. Gen Laws §11-49.2-5(b); S.C. Code §39-1-90(D)(1); Tenn. Code Ann. §2107(a)(1); Tex. Bus. & Com. Code §521.053(a); Utah Code 13-44-102(1)(b); Vt. Stat. Ann. Tit. 9, §2430(8)(B); Va. Code §18.2-186.6(A); Was. Rev. Code §19.255.010(4); W. Va. Code §46A-2A-101(1); Wis. Stat. §134.98(2)(cm)(2); Wyo. Stat. Ann. §40-12-501(a)(i).

[14] *Broadband Privacy NPRM* at ¶ 103.

[15] *Id.* at ¶ 105. The Commission must, however, remain mindful that its authority is limited by the terms of the Communications Act. For example, cable operators are required to annually issue to its subscribers a separate written statement on privacy. 47 U.S.C. § 551(a)(1).

preferable to creation of a mandatory uniform and rigid template.[16] The Commission should make a standardized template available for those providers that want to use a standardized notice but should continue to permit providers to customize privacy policies to account for their unique circumstances.

The Commission should also harmonize customer solicitation and approval requirements for voice and broadband services.[17] That includes seeking opt-out approval upon service initiation and on a biennial basis for use of CPNI for first-party or affiliate marketing of communications-related services. Small providers already complying with existing CPNI rules should be able to continue the current processes in place.

The typical RLEC organizational arrangement is for the RLEC itself to provide local retail voice services and wholesale broadband transmission services and for one or more affiliates to provide resold toll services and retail BIAS service. Were the Commission to treat affiliates as third-parties requiring opt-in notices and procedures, it would wholly confuse consumers and disrupt the operations of RLECs and their toll and retail broadband affiliates. WTA vigorously opposes this approach.

RLECs also engage contractors to perform functions on their behalf to provide service to customers, including outsourced customer and technical support. Making those relationships subject to opt-in approval could frustrate the ability to provide efficient customer service. Furthermore, FTC guidance treats affiliates as third-parties only if the affiliate relationship is unknown or unclear to consumers.[18] The affiliate relationship is undoubtedly clear if a consumer

[16] *Broadband Privacy NPRM* at ¶93.

[17] *Id.* at ¶152.

[18] 2012 FTC Privacy Report at 41-42 (stating that "affiliates are third-parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers.").

receives a single bill from its provider despite subscribing to multiple services from different affiliated entities, as is the case with most small rural providers. Because small RLECs already comply with existing CPNI rules as they apply to affiliate use of customer information with few if any customer complaints, the Commission should not require opt-in approval in such instances but rather should allow these providers to continue business as usual.[19]

The Commission should also harmonize requirements for methods for providing and withdrawing consent with its existing requirements rather than imposing more stringent requirements on broadband and/or voice providers.[20] Current voice rules permit flexibility and allow providers to use a combination of methods to ensure that consumers can opt-out or otherwise change their privacy preferences at anytime.[21] There are no documented instances of customers—particularly those of small and community-based providers—not being able to change their consent preferences. Accordingly, the Commission's proposed rules for broadband should incorporate existing requirements that work rather than imposing more stringent requirements based on speculative consumer harm. The Commission's rules should also exempt entirely from solicitation requirements those providers that refrain entirely from the use of CPNI.

For example, the Commission should not adopt a new requirement that carriers develop a "privacy dashboard."[22] If it does, the Commission should entirely exempt small providers from such a requirement. Although some sophisticated online entities include dashboards that permit

---

[19] *Broadband Privacy NPRM* at ¶ 126.

[20] *Broadband Privacy NPRM*, Proposed Rules, Appendix A, 47 C.F.R. § 64.7002(d).

[21] 47 C.F.R. § 64.2008(d)(3)(v).

[22] *Broadband Privacy NPRM* at ¶ 95. The Commission should also be mindful in defining a customer's rights regarding access to and correction of CPI that Section 222 in this regard is specifically limited to CPNI. *See* 47 U.S.C. § 222(c)(2) (requiring disclosure of "customer proprietary network information, upon affirmative request by the customer"). The Commission must therefore craft its rules in line with the relevant statutory text.

consumers to adjust their privacy preferences on a very granular level, many small providers do not currently have online portals through which consumers may change their privacy preferences[23] and lack web development staff that would make development of such a tool more affordable and practicable. Small providers will need to employ a third-party to develop a privacy dashboard from scratch or work with existing vendors to incorporate a privacy component to existing online systems, with costs varying based on the complexity of the tool required. Because there have been no demonstrated instances of consumers and customers of small providers being prevented from quickly and effectively changing their privacy preferences, such a requirement would constitute an unnecessary and costly burden for providers providing little to no benefit to consumers over the current system in which customer requests are addressed immediately or in a near real-time fashion. Such a requirement would also unnecessarily divert additional resources that are critically needed for broadband deployment in rural areas.

Similarly, the Commission should apply the same one-time use notification requirements for voice and broadband providers.[24] Having two different requirements would cause confusion for consumers and small providers alike, particularly if a consumer subscribes to a bundle of voice and broadband service from the same provider.

As to breach notification, the Commission should apply the same breach notification rules to voice and broadband service, but should not impose the more stringent notification timeline proposed in the NPRM.[25] The existing CPNI breach notification timeline properly

[23] Typically, RLEC customers may contact their provider via customer service and change their opt-out or opt-in preferences. Once a customer has made a request, the change is typically implemented immediately.

[24] *Id.* at ¶ 148.

[25] *Id.* at ¶¶ 236, 241, 254.

reflects the need for victims of a breach and law enforcement to investigate and resolve the breach before providing notice to consumers and the general public. The Commission should therefore not impose a strict 10-day timeline for customer notification and should adopt a requirement that aligns with the vast majority of state privacy and data breach laws that do not impose such stringent timelines for notification. Because small rural providers often live in and have strong ties to the communities they serve, they have strong incentive to provide their customers with complete and accurate information as soon as practicable. It is paramount that these providers are able to investigate and resolve a breach prior to notification because providing their customers with incomplete or inaccurate information could leave the customer leery and could lead to a lack of trust in their provider.

Finally, the Commission should adopt the same certification and compliance requirements for BIAS and voice providers[26] because a single certification will reduce paperwork burdens for small providers. For WTA's members, typically the same staff members handle voice and broadband privacy and customer service. Providers should be permitted to file a single annual compliance certification with the Commission if they offer both voice and broadband services. Additionally, the Commission should apply the existing document retention rules for breach of both voice and broadband providers.[27] With respect to document retention and compliance rules, it makes sense to expand existing requirements that work well and with which carriers are familiar rather than imposing additional and untested requirements, particularly because additional requirements will increase reliance on USF and divert resources away from broadband deployment and adoption efforts where they are needed most.

[26] *Id.* at ¶ 149.

[27] *Id.* at ¶ 252.

III. The Commission Should Avoid Redundant Consumer Notification and Approval Requirements that Result in Notice Fatigue, Consumer Confusion and Impose Unnecessary Costs on Small Providers.

WTA's members also strongly believe that an overly-restrictive opt-in regime for customer approvals would foreclose the ability of RLECs and other small providers with the highest costs to defray the cost of deployment and ongoing investment and decrease reliance on universal service funding through revenue sources apart from customer bills. The transition to a more restrictive approach to customer approval is also likely to frustrate consumers who now will need to provide opt-in approval for what previously required no customer action if they did not want to opt-out. The Commission must also craft privacy and data breach notification rules that reflect the likelihood for consumers to become numb to over-notification and that do not impose unnecessary costs on small providers trying to comply with new rules.

For example, layered privacy notices that include plain-language disclosures in addition to more in-depth disclosure[28] could be problematic and burdensome for small providers and confusing for customers. Having two notices could also cause disputes between companies and their customers if a customer relied solely on representations made in less detailed disclosures to the exclusion of more detailed notices.

Similarly, the Commission should bear in mind that notification of attempted account changes or account access via email could result in notice fatigue[29] while simultaneously leading to the potential for increased phishing attacks if the Commission were to mandate email notification be made. Current rules require voice providers to notify consumers immediately and

[28] *Id.* at ¶ 94.

[29] *Broadband Privacy NPRM* at ¶ 203.

in general terms that account changes were made but do not include an e-mail component.[30] The Commission should not adopt requirements that could inadvertently increase the threat to consumers.

Regarding notification of privacy policies, WTA members typically provide privacy policies on their websites along with their network management practices as required by the *Open Internet Order's* Transparency rules[31] and seek opt-out approval from customers upon service initiation and on a biennial basis if they engage in the use of CPNI. Rarely are changes made to their privacy policies and rarely do customers change their privacy preferences or seek further information about a carrier's CPNI practices. If history is any indication, the administrative cost of providing written annual notices would outweigh the benefits to consumers of receiving annual notices, particularly if the privacy notices must also be persistently available online.[32] Additionally, regarding material changes to privacy policies, the *Open Internet Order* did not impose a specific timeframe for the minimum time in advance that a carrier must make changes to privacy policies known.[33] The Commission should follow that flexible framework.

---

[30] 47 C.F.R. § 64.2010(f) (permitting notification via voicemail, text or postal mail to the customer's address of record).

[31] Although exempt from the enhanced transparency rules, small providers are still subject to the baseline transparency rules established in the *2010 Open Internet Order*. *See* 47 C.F.R. § 8.3 (requiring disclosure by all BIAS providers of information regarding network management, performance, and commercial terms of service).

[32] *Broadband Privacy NPRM* at ¶ 88. Costs to provide written notice would depend on whether they must be sent via postal or electronic mail. Postal mail costs would primarily include printing, postage and work hours relating to preparing the notices. E-mail costs would include work hours to set up an automated system to generate messages, in addition to printed notices for those customers for whom providers lack working e-mail addresses.

[33] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, ¶161, n. 392 (2015) ("*2015 Open Internet Order*").

To reduce the burdens on providers and to prevent consumer frustration or fatigue, the Commission should grandfather existing opt-out approvals, at least for small providers already subject to the CPNI rules.[34] WTA's members have expressed that customers frequently get frustrated when providers seek the same information or approval multiple times even if the repeated inquiry results directly from regulations intended to protect consumers. For example, small town customers are often frustrated that they must provide a password to customer service representatives they know on a personal basis to access account information. Similarly, WTA's members are concerned that their customers will become confused and/or frustrated if bombarded with redundant solicitations. Unlike some providers that serve metropolitan or suburban areas, WTA members serve very rural communities that do not have large population centers and where most residents know each other. Because of the limited size of their customer bases, these small providers largely do not use or sell customer information of any kind to third-parties.[35] As a result the Commission should allow existing approvals to be sufficient moving forward

Similarly, "just in time" notification whenever CPI is collected or used[36] would be unduly burdensome for small providers and result in customer notice fatigue, confusion, and frustration. If the Commission were to adopt its long list of data points included in the definition of CPI, for example to include Internet Protocol ("IP") addresses as CPNI, nearly any time a customer uses a service it might need to provide notification. Because small providers primarily

[34] *Broadband Privacy NPRM* at ¶151.

[35] Not a single WTA members identified that they sell customer information to third-parties for advertising purposes. WTA member use of customer information is limited to marketing of services by the RLEC and its affiliates and sharing with third-parties to the extent necessary to render service (for example, if a third-party were engaged to deliver a package).

[36] *Id.* at ¶ 142.

use customer information for first-party and affiliate marketing (if at all), small providers should be exempt from a requirement to notify customers every time information is collected or used.

As previously discussed, the Commission should also apply the same breach notification rules to voice and broadband service and allow carriers to provide a single notification per unique customer account affected rather than requiring potentially multiple notifications per customer. There is no reason that BIAS providers should have different customer notification requirements for breaches, particularly when many BIAS providers also provide voice and/or video service as part of a bundle. Providing more than one notice could also cause consumer confusion and would be more burdensome and costly than simply requiring one notice per affected customer. In keeping with the theme of harmonization and consistency with state laws, the Commission should adopt the same flexible timeline for customer notification as already applies to voice providers. Additionally, in keeping with state laws that include a harm analysis before breach notification is required,[37] the Commission should only require notification of actual breaches that result in harm[38] to avoid over-notification and consumer notice fatigue.

[37] *See, e.g.,* Alaska Stat. §45.48.010(c); Ariz. Rev. Stat. Ann. §44-7501(L)(1); Ark. Code Ann. §4-110-105(d); Colo. Rev. Stat. §6-1-716(2)(a); Conn. Gen. Stat. §36a-701b(b)(1); Del. Code Ann. Tit. 6, §12B-102(a); Fla. Stat. Ann. §501.171(4)(c); Haw. Rev. Stat. §487N-1; Id. Code Ann. §28-51-105(1); Ind. Code §24-4.9-3-1(a); Iowa Code §715C.2(6); Kan. Stat. §50-7a02(a), 50-7a01(h); Ky. Rev. Stat. Ann. §365.732(1)(a); La. Rev. Stat. Ann. §51:3074(G); Maine Rev. Stat. Ann. Tit. 10, §1348(1)(B); Md. Code Ann., Com. Law §14-3504(b)(2); Mich. Comp. Laws §12(1); Miss. Code §75-24-29(3); Mo. Rev. Stat. §407.1500.2(5); Mont. Code Ann. §30-14-1704(4)(a); Neb. Rev. Stat. §87-803(1); N.H. Rev. Stat. Ann. §359-C:20(I)(a); N.J. Stat. Ann. §56:8-163(a); N.C. Gen. Stat. §71-61(14); Ohio Rev. Code Ann §1349.19(B)(1); Okla. Stat. tit. 24 §163(A); Ore. Rev. Stat. § 604(7); R.I. Gen Laws §11-49.2-4; S.C. Code §39-1-90(A); Utah Code 13-44-202(1)(a); Vt. Stat. Ann. Tit. 9, §2435(d)(1); Va. Code §18.2-186.6(A), (B); Was. Rev. Code §19.255.010(1); W. Va. Code §46A-2A-102(a),(b); Wis. Stat. §134.98(2)(cm); Wyo. Stat. Ann. §40-12-502(a).

[38] *Broadband Privacy NPRM* at ¶ 242.

IV. The Commission's Data Security Requirements Must Acknowledge the Unique Challenges Faced by Small Telecommunications Carriers in Ensuring Network and Customer Information Security.

WTA also has strong concerns about various aspects of the Commission's data security mandate proposal. The Commission's rules must reflect the reality that no firm or individual is immune from cyber threats and under no circumstance should the Commission take the position that existence of a breach is indicative of poor data security practices.[39] For example, the Commission's proposal that providers perform "regular risk assessment and promptly address any weaknesses" identified by such assessment fails to account for the reality that difficult decisions must be made and acceptable risk trade-offs are a critical aspect of a risk management approach to data security. Furthermore, not every vulnerability found in a risk assessment may be exploitable and therefore may not need to be remedied nor would it be possible to address every vulnerability. The Commission must also bear in mind that the challenge of data security is bigger than simply mandating implementation of technical protection measures, considering that employees are the number one threat to information security. Small providers do everything in their power to make sure that vulnerabilities are minimized, but they cannot be required to dedicate precious limited resources to combat a vulnerability that is not likely to be a substantial threat to the rest of the network and other services provided to their customers.

Because telecommunications carriers remain subject to FTC jurisdiction for their non-common carrier activities[40] and the FTC has a substantial record of data security guidance and

---

[39] From the FTC's perspective, "the mere fact that a breach occurred does not mean that a company has violated the law." *See* Prepared Statement of the Federal Trade Commission, "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches," Before the Senate Committee on Commerce Science, and Transportation, 113th Cong., March 26, 2014, *available at* https://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf ("*FTC Testimony on Data Breaches*").

[40] *See* FCC-FTC MOU at 2.

enforcement, including enforcement against entities in the online ecosystem that have substantial ability to track online consumer activity and the Commission admits are outside of its jurisdiction, it makes sense for the Commission to closely align its expectations regarding data security with those expectations already in place and enforced by the FTC.[41] Small BIAS providers in particular are at a disadvantage and lack the resources to comply with multiple regulatory regimes because they lack the sophisticated technical and legal teams necessary for compliance with varying requirements at the state and federal level as well as among federal regulations. Small BIAS providers also do not engage in the collection and retention of sensitive consumer information to the extent that other industry participants that are subject to the FTC enforcement do. Furthermore, consumers are likely to be confused or frustrated by a varying level of protection and complex regulatory schemes for similar information held by different online ecosystems (or even the same entity providing differently regulated services).

Additionally, the Commission should not stray from the flexible, best practices approach to data security by adopting specific administrative, technical or physical requirements for implementing data security requirements.[42] Nor should the Commission establish safe harbors with respect to minimum data security standards as this could be seen by some as all that is required, rather than encouraging providers to take additional steps as appropriate to manage their cyber risk.[43] Although some providers already engage in regular penetration tests of their systems, evaluate their risk management strategies using the National Institutes of Science and

---

[41] *See* Federal Trade Commission, *Start with Security: A Guide for Business* (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[42] *Broadband Privacy NPRM* at ¶¶175, 179. For example, the Communications Security Reliability and Interoperability Council provided a highly detailed and useful tool adapting the NIST Framework for Critical Infrastructure Cybersecurity. Tools such as this provide flexible and useful, non-binding guidance for carriers to use in shoring up their network and information security.

[43] *Id.* at ¶ 178.

Technology ("NIST") or other frameworks, use firewalls, and encrypt stored information, every provider has a different posture and needs and the challenge is greatest for small BIAS providers for whom expertise and resources are limited. The Commission should encourage—but not require—providers to use technical audits and penetration testing[44] because the cost to conduct such audits and testing can be substantial, particularly for small provides lacking in-house security staff and in rural areas where such expertise is in short supply. The Commission should likewise refrain from imposing a multi-factor authentication technical mandate that would require providers (and their vendors) to revise customer authentication requirements.[45] Setting specific guidelines as to multi-factor authentication or other technical measures would provide bad actors with a roadmap of what they need to effectively gain access to systems through social engineering or other methods and would be particularly burdensome for small carriers.

Similarly, the Commission should encourage—but not require—that all CPI be encrypted when stored by ISPs due to the cost of encryption that may outweigh the benefit.[46] The Commission could encourage encryption through incorporating an encryption element into the definition of "breach" or CPI as many states have done.[47] If the Commission were to decide to

---

[44] *Id.* at ¶ 181.

[45] *Id.* at ¶ 194.

[46] *Id.* at ¶ 216. For example, a WTA member reports initial costs of $300,000 to encrypt its primary customer database. Additional software, administrative and personnel costs are expected as the carrier implements encryption for other database systems, upgrades to software and increases the complexity of its systems.

[47] *See, e.g.,* Alaska Stat. §45.48.090(7); Ariz. Rev. Stat. Ann. §44-7501(L)(6)(a); Ark. Code Ann. §4-110-103(7); Cal. Civ. Code §1798.82(h); Colo. Rev. Stat. §6-1-716(1)(d)(I); Conn. Gen. Stat. §36a-701b(a)(incorporating an encryption element in the definition of "breach"); Del. Code Ann. Tit. 6, §12B-101(4); Fla. Stat. Ann. §501.171(1)(g); Ga. Code Ann. §10-1-911(6); Hawaii Rev. Stat. §487N-1; Id. Code Ann. §28-51-104(5); 815 Ill. Comp. Stat. 530/5; Ind. Code §24-4.9-2-10; Iowa Code §715C.1(11); Kan. Stat. Ann. §50-7a01(g); Ky. Rev. Stat. §365.732(1)(a)(incorporating an encryption element into the definition of "breach"); La. Rev. Stat. Ann. §51:3073(4); Maine Rev. Stat. Ann. Tit. 10, §1347(6); Md. Code Ann., Com. Law §14-3501(D)(1); Mass. Gen. Laws. 93H, §1(a) (incorporating an encryption element into the definition of "breach"); Minn. Stat. §325E.61, Subdiv.1(e); Miss. Code §75-24-

adopt an encryption mandate, it should exempt small providers as such a requirement would be unduly costly and burdensome to implement.

The Commission should continue to provide guidance and work with carriers building on the NIST Framework and other guidance but should not make any single or combination of methods mandatory.[48] Micromanaging of data security practices in this manner would be problematic and would result in a "one-size-fits-all" rule for hundreds of BIAS providers. Instead, the Commission should adopt its proposal to allow each BIAS provider to determine the particulars of and design its own risk management program, taking into account the probability and criticality of threats and vulnerabilities,[49] as well as the nature and scope of a provider's business activities and the sensitivity of the underlying data.[50] The final rule adopted by the Commission must also expressly take into account the entity's size and the cost of implementation of security measures as factors for consideration.[51] RLECs are subject to substantial limitations of the corporate operations and other operating expenses recoverable through High-Cost support, and the Commission must not impose data security requirements that

---

29(2)(a)(incorporating an encryption element into the definition of "breach"); Mo. Rev. Stat. §407.1500.1(9); Mont. Code Ann. §30-14-1704(4)(b)(i); Neb. Rev. Stat. §87-802(5); Nev. Rev. Stat. §603A.040; N.H. Rev. Stat. Ann. §359-C:19(IV)(a); N.J. Stat. Ann. §56:8-161(incorporating an encryption element into the definition of "breach"); N.C. Gen. Stat. §75-61(14) (incorporating an encryption element into the definition of "breach"); N.D. Cent. Code §51-30-01(4)(a); Ohio Rev. Code Ann §1349.19(A)(7)(a); Okla. Stat. tit. 24 §162(6); Or. Rev. Stat. §602(11)(a),(b); 73 Pa. Stat. §2302; R.I. Gen Laws §11-49.2-5(c); S.C. Code §39-1-90(D)(3); Tenn. Code Ann. §2107(a)(3)(A); Tex. Bus. & Com. Code §521.002(a)(2); Utah Code 13-44-102(3)(a); Vt. Stat. Ann. Tit. 9, §2430(5)(A); Va. Code §18.2-186.6(A); W. Va. Code §46A-2A-101(6); Wis. Stat. §134.98(1)(b).

[48] *Broadband Privacy NPRM* at ¶ 215 (discussing setting criteria for secure passwords, network segmentation, patching/updating software).

[49] *Id.* at ¶ 181.

[50] *Id.* at ¶¶ 217-220.

[51] *See FTC Testimony on Data Breaches* at 4 (noting that the FTC determines whether a company's data security measures are reasonable and appropriate "in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities").

would substantially increase costs for these providers already feeling the weight of insufficient budgets and significant broadband build-out requirements. It makes no sense to force companies to make substantial investments of scarce funds in measures to address unlikely risks or risks that would be unduly expensive to eliminate.

The Commission should likewise not define how regularly providers must conduct risk assessments.[52] Risk assessment is an ongoing process and setting a minimum frequency of assessment could discourage providers from taking affirmative steps to address risk on a continual basis. Nor should the Commission define "promptly" as part of its requirement to address any uncovered weaknesses[53] because risk management requires difficult decisions to be made regarding the acceptable level of risk for an organization in light of the resources available and the likelihood of a bad actor taking advantage of a vulnerability. Some vulnerabilities may be highly unlikely to be exploited yet expensive to fully eliminate. The Commission's rules must reflect that no entity is immune – no matter its size – or will ever be entirely secure, and that not all vulnerabilities can—or should—be resolved entirely. Also, the Commission should not require providers to disclose specifics regarding their data security practices in their privacy policies or network management disclosures.[54] Although it could provide useful information to consumers, it would also provide a playbook for bad actors.

Finally, the Commission must remain mindful of the high demand and low supply of sufficiently qualified cybersecurity professionals in contemplating a requirement that senior management officials have certain qualifications or security certifications.[55] Although some

[52] *Broadband Privacy NPRM* at ¶ 183.

[53] *Id.* at ¶ 184.

[54] *Id.* at ¶ 84.

[55] *Id.* at ¶ 190.

large companies might have information security experts on staff, requiring management-level hiring of specialized security experts in order to comply with new regulations would be particularly unreasonable for small, resource constrained RLECs due to their already small staff sizes and resources as compared to the salaries that full-time (or even part-time) experts can demand, as well as the lack or shortage of cybersecurity professionals in many rural areas. In light of these considerations, the Commission should provide an exemption for small providers of the requirement to have senior management specialized in cybersecurity.

Small providers have less ability than large BIAS providers to train and hold their contractors and other third-parties accountable for data security practices.[56] They may be able to obtain contractual commitments but have less ability to follow through on monitoring those commitments due to resource constraints. The Commission should take into account the fact that -parties are most likely already subject to the FTC's guidance on data security. Additionally, it is often outside contractors that must train small providers and their employees on information security and CPNI requirements. Therefore, the Commission should exempt small BIAS providers from the requirement to train and monitor the data security practices of third-parties. The Commission should draw heavily from the FTC's flexible approach to data security to ensure that entities have the ability to adapt and implement security measures appropriate to their businesses.

V. The Commission Should Not Adopt Prescriptive Rules Regarding Network Management and Other Business Practices That Benefit Consumers.

WTA urges the Commission to take a pause before adopting prescriptive rules that could interfere with the ability for carrier to engage in network management and other business practices that benefit consumers and reduce burdens and costs for providers. For example, deep

[56] *Id.* at ¶¶ 174, 211.

packet inspection has legitimate network management purposes such as use in resolving congestion issues, addressing distributed denial of service attacks, and resolving issues that arise in telecommunications networks.[57] Small BIAS providers have no incentive to engage in deep packet inspection for non-network management purposes and actually have a disincentive to use ongoing monitoring of customer traffic due to the service provider safe harbor provisions of the Digital Millennium Copyright Act.[58]

RLECs also use aggregate information regarding Internet traffic to make network management and investment decisions, such as whether to seek caching servers if a large segment of network traffic during peak hours relates to a single source (e.g., Netflix). Small providers that use aggregate information solely for network management-related functions should be exempt from any document retention, public commitment and disclosure requirements because there is no threat to consumer privacy in such circumstances.[59] Furthermore, a statement in a carrier's privacy policy is sufficient to constitute a public commitment not to re-identify aggregate CPI.[60] This would also more closely follow the FTC's Section 5 unfair and deceptive practices approach to privacy and security that holds providers accountable to statements in their privacy policies and for practices that cause substantial injury to consumers

[57] 2012 FTC Privacy Report at 56, n. 268 (noting strong concerns about use of deep packet inspection without consent, but expressly excluding from those concerns the use of deep packet inspection "for network management, security, or other purposes consistent with the context of a consumer's interaction with their ISP").

[58] *See* 17 U.S.C. § 512 (establishing a series of safe harbors from copyright infringement claims for ISPs acting as mere conduits for their customer's Internet traffic and establishing a duty to address the infringement upon the service provider becoming aware of such infringement).

[59] *Broadband Privacy NPRM* at ¶ 164.

[60] *Id.* at ¶ 160.

that is neither reasonably avoidable by consumers not outweighed by countervailing benefits to consumers or to competition.[61]

Finally, although small BIAS providers such as WTA's members have not explored targeted advertising to the extent that large providers have, the Commission should not altogether foreclose that revenue opportunity (or similar potential revenue streams). Any rules adopted by the Commission in this proceeding should retain the ability for carriers to expand their revenue sources so long as such expansions are transparent and consistent with consumer expectations. The Commission's broadband privacy and data security rules should reflect that certain practices that might be inappropriately used by bad actors can actually benefit consumers through innovative services and lower costs when used appropriately and ethically after full disclosure to consumers.

VI. Conclusion

WTA's members are already deeply familiar with the existing CPNI rules in the voice context, and some refrain altogether from the use of CPNI for marketing purposes and have no intention to explore its use in the broadband context. Those carriers that engage in use of CPNI for marketing purposes have systems in place to obtain the proper customer approvals, and these systems work well. The Commission should not impose any requirements regarding customer disclosure and solicitation of customer approvals on carriers with 100,000 or fewer customers and providers that do not engage in the use of CPNI for marketing purposes or for sale to third-

[61] *See, e.g.*, Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984) *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception; Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

parties. Imposing additional stringent privacy requirements will only divert critically needed resources from broadband infrastructure deployment to regulatory compliance.

With regards to data security and risk management policies, the Commission must refrain from adopting "one-size-fits-all" policies or micromanaging the practices of telecommunications providers. Under no circumstances should the Commission adopt specific technical requirements for data security risk management. Any data security standard adopted should align with expectations already in place and enforced by the FTC to ensure parity in regulation of entities in the online ecosystem and limit consumer confusion.

Finally, the Commission should not adopt prescriptive rules that could interfere with the ability for carriers to engage in effective network management and other business practices that benefit consumers and reduce burdens and costs for providers. For example, deep packet inspection and the use of aggregate information regarding Internet traffic contribute substantially to improved network management and investment decisions and should not be prohibited. Similarly, the Commission should not prohibit the ability of providers to explore additional revenue streams and offer innovative services so long as consumers are fully informed.

Respectfully Submitted,
WTA – Advocates for Rural Broadband

By: /s/ Derrick B. Owens
Derrick B. Owens
Vice President of Government Affairs
400 7th Street NW, Ste. 406
Washington, DC 20004
(202) 548-0202

By: /s/ Patricia Cave
Patricia Cave
Director of Government Affairs
400 7th Street NW, Ste. 406
Washington, DC 20004
(202) 548-0202

By: /s/ Gerard J. Duffy
Gerard J. Duffy, Regulatory Counsel
Blooston, Mordkofsky, Dickens, Duffy & Prendergast, LLP
2120 L Street NW, Suite 300
Washington, DC 20037
(202) 659-0830