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
	)	
	)	
	)	

Reply 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: July 6, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY……..……...…….iii

I. The Record Demonstrates that Small Providers are Differently Situated than Large Providers and an Alternative Approach to Privacy and Security for Small Providers is Appropriate and Necessary to Promote Broadband Deployment…..…1

II. Commenters Agree That the Commission Should Establish an Exemption for Small Providers and Those That Do Not Share Customer Information With Third Parties..……..……...5

A. Privacy Notice Format, Contents, and Frequency……..…6

B. Securing Approvals and Consents from New and Existing Subscribers…….7

C. Privacy Dashboard……8

D. Requiring Opt-In Approval and "Communications-Related Services" Defined……..10

III. Commenters Agree That the Commission's Proposed Data Security Standards and Breach Notification Timelines are Unprecedented and Must be Re-Calibrated to Account for Practical Realities, Particularly as Applied to Small Providers..……12

IV. Commenters Agree that The Commission Must Craft its Rules in a Manner that Reduces Disparity in Regulation of Entities in the Online Ecosystem..……..17

V. Conclusion……19

EXECUTIVE SUMMARY

As WTA explained in its initial comments, RLECs are already deeply familiar with the existing CPNI rules in the voice context, and many refrain altogether from the use of CPNI for marketing purposes and have no intention to explore its use in the broadband context. There is simply no incentive for small providers to engage in the conduct the Commission seeks to address in this proceeding, and most small providers find marketing their services to the general public in their service areas to be more cost-effective. Furthermore, small carriers have close ties to their communities that operate to strongly disincentivize misuse of customer data. Those carriers that do engage in use of CPNI for marketing purposes have the necessary systems in place to obtain customer approvals, and these systems have worked well for many years. Given the absence of problems and the lack of financial or other incentives for small carriers, 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 parties.

The Commission's data security proposals will also impose substantial burdens on small providers that are least likely to be able to meet a strict liability standard for security. Not only does the proposal include an unrealistic expectation of guaranteed security and confidentiality of customer data, but it also includes unprecedented notification requirements that would severely limit the ability for carriers to ensure they provide accurate notice to affected customers which will likely cause consumer confusion and distrust. Imposing additional stringent privacy and data security requirements as envisioned in the NPRM on small providers will only divert critically needed resources from broadband infrastructure deployment to regulatory compliance and result in disparate regulatory treatment for broadband providers seeking to explore new business models in the online ecosystem.

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
	)	
	)	
	)	

Reply Comments of WTA – Advocates for Rural Broadband

WTA-Advocates for Rural Broadband ("WTA")[1] hereby submits these reply comments in response to comments in the record regarding 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. The Record Demonstrates that Small Providers are Differently Situated than Large Providers and an Alternative Approach to Privacy and Security for Small Providers is Appropriate and Necessary to Promote Broadband Deployment.

Although 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] only a small minority of RLECs and their Internet service provider ("ISP")

[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

affiliates use voice or broadband CPNI for marketing or other advertising purposes, and virtually none provide it to third parties for such use. As stated in WTA's initial comments, small 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. Small carriers are typically locally-based organizations whose employees live in the same communities as their customers and maintain close relationships with them. As compared to their larger regional and national counterparts, small carriers have a strong incentive to adopt and follow reasonable policies that protect the privacy interests of their customers,[4] which in many cases include friends and family.

Contrary to assertions in the NRPM that BIAS providers have boundless ability to access and use customer data traversing over their networks, small BIAS providers simply do not engage in the comprehensive stockpiling and tracking of customer data online, nor do they sell or otherwise share customer information with non-affiliated third parties for purposes other than to provide service to their subscribers.[5] WTA and others are unaware of a single action against small providers for the types of potential privacy violations at issue in the NPRM,[6] particularly incidents regarding manipulation and insertion of non-essential information into customer traffic.

---

pursuant to Section 222 of the Communications Act in the Lifeline context, WTA generally supports the goal of protecting customer data and telecommunications networks.

[4] *See* Comments of Competitive Carriers Association ("CCA") at 33.

[5] Comments of Rural Wireless Association ("RWA"), at 3-4. Many small providers, in particular, rely on third-party vendors for billing, installation, customer service, help-desk support, etc. It would be unduly burdensome and unreasonable to require these carriers to obtain customer permission to share customer information with these vendors when such sharing is necessary in relation to providing service to the customer.

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

Even if it would not anger and offend their friends, neighbors and other customers, small BIAS providers have no business case to justify active and persistent monitoring of online activity of their limited subscriber bases[7] because third parties want much more widespread and comprehensive data. Moreover, small providers would need to make substantial investments in hardware, software and training in order to analyze and categorize customer browsing data in order to make it useful in the manner envisioned in the NPRM.[8] Small providers simply are ill-equipped from both technical and resource perspectives to engage in such conduct. The Commission must take into account these considerations and other comments in the record describing the differences among small and large providers with respect to market incentives, business models and practices when crafting its privacy and security rules..

As previously stated by WTA and others in the record, the proposed rules could potentially disrupt the policies and practices of telecommunications providers already in compliance with existing CPNI rules.[9] Incompas wisely points out that some of the proposed rules would be more difficult to comply with and would require significant modifications to current CPNI practices for voice.[10] For example, the requirement to obtain opt-in customer approval to use CPNI or CPI for the marketing of certain types of services that were previously

---

[7] Comments of RWA at 5.

[8] During a Congressional hearing regarding the Commission's proposal, Paul Ohm elaborated on current information collection practices of ISPs today and the use of browsing history for advertising. He stated that "[he] will be the first to concede that the way [users' information] is stored right now would require some engineering to extract it and to start advertising on it." Testimony of Paul Ohm, Professor, Center on Privacy and Technology, Georgetown University Law Center, before the House Energy and Commerce Subcommittee on Communications and Technology (June 20, 2016) *available at* https://energycommerce.house.gov/hearings-and-votes/hearings/fcc-overreach-examining-proposed-privacy-rules.

[9] Comments of Incompas at 3. *See also* Comments of CompTIA at 2 (nothing that the Commission's proposed definitions are "far too broad and could be interpreted to include just about any customer information").

[10] *Id.*

subject to an opt-out mechanism not only would require providers to revisit and re-do much of their existing customer approval process but also would confuse customers that had previously determined not to opt out. Providers already complying with existing CPNI rules will likely need to implement new systems or modify existing systems to track customer consents because the proposed rules are much more expansive in scope and impose new limitations than current rules.[11]

WTA agrees with WISPA that imposing additional regulations at this time will likely frustrate the congressional mandate and Commission policy to encourage the deployment of broadband to all Americans, reduce market entry barriers for small businesses and reduce barriers to investment.[12] Even carriers that are familiar with the existing CPNI rules and other privacy regulations and requirements will necessarily need to re-write existing and acceptable privacy policies, to change opt-out and opt-in procedures, to incorporate new data security and record retention requirements, and to provide notice of both intentional *and* unintentional breaches in an unreasonably expeditious manner for a very broad class of allegedly personally identifiable information regardless of whether the alleged breach is likely to cause any harm.[13]

Such additional compliance costs are likely to reduce or eliminate already minimal BIAS profits, and will ultimately require providers to increase their retail prices to consumers,[14] particularly in rural service areas where the need for broadband deployment is greatest. Rather

[11] Comments of ACA at 30. *See also* Comments of Cincinnati Bell at 5-6 (noting that with the Commission's definitional approach to CPI to include PII could require significant and expensive system changes).

[12] Comments of Wireless Internet Service Providers Association ("WISPA") at 4.

[13] *Id.* at 5.

[14] *Id.* at 27. *See also* Comments of Cincinnati Bell at 15 (stating that the Commission's proposals will likely result in higher prices or force providers to divert resources that could be used to enhance cybersecurity or expand broadband deployment).

than encouraging investment and broadband deployment, the proposal will discourage deployment by increasing costs for service providers and their customers.[15] The burden and expense of implementation will be greatest for small providers with the fewest available resources. Resources expended for expanded CPNI compliance would be better used by small providers to increase broadband deployment and availability and promote broadband literacy and adoption efforts in their communities.[16] The Commission should therefore adopt exemptions from new privacy requirements and a more flexible approach to data security for small providers and those that do not engage in the sharing of customer information with non-affiliated third-parties.

II. Commenters Agree That the Commission Should Establish an Exemption for Small Providers and Those That Do Not Share Customer Information With Third Parties.

Whereas WTA generally supports harmonizing voice and broadband customer privacy rules, it agrees that "harmonization should be pursued only to the extent that such reconfiguration does not increase obligations with regard to voice services."[17] Because so few RLECs and ISP affiliates that use, or are considering the use of, broadband CPNI for marketing purposes, new rules for broadband providers should correspond as much as practicable to the existing rules for voice that have been more than sufficient to protect telephone customer privacy. Substantially similar rules and procedures for the handling and use of confidential customer information make it easier both for customers to understand and enforce their rights and for small BIAS providers' employees to understand and comply with their obligations.

---

[15] Comments of Washington Legal Foundation at 6.

[16] The Commission's proposal is also likely to even further stifle small provider participation in cyber threat information sharing efforts as a result of increased uncertainty regarding what information carriers will be permitted under the rules to share.

[17] Comments of NTCA-The Rural Broadband Association ("NTCA") at 35.

Several particular aspects of the proposed new rules discussed below constitute substantial departures from existing practices and will be particularly burdensome for small providers if adopted. In order to avoid imposing undue burdens on small providers that would arise from these proposed rules, and to the extent that the Commission desires to increase privacy requirements in this proceeding, the Commission should exempt small providers serving 100,000 or fewer subscribers as well as providers that do not share or sell information with non-affiliated third parties from additional privacy requirements.[18]

A. Privacy Notice Format, Contents, and Frequency

Commenters in the record agree that a standardized notice format could be helpful as a safe harbor for providers and as simplification for consumers.[19] Similarly, providers should have flexibility to provide a single privacy notice that combines notification with respect to bundled services.[20] Permitting a single comprehensive notice rather than multiple notices is less burdensome for providers and provides more clarity and less likelihood of confusion for consumers.[21]

---

[18] *See* Comments of USTelecom at 9 (proposing a 100,000 subscriber threshold for a small provider exemption); Comments of RWA at 2 (proposing a 100,000 subscriber threshold for a small provider exemption); Comments of WISPA at 2 (urging exemption of small providers from new rules that would require alteration to business practices insignificant ways that would create additional costs and compliance burdens, and an extended implementation schedule for small carriers). *See also* Comments of CCA at 33 (seeking an exemption for providers that do not use customer proprietary information for marketing purposes of any kind from implementing an opt-in/opt-out interface).

[19] Comments of NTCA at 41; Comments of RWA at 7; Comments of WISPA at 16 (not opposing a standardized notice format); Comments of Hughes Network Systems ("HughesNet") at 3-4; Comments of ViaSat at 4; Comments of Electronic Frontier Foundation at 13 (stating that a standardized format could relieve regulatory burdens for providers).

[20] Comments of WISPA at 16.

[21] Although layered and more detailed notices might provide limited benefits, requiring two notices will most likely lead to more confusion and would be an additional and unnecessary regulatory compliance burden for carriers. *See* HughesNet at 3.

Nor should carriers be required to identify specifically the entities with which they share customer information and notify customers each time a new potential vendor is identified,[22] particularly if such sharing is done to facilitate service to the customer. Carriers change vendors for various reasons and are constantly exploring new options to improve their systems. Requiring updates to privacy policies to account for an evolving set of entities or having to notify every customer each time a new potential vendor or partner is identified would constitute an ongoing and unnecessary burden on providers[23] while providing little or no benefits to consumers.

Carriers should also have to provide privacy notices at the point of sale and on the carrier's website[24] rather than through periodic dissemination in customer bills or other format (for example, as a standalone mailing or e-mail. Requiring periodic dissemination of information by mail or e-mail that is easily accessible on the carriers website will provide only marginal consumer benefits and would be an additional expense increasing the costs particularly for small providers that are unlikely to make changes or engage in conduct likely to implicate privacy concerns.

B. Securing Approvals and Consents from New and Existing Subscribers

Similarly, commenters agree that needing to obtain just-in-time approval would be unduly burdensome for small providers and is likely to increase notice fatigue for consumers.[25] Given the Commission's broad proposed interpretation of the scope of customer information subject to Section 222 (even if such information is publicly available), providers will likely feel

[22] Comments of NTCA at 53.

[23] *Id.*

[24] *Id.* at 36.

[25] *Id.* at 54.

compelled to solicit consent prior to *any* use of almost *every* kind of information they obtain from their customers.[26] The Commission should therefore refrain from imposing just-in-time approval requirements or notifications.

Commenters also agree that small providers should be permitted to grandfather existing customer consents, and that small providers should be exempt from the requirement to obtain additional approvals to use and disclose customer information, provided they do not share with unaffiliated third parties for marketing purposes.[27] Because of the limited size of their customer bases, most small providers know many of their customers. And although small providers largely do not use or sell customer information for marketing purposes, many conduct biennial opt-out solicitations in accordance with existing CPNI rules. As a result, some have existing approvals to use CPNI for certain purposes subject to customers opting out in the future. WTA's members are very concerned that their customers will become confused and/or frustrated if bombarded with redundant solicitations, particularly in light of the close personal and business relationships between small providers and their customers. Requiring these carriers to seek additional customer approval would also result in an unnecessary expense for small providers that already have complied with existing CPNI approval requirements. The Commission should therefore grandfather such approvals, reducing the potential burden on small providers under the new rules.

C. Privacy Dashboard

The prospect of a mandatory "privacy dashboard" is likewise troubling for WTA members and other small providers. The American Cable Association ("ACA") describes it best

[26] Comments of ITTA at 22.

[27] Comments of ACA at 45. *See also* Comments of CCA at 33; Comments of NTCA at 55; Comments of USTelecom at 19; Comments of WISPA at 31.

in its comments that such an interface would be "a near-impossible task" for small BIAS providers.[28] WTA agrees with this characterization and urges the Commission against further consideration of this proposal. If, however, the Commission decides such a dashboard is necessary, it should exempt small providers and those that do not share customer information with, or sell customer information to, non-affiliated third parties for marketing purposes.[29]

Whereas the Federal Trade Commission ("FTC") suggests that providers include "privacy settings menus" on their websites and applications so that consumers can revisit the choices they made upon signing up for service,[30] WTA's members explain that rarely—if ever—do their customers seek to change their preferences despite their continuing ability to change preferences at any time as well as the biennial notice of the ability to opt-out. Accordingly, such a requirement would only constitute the need to make vast IT expenditures while providing little benefit to consumers.[31] This will be a particularly heavy burden for small carriers.[32] Such expenditures will result in higher prices for customers or force providers to divert resources that are critically needed at this time to expand the reach and speeds of their broadband networks.

A privacy dashboard as envisioned in the NPRM would require providers to aggregate information that is likely housed today on multiple systems and develop both internal and

[28] Comments of ACA at 38-39 (describing the challenges of implementing a privacy dashboard as envisioned in the NPRM).

[29] Voice and BIAS providers must always be permitted to share information with unaffiliated third-parties that assist in providing billing, installation, and other services necessary in the scope of providing service to their customers.

[30] Comments of Staff of the Consumer Protection Bureau of the Federal Trade Commission ("FTC Staff") at 25.

[31] Comments of Cincinnati Bell at 15.

[32] Comments of Electronic Frontier Foundation at 13.

external user interfaces. Not only would this require significant resources[33] (either due to dedicating internal staff time to developing the database or needing to engage a third-party web developer to construct and/or license such a dashboard) but such a database will only become a target for bad actors seeking to exploit databases with such large amounts of data on individual consumers. This dashboard indeed would require BIAS providers to construct full comprehensive profiles of every broadband customer, precisely the behavior the Commission seeks to deter in this proceeding. As a matter of data security, the Commission should not encourage carriers to consolidate all information relating to individual customers in a single location particularly considering the scope of information the Commission believes would be included in a privacy dashboard.[34]

D. Requiring Opt-In Approval and "Communications-Related Services" Defined

As a result of the proposed dramatic expansion of the Commission's interpretation of what data points are within the scope of Section 222 and the substantially narrowed view of "communications-related services," WTA shares concerns in the record that the Commission's definitions and a transition to a strict opt-in regime will likely "limit the ability of providers to even engage in the marketing of certain of their own products to their own customers, let alone engage in general advertising[.]"[35] As the Consumer Technology Association points out,

---

[33] Comments of NTCA at 42. Although one commenter appears to provide a "data privacy management" solution, the cost and technical requirements involved for carriers to consolidate customer information databases are unknown and will likely vary significantly from carrier to carrier depending on existing data management systems. *See* Notice of Ex Parte of Atomite, Inc., WC Docket 16-106 (fil. June 28, 2016).

[34] WTA also notes that Section 222(c)(2) explicitly directs that carriers shall disclose to customers only "customer proprietary network information" rather than the broader category of "customer proprietary information." The Commission therefore lacks authority to require carriers to disclose and provide the ability to correct non-CPNI.

[35] Comments of Mobile Future at 5. *See also* Comments of ITTA (stating that the Commission's proposal amounts to a de facto opt-in requirement for many uses of customer information, including for the marketing of an ISPs own products and services).

providers could be prohibited under the new rules from "marketing without consent a smartphone to their own customers, as they would need to use some customer information (e.g., name and email address) to market the phone" and the marketing of the phone might not meet the new definition of a "communications-related service."[36] As ACA notes, many small providers seeking to expand the services they provide will also likely need to engage an attorney to determine if a particular line of business the carrier is contemplating entering or seeking to market to its existing customers is "communications-related" or not.[37]

As WTA noted in its original comments, small providers are increasingly seeking ways to diversify their businesses and enter new markets, including through providing managed services and premium technical support to their customers. Marketing of such services under the Commission's restrictive view of "communications-related services" would require strict adherence to an opt-in customer approval process despite the fact they those services are related to the communications services offered by the provider but are not "telecommunications" or services otherwise regulated by the Commission. Accordingly, to provide clarity and coherence, the Commission should not further restrict the definition of "communications-related services," and such services should include those services offered by a provider or its affiliates that rely upon the core communications service offered by the provider,[38] including services related to provision or maintenance of customer premises equipment as under current rules.[39]

---

[36] Comments of Consumer Technology Association ("CTA") at 8-9.

[37] Comments of ACA at 29.

[38] Comments of NTCA at 31.

[39] Additionally, opt-out approval should continue to be sufficient to constitute consumer choice as long as the affiliate is known to the customer, for example by common branding or provision of a single bill for all services. This is of particular concern for small telephone companies that offer broadband and other services through affiliated ISPs.

III. Commenters Agree That the Commission's Proposed Data Security Standards and Breach Notification Timelines are Unprecedented and Must be Re-Calibrated to Account for Practical Realities, Particularly as Applied to Small Providers.

The record also demonstrates that the Commission's proposal with respect to data security standards and breach notification requirements for broadband providers is unrealistic and impracticable, and must be re-calibrated. Industry and government have coalesced around a "risk management" approach to security across all sectors based on reasonableness. This approach includes an inherent acknowledgement that all entities have an acceptable level of risk and each organization will tailor its policies and procedures to manage that risk in the most cost-effective and realistic manner under the circumstances. It is clear from the record, however, that the Commission's proposal approaches—if not surpasses—strict liability for security of customer information possessed by broadband providers.[40] Such a proposal is particularly inappropriate for small providers that lack the resources to install the expensive and constantly evolving safeguards necessary to comply with a strict liability regime.

As ACA highlights, it is often infeasible—particularly for small providers—to address *any* newly arising weakness promptly due to: (a) interrelationships and interdependencies of some of the weaknesses; (b) limited resources and expertise; and (c) the need to prioritize the most serious risks and threats.[41] A strict liability standard for security "could force an ISP to spend scarce resources on efforts to encrypt large swaths of non-sensitive data to avoid the risk

[40] *See* Comments of FTC Staff at 27 (stating that the Commission's proposed rule "would impose strict liability on companies for 'ensuring' security" and suggesting modifications to require providers to instead ensure a reasonable level of security); Comments of ACA at 24 (noting that "no provider can the security of all customer PI"); Comments of Cincinnati Bell at 8 (stating that responsibility for a security breach should not be a strict liability analysis); Comments of CompTIA at 2 (stating that "ensuring" customer PI against every threat is not feasible); Comments of CTA at 12 ("Perfect security simply does not exist, and there is a limit to how practical or feasible it is to use the same level of security in all instances, especially given a company's limited resources."); Comments of Online Trust Alliance at 3 ("There is no perfect security from a determined adversary.").

[41] Comments of ACA at 24.

of being subject to enforcement. This could be a death knell for smaller ISPs."[42] Moreover, as threats and intrusions constantly arise and evolve, a strict liability standard requires a time and resource-intensive process of surveillance, analysis and network upgrades that is beyond the capabilities of most small entities.

Rather than require that BIAS providers "ensure the security, confidentiality, and integrity of all CPI the BIAS provider receives, maintains, uses, discloses, or permits access to" as proposed in the NPRM,[43] the Commission should instead retain the existing requirement for carriers to "take reasonable measures" to protect CPNI from unauthorized access.[44] Reasonableness has become the touchstone of data security and the Commission should not divert from this approach, particularly considering that this approach will continue to govern the security practices of others in the online ecosystem that have substantially more incentive to store and analyze large amounts of consumer data. WTA and others in the record also strongly urge the Commission to include size and resources available to an entity as an explicit factor in the analysis of the reasonableness of a carrier's approach to implementing information and network security procedures,[45] and refrain from mandating specific technical or other requirements for small providers.[46] Specific security requirements will divert limited resources from network deployment and offering of innovative services to regulatory compliance without

[42] Comments of CTA at 10.

[43] *Broadband Privacy NPRM*, Proposed Rules, Appendix A, 47 C.F.R. § 64.7005(a).

[44] 47 C.F.R. § 64.2010(a).

[45] Comments of RWA at 10; Comments of ACA at 44.

[46] This would include exempting small providers from requirements that certain employees possess or obtain expensive certifications solely to comply with regulatory requirements, encrypt large amounts of stored data, and engage in frequent comprehensive system penetration tests. *See* Comments of ACA at 25 (opposing senior management have expertise as problematic for small providers); Comments of RWA at 12 (stating that "saddling small carrier employees with qualification requirements in rural markets is counterproductive and may force small rural carriers into unnecessary additional hires").

real and sustained security benefits.[47] Likewise, the Commission should not require carriers to disclose specific security practices because this would provide "a roadmap to those seeking to inflict nefarious designs upon the company's processes."[48]

Comments in the record also further highlight the unprecedented nature of the Commission's proposal with respect to including even unintentional and good-faith access by employees as a breach of security and requiring notification for access that does not result in any actual harm to consumers.[49] As Incompas accurately states, without an intent or harm standard, "customers will not understand the potential impact of breaches in the notifications they receive."[50] A requirement that carriers "ensure" confidentiality of customer information in combination with the broad interpretation of the proper scope of "customer proprietary information" are also likely to bring unintended outcomes, such as requiring notification of an alleged "breach" when a customer's bill is delivered to the wrong address[51] or carriers having to collect additional personal information in order to provide the necessary customer notifications.[52]

Small providers in particular have strong incentives to maintain their reputation and relationship with their customers and will notify their customers should harm be reasonably likely to occur. In fact, because small rural providers personally know most of their customer

[47] Comments of ACA at 53-54.

[48] Comments of NTCA at 39. *See also* Comments of Incompas at 13 (advocating against a requirement to disclose security practices); Comments of XO Communications at 16 (stating that it would be "unwise to require providers to disclose their specific security practices because it can make data and corresponding systems more vulnerable to attack and would diminish rather than advance consumer protection).

[49] Comments of Cincinnati Bell at 14 (noting that "where the account access was by an ISP employee, but was inadvertent or there was no external disclosure of CPI, there should be no obligation to report that circumstance as a 'breach' as the customer suffered no harm or potential harm"); Comments of XO Communications at 6-7 (stating that the breach definition does not include any risk analysis and thus would trigger notification for incidents of access that do not pose risk of harm).

[50] Comments of Incompas at 16.

[51] Comments of NTCA at 32-33.

[52] Comments of Coalition of Advertisers at 6-7.

and are often the largest employers in their communities, there is little to no ability or incentive to engage in deceptive or otherwise improper practices that harm their customers. Additionally, the Supreme Court has also ruled that consumers must suffer actual harm (or be reasonably likely to suffer harm) to have standing under Article III[53] and would constitute a substantial departure from existing state laws in the vast majority of states that require some analysis of harm before affected customers are notified.

Finally, commenters nearly unanimously agree that Commission's proposed breach notification rules present an unrealistic and burdensome set of criteria and requirements for alerting customers, law enforcement and the Commission about actual and inadvertent breaches whether or not such breaches result in harm (or are even a breach at all).[54] For example, the 10-day customer notification window is unprecedented even as compared to the most stringent state and federal security laws.[55] By contrast, only eight states provide any specific timeframe in their information security laws (ranging from 30 to 90 days) and the time between discovery and notification of a breach is reported to be around 40 days.[56] Such a short 10-day window provides

[53] *Spokeo v. Robins*, 136 S.Ct. 1540 (2016) (noting that "a plaintiff does not automatically satisfy the injury-in-fact requirement whenever a statute grants a right and purports to authorize a suit to vindicate it" and that "a violation of one of the [Fair Credit Reporting Act's] procedural requirements may result in no harm").

[54] Comments of Incompas at 14-15.

[55] Indeed, President Obama's data security breach notification proposal included "without reasonable delay" standard with a maximum notification timeline for notification of 30 days with a possible 30-day extension. Personal Data Notification and Protection Act, *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (last accessed July 6, 2016).

[56] BakerHostetler, Is your Organization Compromise Ready?, 2016 Data Security Incident Response Report, *available at* https://bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf (finding an average of 40 days between discovery of a breach and notification) (last accessed July 6, 2016); Navigant, Information Security and Data Breach Report, October 2014 Update, *available at* http://www.navigant.com/~/media/WWW/Site/Insights/Disputes%20Investigations/Data%20Breach%20Q2%202014_Oct%20FINAL.pdf (noting an average of 42 days from discovery to notification) (last accessed July 6, 2016); Kamala D. Harris, Attorney General, California Department of Justice, Data

inadequate time for carriers to investigate breaches[57] and provide complete and accurate notifications,[58] which ultimately will lead to notice fatigue, consumer aggravation and inconvenience, and distrust for those customers that receive multiple possibly conflicting updates stemming from a single breach.[59] Such a short window also would force providers to give notice before the nature and extent of an incident may have been ascertained, which might ultimately undermine law enforcement efforts.[60] A 2013 study also found that quick notification to consumers of a breach (defined as notification within 30 days of discovery) can actually result in higher costs.[61]

Providing accurate notification under such an expedited timeline will be particularly difficult and costly for providers with only a handful of employees who take on many roles within their organizations and may need to investigate a breach and restore security (or work with an outside vendor for incident investigation and response) while simultaneously consulting

---

Breach Report, Feb. 2016, *available at* https://oag.ca.gov/breachreport2016 (noting an average of 40 days from discovery to notification and a median time to notification of 30 days).

[57] *See* Comments of XO Communications at 12 (stating that providers "need time to contain and investigate the scope of a breach, and identify the relevant scope of data subjects at issue, so that they can provide meaningful and accurate notices to an identifiable set of consumers."). *See also* Comments of Incompas at 17-18 (arguing that the proposed reporting timeline "does not provide enough time for carriers to make data breach determinations, conduct an appropriate investigation, identify affected consumers, put remedies in place, and send notification").

[58] *See* Comments of FTC Staff at 32-33 (noting that the 10 day timeline "may not allow companies sufficient time to conduct an investigation" and that consumers are likely to get erroneous information with an artificially short notification window).

[59] Comments of ACA at 36-37; Comments of Cincinnati Bell at 13 (urging that companies should not be required to notify consumers before they have all the facts, which could lead to customer confusion); Comments of CompTIA at 5 (noting the unprecedented nature of a 10-day notification window and the additional risk to both ISPs and their customers due to incomplete or inaccurate notification that will have to be corrected); Comments of FTC Staff at 31; Comments of XO Communications at 10; .

[60] Comments of Association of National Advertisers at 30.

[61] Ponemon Institute, 2013 Cost of a Data Breach Study: United States, (May 2013) at 9 (finding that U.S. companies incurred quick customer notification resulted in higher breach notification costs) http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf (last accessed July 6, 2016).

with attorneys and insurance agents to ensure proper customer, law enforcement and regulatory notifications are complete. Small providers have every incentive to protect their customers' sensitive personal information at the same time as providing notice to their customers as soon as they have the requisite knowledge about a breach and have resolved the vulnerability at issue, and imposing unnecessarily stringent timelines and requirements will only increase costs without providing any benefits to consumers (and potentially increasing consumer distress arising out of a breach). The Commission should instead provide the same flexibility offered by current state and federal laws that enable companies to provide the best information possible to affected customers in a reasonably timely manner while balancing the need to resolve the incident or vulnerability at issue.[62]

IV. Commenters Agree that The Commission Must Craft its Rules in a Manner that Reduces Disparity in Regulation of Entities in the Online Ecosystem.

The record also demonstrates that applying wholly different rules to BIAS providers than those applicable to other major Internet participants will likely result in confusion for consumers regarding which entities are subject to heightened privacy and security requirements.[63] This is also the case for providers (including RLECs and their affiliates) which engage in non-common carrier activities[64] in trying to navigate the applicable regulatory landscape, both at the Federal

[62] Comments of Incompas at 18.

[63] For example, a customer could assume that it is immune from cyber threats due to the BIAS provider's protection of their customer information not realizing that the provider is limited

[64] *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.

and state levels. As the FTC explains, "[t]his outcome is not optimal."[65] WTA agrees that the Commission's approach to privacy and security "should be as similar as possible to that . . . which continues to govern the conduct on non-carrier participants in the Internet."[66] Indeed, 90 percent of consumers agree that all Internet companies should operate under the same set of rules.[67]

Not only would it be patently unfair as a matter of policy to apply stringent opt-in approval requirements and a strict liability security standard for BIAS providers and not for edge providers,[68] but such limited application would constitute an arbitrary distinction from a regulatory and consumer perspective. Consumers could mistakenly believe that all of their online activity is safe from bad actors because a BIAS provider must "ensure" security. However, as the record demonstrates, the same information available to BIAS providers arising out of the carrier-customer relationship is collected, used and exchanged online by edge providers and other entities.

Furthermore, the regulatory costs and complexity that would arise from an additional regulatory regime for privacy and security which small BIAS providers will need to navigate and comply with will divert resources away from broadband deployment in rural communities. Even if the Commission pre-empts applicable state laws, BIAS providers will still be subject to state and federal privacy and security laws and regulations pertaining to their non-common carrier

[65] Comments of FTC Staff at 8. *See also* Comments of Mobile Future at 6 (stating that there is "[n]o valid justification for applying more prescriptive rules to ISPs than to other members of the online ecosystem.").

[66] Comments of Cincinnati Bell at 12.

[67] Comments of Progressive Policy Institute.

[68] Comments of WISPA at 18.

activities. Particularly for small providers, "[i]nevitability of parallel enforcement underscores the need for harmonization."[69]

V. Conclusion

RLECs are already deeply familiar with the existing CPNI rules in the voice context, and many 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 have worked well for many years. WTA is aware of no significant instances of CPNI misuse or abuse by its members or other RLECs, nor any hacking attacks or other intrusions that have resulted in the theft of CPNI data from its members or other small RLECs. Given this absence of problems, 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 parties. Imposing additional stringent privacy and data security requirements as envisioned in the NPRM will only divert critically needed resources from broadband infrastructure deployment to regulatory compliance and result in disparate regulatory treatment for broadband providers seeking to explore new business models in the online ecosystem.

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

[69] Comments of Center for Technology, Innovation and Competition at 7.

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

Dated: July 6, 2016