

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

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

To: The Commission

**COMMENTS OF  
THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION**

Stephen E. Coran  
S. Jenell Trigg  
Deborah J. Salons  
Lerman Senter PLLC  
2001 L Street, N.W., Suite 400  
Washington, DC 20036  
(202) 429-8970  
*Counsel to the Wireless Internet Service Providers Association*

May 27, 2016

**TABLE OF CONTENTS**

Summary ..... iii

Background ..... 2

Discussion ..... 5

I. THE COMMISSION HAS LIMITED STATUTORY AUTHORITY TO ADOPT BROADBAND PRIVACY RULES ..... 5

II. EVEN IF IT HAS STATUTORY AUTHORITY, THE COMMISSION SHOULD ADOPT BROADBAND PRIVACY RULES THAT ALIGN WITH THE INDUSTRY FRAMEWORK ..... 8

    A. In Contrast To The Commission’s Proposal, The Industry Framework Promotes Consistency With Existing Regulatory Frameworks ..... 10

    B. In Contrast To The Commission’s Proposal, The Industry Framework Promotes Flexibility ..... 11

    C. In Contrast to the Commission’s Proposal, The Industry Framework Promotes Consumer Choice Mechanisms Available To All Entities In The Internet Ecosystem ..... 17

    D. In Contrast to the Commission’s Proposal, The Industry Framework Promotes A Reasonable Approach To Data Security ..... 19

        1. The Commission’s Proposed Definition Of “Breach” Is Overinclusive ..... 19

        2. The Commission’s Proposed Definition Of “Customer” Is Overinclusive ..... 23

    E. The Commission Should Not Expand The Scope Of Its CPNI Rules For Voice ..... 25

III. SMALL PROVIDERS SHOULD BE AFFORDED ADDITIONAL TIME TO COMPLY WITH ANY NEW RULES THE COMMISSION ADOPTS AND SHOULD BE EXEMPT FROM CERTAIN OTHER OBLIGATIONS. .... 26

    A. Small Businesses Lack The Resources To Comply With A Prescriptive And Detailed Regulatory Scheme ..... 26

    B. Small Businesses Should Have Two Years To Comply With The New Rules ..... 27

    C. Small Providers Should Be Exempt From Onerous Notice And Data Security Obligations ..... 31

IV. THE COMMISSION SHOULD ADOPT A CLEAR AND STREAMLINED ENFORCEMENT PROCESS ..... 34

Conclusion ..... 36

## Summary

The Wireless Internet Service Providers Association (“WISPA”), a trade association representing hundreds of small broadband Internet access service providers serving millions of Americans, comments in support of the flexible Industry Framework as a more efficient and effective means to protect consumers’ privacy interest than the prescriptive and expansive rules the Commission proposes. To reduce the substantial costs and compliance burdens of new rules that will disproportionately disadvantage small providers, WISPA specifically recommends that small providers be afforded an additional two years to comply with the new rules and be exempt from certain data security and breach notification requirements.

As a threshold matter, the Commission lacks authority to adopt rules extending beyond the protection of Customer Proprietary Network Information (“CPNI”). Without explicit authority, Congress cannot adopt rules regarding its contrived new category of information, which it calls “customer proprietary information.” The Commission’s reliance on Section 706(a) of the Telecommunications Act of 1996 is misplaced because adoption and application of detailed and burdensome rules will discourage, not encourage, deployment of broadband, especially for small providers that do not have, and cannot afford, compliance departments and exhaustive training programs. Section 705 of the Communications Act of 1934, as amended, is a general statute that is unrelated to the protection of private information.

The Industry Framework satisfies the Commission’s goals of transparency, consumer choice and security. Unlike the new and prescriptive structure described in the *NPRM*, the Industry Framework complements the FTC Act by prohibiting “unfair and deceptive” practices, and allowing broadband providers to adopt the methods by which it complies with this standard. This flexible approach, augmented by additional relief for small providers, strikes the appropriate balance between the privacy interests of customers and the costs and obligations of broadband

providers. By contrast, the Commission proposes a tsunami of new regulations that would micro-manage broadband providers and add significant, though undocumented, costs that outweigh whatever benefits the consumer may see.

As examples, and in addition to the expansion of rules beyond the existing CPNI rules, the Commission's proposed definitions of "breach" and "customer" do not demonstrate reasonableness. A breach should not include mere "access" to protected information or "unintentional" disclosures, but should instead be limited to actual harms such as identity theft. The proposed rules also fail to distinguish between *sensitive* personally identifiable information and *non-sensitive* personally identifiable information, which should not be treated the same. Applicants for broadband service should not be deemed "customers," a result that would prevent broadband providers from engaging in basic follow-up with those browsing for service where the privacy policy is posted on the provider's web site. In suggesting that providers provide notice of any "material change," the Commission should adopt a customer-facing definition that looks to the rights of the customer and the responsibilities of the provider. Rather than adopting broad, new rules for broadband providers and then applying them to voice providers, the Commission should restrict its new rules to the protection of CPNI and make corresponding minor edits as necessary to reflect differences in terminology.

Small broadband providers will face the difficult, if not impossible, task of complying with a vast new regulatory regime fraught with excessive implementation costs and compliance burdens that will far exceed the costs to comply with the enhanced transparency rules adopted in the *2015 Open Internet Order*. The Commission does not attempt to quantify these costs and burdens in the *NPRM* – that will be the subject of a *post hoc* Paperwork Reduction Act proceeding – but there can be no doubt that a small provider operating on a shoestring budget

must be able to budget and plan to hire lawyers, consultants and privacy experts to re-write privacy policies, re-train personnel, implement new security measures and otherwise comply with the new rules.

To this end, WISPA recommends that small providers be afforded two years to meet the new rules. Further, small providers' privacy policies should be grandfathered to avoid the need to immediately re-write acceptable policies. Small providers should be exempt from the explicit methods of protecting data proposed in Section 64.7005(a) and the size of the provider should be a factor articulated in Section 64.7005(b), to the extent the Commission adopts those or similar rules. WISPA also favors the development of a "safe harbor" template for consumer notices through the Consumer Advocacy Committee or other similar industry group. Adopting this small business relief would be consistent with the Commission's historical treatment of small businesses and the express language of the Regulatory Flexibility Act.

Finally, it is critical for the Commission to establish a streamlined and certain enforcement regime. Providers and customers should continue to be able to use arbitration to resolve their disputes, and customers should only be permitted to file informal complaints after they have attempted to privately address their privacy concerns with its provider. Sanctions should be written into the rules so that financial exposure for violations of privacy rules is both quantifiable and certain, with size and inability to pay remaining mitigating factors.

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

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

To: The Commission

**COMMENTS OF  
THE WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION**

The Wireless Internet Service Providers Association (“WISPA”), pursuant to Sections 1.415 and 1.419 of the Commission’s Rules,<sup>1</sup> hereby comments in response to the Notice of Proposed Rulemaking (“*NPRM*”) in the above-captioned proceeding.<sup>2</sup> In these Comments, WISPA submits that the Commission lacks authority to create the prescriptive and expanded broadband privacy rules it proposes in the *NPRM*. Even if the Commission has authority to adopt rules regulating broadband privacy, it should exercise restraint and follow the flexible approach proposed in the Industry Framework,<sup>3</sup> which supports the Commission’s stated objectives of consumer choice, transparency and security. The Commission’s proposed regulatory regime would unnecessarily expand the current privacy structure at significant, but unquantified, cost to the detriment of broadband providers and the customers they serve.<sup>4</sup>

---

<sup>1</sup> See 47 C.F.R. §§ 1.415 and 1.419.

<sup>2</sup> See *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 (rel. April 1, 2016) (“*NPRM*”).

<sup>3</sup> See Letter from Matthew M. Polka, President & CEO, Am. Cable Ass’n, *et al.*, to The Honorable Tom Wheeler, Chairman, FCC (Mar. 1, 2016) (on file with WCB) (Privacy Framework Discussion Paper attached to the letter will be referred to herein as the “Industry Framework”).

<sup>4</sup> Prior to adopting any final rules, the Commission should publish the specific rules it plans to adopt and invite further public comment. This practice will promote transparency in the rulemaking process by affording all parties a reasonable opportunity to weigh in on the actual final proposed rules once the pleading cycle and ex parte process have concluded.

Regardless of the approach it ultimately takes, the Commission should exempt small broadband providers from specific obligations that would impose significant and disproportionate financial and implementation burdens that will distort the Commission’s goal of a “virtuous cycle” into a “vicious cycle.” As discussed in Section III of these Comments, small broadband providers should have additional time to implement any new rules the Commission may adopt and be exempt from certain new rules that would require them to alter their business practices in significant ways that would create additional costs and compliance burdens. The regulatory regime the Commission envisions largely appears to presume that broadband providers have regulatory compliance departments that can easily incorporate new requirements into their operations. In fact, thousands of small providers – many with only a handful of staff – will face enormous financial and human resource limitations that would be passed on to their customers, many of whom live in rural and underserved areas and lack the means to pay additional costs that would be passed through to them.

### **Background**

WISPA is the trade association of more than 800 members that represents the interests of wireless Internet service providers (“WISPs”) that provide IP-based fixed wireless broadband services to consumers, businesses and anchor institutions across the country.<sup>5</sup> WISPA estimates

---

<sup>5</sup> WISPA has actively participated in the Open Internet proceeding, advocating for exemptions for small providers and fixed wireless broadband providers that use unlicensed spectrum. *See, e.g.*, Comments of the Wireless Internet Service Providers Association, GN Docket No. 14-28 (filed July 16, 2014) (“WISPA Open Internet Comments”); Comments of the Wireless Internet Service Providers Association regarding the Initial Regulatory Flexibility Analysis, GN Docket No. 14-28 (filed July 16, 2014) (“WISPA IRFA Comments”); Comments of the Wireless Internet Service Providers Association, GN Docket No. 14-28 (filed Sept. 15, 2014); Comments of the Wireless Internet Service Providers Association, GN Docket No. 14-28 (filed Aug. 5, 2015); Comments of the Wireless Internet Service Providers Association Regarding the Paperwork Reduction Act, GN Docket No. 14-28 (filed July 20, 2015) (“WISPA PRA Comments”). WISPA is also a party in the pending petition for review of the *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) (“2015 Open Internet Order”). *See USTelecom Ass’n v. FCC*, No. 15-1063 (D.C. Cir. Oral Argument Dec. 4, 2015).

that WISPs serve more than 3,000,000 people, many of whom reside in rural areas where wired technologies like FTTH, DSL and cable Internet access services are not available. All of WISPA's members currently have fewer than 250,000 broadband subscribers, a number that the U.S. House of Representatives, by a unanimous 411-0 vote, defined as "small" for purposes of approving an exemption from enhanced open Internet disclosure obligations.<sup>6</sup> A large majority of WISPA's members also have fewer than 25 employees (many have fewer than 10 employees) and are also regarded as "small entities" under the Small Business Act.<sup>7</sup> They exist on shoestring budgets and dedicate scarce resources to building and expanding broadband networks to rural, unserved and underserved areas where demand is greatest. As WISPA previously stated:

Unlike larger broadband access Internet providers that have nationwide or regional footprints, market power and increased financial human resources, WISPs are typically small, locally owned businesses with limited financial resources and small staff. Some are one-person shops in which the owner handles sales, marketing, tower-climbing, installation, billing and customer service. Many others have staff of less than ten in which these responsibilities are shared, or perhaps certain tasks such as tower-climbing or installation are contracted to third parties.<sup>8</sup>

WISPA agrees with the Commission's overarching goals of providing broadband consumers with meaningful choice, greater transparency and strong security protections.<sup>9</sup> However, as discussed below, WISPA questions both the Commission's authority to expand the

---

<sup>6</sup> H.R. 4596, 114<sup>TH</sup> Cong. (2016). The "Small Business Broadband Deployment Act" passed in the House of Representatives on March 16, 2016. A similar bill is pending in the Senate. As discussed *infra*, WISPA does not object to a larger number to define "small provider," such as the 500,000 customer metric that the Small Business Administration uses. See *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Phase II Compliance Deadlines for Non-Nationwide CMRS Carriers*, Order to Stay, 17 FCC Rcd 14841, 14847-48 ¶¶ 22-24 (2002) ("E911 Stay Order") (classifying commercial mobile radio service ("CMRS") carriers with 500,000 subscribers or fewer as of the end of 2001 as "Tier III" wireless carriers approval from the SBA); Letter from Hector V. Barreto, Administrator, SBA, to Blaise Scinto, Acting Chief, Policy Division, Wireless Telecommunications Bureau, FCC (dated Jan. 21, 2003) (approving the "Tier III" wireless classification as a small business size standard).

<sup>7</sup> See Comments of WISPA, GN Docket No. 14-28 (filed July 16, 2014), at 9.

<sup>8</sup> WISPA Open Internet Comments at 17.

<sup>9</sup> See generally *NPRM*.

scope of privacy regulation and the imposition of detailed, prescriptive rules that would outweigh the additional consumer benefits the Commission perceives to exist.

The Commission rightfully recognizes that its rules will burden small providers.<sup>10</sup> Although “privacy is a concern which applies regardless of carrier size or market share,”<sup>11</sup> it does not necessarily follow that the *same* rules should apply across the board. As is the case today, the overall privacy *framework* should be the same for all broadband providers, but the limited financial and staffing resources of small providers should be taken into account, consistent with the statutory requirements of the Regulatory Flexibility Act, as amended (“RFA”)<sup>12</sup> and Section 257 of the Communications Act of 1934, as amended (the “Act”).<sup>13</sup>

Given the challenges that small broadband providers face and the critical role they play in delivering fixed broadband access to rural and underserved areas, imposing additional regulations would frustrate Congressional mandate and Commission policies intended to encourage the deployment of broadband services to all Americans, to reduce market entry barriers for small businesses,<sup>14</sup> and to reduce barriers to investment.<sup>15</sup> In addition, reducing the economic impact on small businesses is very important. As President Obama stated, “[i]n the current economic environment, it is especially important for agencies to design regulations in a cost-effective manner consistent with the goals of promoting economic growth, innovation, competitiveness, and job creation.”<sup>16</sup> By contrast, the proposals set forth in the *NPRM* will

---

<sup>10</sup> *Id.* ¶ 151.

<sup>11</sup> *Id.* ¶ 219.

<sup>12</sup> 5 U.S.C. §§ 601, *et seq.*

<sup>13</sup> 47 U.S.C. § 257.

<sup>14</sup> *Id.*

<sup>15</sup> *See* 47 U.S.C. § 1302(a) and (b).

<sup>16</sup> *See* Presidential Memorandum at 3828. Presidential Memorandum of January 18, 2011, *Regulatory Flexibility, Small Business, and Job Creation, Memorandum for the Heads of Executive Departments and Agencies*, 76 Fed. Reg. 3827, 3828 (Jan. 21, 2011) (when initiating a rulemaking give “serious consideration to whether and how it is appropriate, consistent with law and regulatory objectives, to reduce regulatory burdens on small businesses,

especially and disproportionately burden small providers by, for example, forcing them to re-write existing and acceptable privacy policies, to change implied consent, “opt-in” and “opt-out” approval procedures, to incorporate new data security and record retention requirements, and to provide notice of intentional and unintentional data breaches in an unreasonably expeditious manner, for a very broad class of personally identifiable information (“PII”).

## Discussion

### **I. THE COMMISSION HAS LIMITED STATUTORY AUTHORITY TO ADOPT BROADBAND PRIVACY RULES.**

The Commission claims authority to adopt broadband privacy rules under Section 222 of the Act, and believes there is also support in Sections 201, 202 and 705 of the Act, and Section 706 of the Telecommunications Act of 1996 (the “Telecom Act”).<sup>17</sup> These sources of potential authority are legally suspect.

In the *2015 Open Internet Order*, the Commission concluded that Section 222 should be applied to newly-classified Title II broadband Internet access service.<sup>18</sup> As a result of reclassification, the Commission assumed the Federal Trade Commission’s (“FTC”) authority to regulate broadband<sup>19</sup> because Section 5 of the FTC Act specifically bars the FTC from regulating common carriers when they are acting as common carriers.<sup>20</sup> If the D.C. Circuit Court of

---

through increased flexibility”) (“Presidential Memorandum”). The Presidential Memorandum was issued concurrently with Executive Order 13563, which reinforced the importance of compliance with the RFA for all federal agencies. 76 Fed. Reg. 3821 (Jan. 21, 2011). President Obama issued subsequent Executive Order 13579 that expressly imposed the obligations of Executive Order 13563 on independent regulatory agencies. 76 Fed. Reg. 41587, § 1(c) (July 14, 2011) (“Executive Order 13563 set out general requirements directed to executive agencies concerning public participation, integration and innovation, flexible approaches, and science. To the extent permitted by law, independent regulatory agencies should comply with these provisions as well.”).

<sup>17</sup> *NPRM* ¶ 294.

<sup>18</sup> *See 2015 Open Internet Order* ¶ 456.

<sup>19</sup> 15 U.S.C. § 45(a)(1).

<sup>20</sup> *See* 15 U.S.C. § 45(a)(2). When broadband service was classified as an information service and not a common carrier service, the FTC released a series of precedent-setting consent orders focusing on transparency, choice and security for broadband customers. *See NPRM* ¶ 8.

Appeals in *USTelecom*<sup>21</sup> rejects reclassification of broadband providers as Title II common carriers, so, too, must the Commission's claim of authority fail under Sections 201, 202 and 222, and the FTC's authority would be reinstated.

Assuming the D.C. Court of Appeals upholds the Commission's reclassification of broadband Internet access service as a Title II service, the Commission's regulatory authority would be extremely limited by the plain language of Section 222. In adopting that statutory provision in 1996, Congress restricted the Commission to implementing rules "with respect to CPNI" and no more.<sup>22</sup> CPNI – Customer Proprietary Network Information – is defined in Section 222 as: "information that relates to the quantity, technical configuration, type, destination, location, and amount of use a telecommunications service subscribed to by any customer of a telecommunications carrier, and this is made available to the carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."<sup>23</sup> Congress did not give the Commission authority under Section 222 to implement rules that extend beyond information deemed to be CPNI.<sup>24</sup>

Further, Sections 201 and 202 are not independent sources of authority, but rather rules of general application that cannot be construed to permit the Commission to exceed the limiting language of Section 222, which permits the Commission to regulate only CPNI. Had Congress intended the Commission to broadly regulate the privacy of consumer information, it would have

---

<sup>21</sup> *USTelecom Ass'n v. FCC*, supra note 5.

<sup>22</sup> See H.R. Rep. No. 104-458, at 205 (1996) (CONF. REP.) ("In general, the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI"). *Id.*

<sup>23</sup> 47 U.S.C. § 222(h)(1).

<sup>24</sup> See supra note 22.

expressly included that specific directive in Section 222 of the statute. Instead, Congress limited the Commission to adopting rules concerning CPNI.

To bootstrap its claim of statutory authority, the Commission claims that “rules governing the privacy and security practices of BIAS providers, such as those discussed in this Notice, would be independently supported by Section 706 [of the 1996 Telecom Act].”<sup>25</sup> Yet, Section 706(a) requires the Commission to “encourage the *deployment* on a reasonable and timely basis of advanced telecommunications capability to all Americans” and to utilize “methods that *remove barriers* to infrastructure investment.”<sup>26</sup> The *NPRM* fails miserably to articulate how a prescriptive and onerous privacy regulatory scheme will encourage deployment and remove barriers. Rather, the Commission recites the “virtuous cycle” mantra that the proposed requirements “have the *potential* to increase customer confidence in BIAS providers’ practices, thereby boosting confidence in and therefore use of broadband services, which encourages the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.”<sup>27</sup>

The Commission provides no economic or market studies to support this “potential” outcome. To the contrary, for small providers, it is exceedingly more likely that the burdens and costs to implement the Commission’s proposals will have the opposite effect. New entrants will stay on the sidelines, and existing small providers will be forced to expend money and human resources on excessive compliance measures that will divert investment away from deployment to areas where broadband access or competition is lacking and creating distrust with consumers through “notice fatigue.” Small providers have already demonstrated that they have decreased

---

<sup>25</sup> *NPRM* ¶ 209.

<sup>26</sup> 47 U.S.C. § 1302(a) (emphasis added).

<sup>27</sup> *NPRM* ¶¶ 98-99 (emphasis added).

investment in broadband deployment as a result of the *2015 Open Internet Order*,<sup>28</sup> and dictating a new privacy regulatory regime on top of that will make matters far worse. While citing the “virtuous cycle” may be convenient, it simply does not hold up under even cursory scrutiny when the interests of small providers are considered. When properly considered, the “virtuous cycle” transforms into a “vicious cycle.”

Section 705(a) of the Act likewise cannot be an independent source of authority for regulating common carriers’ privacy practices.<sup>29</sup> That statute states in relevant part that “no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception.”<sup>30</sup> To the extent this language relates at all to bits traversing the Internet, it concerns only the information that is transmitted and received, not any of the information that a broadband provider may store that is not transmitted by wire or radio communications, such as PII.

## **II. EVEN IF IT HAS STATUTORY AUTHORITY, THE COMMISSION SHOULD ADOPT BROADBAND PRIVACY RULES THAT ALIGN WITH THE INDUSTRY FRAMEWORK.**

The Commission seeks comment on the publicly proposed broadband privacy frameworks and recommendations of various stakeholders and how these proposals correspond

---

<sup>28</sup> See *Protecting and Promoting the Open Internet*, Joint Petition for Stay of United States Telecom Association, *et al.*, GN Docket No. 14-28 (May 1, 2015), at Exhibits 1-3 and 5-7 (Declaration of Nathan Stooke, CEO of Wisper ISP, Inc.; Declaration of L. Elizabeth Bowles, President and Chairman of Aristotle Inc.; Declaration of Kenneth J. Hohhof, President of Express Dial Internet dba KWISP; Declaration of Clay Stewart, CEO of SCS Broadband; Declaration of Forbes H. Mercy, President of Washington Broadband, Inc.; and Declaration of Josh Zuerner, President and CEO of Joink LLC).

<sup>29</sup> 47 U.S.C. § 705(a).

<sup>30</sup> *Id.*

with the Commission’s proposed framework.<sup>31</sup> WISPA endorses the Industry Framework, a proposal submitted by a number of industry stakeholders to the Commission and Congress.<sup>32</sup> WISPA agrees with the Industry Framework that “[t]he FCC’s rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach”<sup>33</sup> and that the Commission’s policies, rules, and enforcement practices should “conform to the longstanding limiting principles articulated in the FTC’s Unfairness and Deception Policy Statements.”<sup>34</sup>

Both the Industry Framework and the Commission’s proposals are predicated on meeting the objectives of transparency, choice and data security. Beyond those overarching goals, however, the two proposals diverge significantly, with the Industry Framework promoting flexibility and harmony with the FTC Act while the Commission is suggesting an elaborate set of prescriptive and intrusive rules that would micro-manage the relationship between the broadband provider and its customer. Rather than a set of prescriptive and onerous rules, the Industry Framework complements the existing foundation in the well-established and successful FTC Act by proposing reasonable guidelines and principles to “provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments.”<sup>35</sup>

WISPA agrees that “[a]doption of this approach would be less disruptive for the broadband ecosystem, minimize consumer confusion, subject all entities in the Internet ecosystem to comparable privacy regimes, and protect consumer privacy in a manner that

---

<sup>31</sup> *NPRM* ¶¶ 278-9.

<sup>32</sup> Industry Framework.

<sup>33</sup> *Id.*

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

provides the flexibility the marketplace needs in order to innovate and evolve.”<sup>36</sup> These benefits resonate more clearly for small broadband providers, which will under the Industry Framework be able to retain existing privacy policies that are compliant with FTC policies, state law requirements and longstanding industry practices.

To quote the Industry Framework, “[n]othing has changed in the way ISPs collect and use data. The only thing that has changed is that the FCC’s action in reclassifying broadband service has negated the FTC’s power to apply its well-accepted framework to ISPs.”<sup>37</sup> That assumption of authority does not require the Commission to exceed the well-reasoned regulatory construct that has effectively served consumers and broadband providers, a fact the Commission recognizes by not identifying any defects with FTC privacy regulation or with state laws. Rather, in the absence of harm to consumers, the Commission implicitly should exercise restraint and not erect barriers that will thrust a stick into the spokes of the “virtuous cycle” and upend the ability of providers – especially small providers – to deploy, invest and compete.

**A. In Contrast To The Commission’s Proposal, The Industry Framework Promotes Consistency With Existing Regulatory Frameworks.**

The *NPRM* observes that “both Commissions have found that Section 201 of the Communications Act and Section 5 of the FTC Act can be read as prohibiting the same kinds of acts or practices.”<sup>38</sup> The FTC Act prohibits “unfair or deceptive acts or practices affecting commerce”<sup>39</sup> and Section 201(b) of the Act states that common carrier “practices ... in connection with such communication service, shall be just and reasonable, and any such ... practice ... that is unjust or unreasonable is hereby declared to be unlawful.”<sup>40</sup> The Commission

---

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *NPRM* ¶ 306.

<sup>39</sup> 15 U.S.C. § 45(1).

<sup>40</sup> 47 U.S.C. § 201(b).

states in the *NPRM* that “[t]here is a distinct congruence between the practices that are unfair or deceptive and many practices that are unjust, unreasonable, or unreasonably discriminatory.”<sup>41</sup>

The FTC’s standard is not broken and has worked to protect broadband consumers for many years, and there is no evidence presented in the *NPRM* that broadband providers are causing increased consumer harm. It is therefore unnecessary for the Commission to go beyond the FTC’s “unfair and deceptive practices” approach that delegates the means of compliance to the provider consistent with reasonable business practices, mandatory standards, and the features and resources of the provider, including its size. Ultimately, for small providers that exist on a shoestring budget, additional compliance burdens will mean less capital to invest in broadband deployment, higher prices, fewer customers and therefore, slower adoption.

WISPA also agrees that the Industry Framework will enable the Commission and the FTC to achieve the goals stated in their Memorandum of Understanding by avoiding “duplicative, redundant or inconsistent oversight” and consistent policies and basis for enforcement.<sup>42</sup> Adopting the Industry Framework along with WISPA’s recommendations in Section III will allow a seamless transition between the two agencies, reduce administrative burdens, avoid duplication of regulations and provide certainty for providers and their customers, with appropriate enforcement mechanisms for those entities that do not comply.

**B. In Contrast To The Commission’s Proposal, The Industry Framework Promotes Flexibility.**

Any new rules should, consistent with the Industry Framework, provide a flexible framework for broadband providers, especially small providers, to “implement and update their practices and update their practices in ways that meet the privacy and security needs and wants

---

<sup>41</sup> *NPRM* ¶ 306.

<sup>42</sup> Industry Framework, *citing to* FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 2015).

of their customers and address changing and new developments in this space.”<sup>43</sup> WISPA agrees that the “framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals.”<sup>44</sup> Adopting a flexible approach will allow large and small providers to implement core privacy principles based on existing and evolving consumer interests and privacy protection methods, not the interests of a federal regulator that cannot possibly understand the structure, resources and limitations of every broadband provider or the relationship between the provider and its customers.

By contrast, the *NPRM* proposes specific disclosure and notice requirements for a broadband provider’s privacy and security policies, as well as specific requirements regarding notice of a “material change” to a broadband provider’s privacy policy.<sup>45</sup> WISPA opposes these far-reaching requirements because detailed and prescriptive rules do not permit variations in the way policies are disclosed in a clear and conspicuous manner and do not permit innovation in the way that data can be used and stored. Instead, WISPA agrees with the Industry Framework’s proposed principle for transparency: “A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.”<sup>46</sup> This principle intentionally tracks the FTC’s focus on preventing deceptive and unfair practices without prescribing the specific methods for doing so.

This approach also exposes a serious flaw in the Commission’s proposed scheme — the vast expansion of the universe of information that would be subject to protection. Rather than

---

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *NPRM* ¶ 82.

<sup>46</sup> Industry Framework.

using the existing definition of CPNI and adapting it to reflect the inherent differences between a customer's voice and broadband information, the Commission proposes to classify information that would be protected under Section 222 as *customer proprietary information*<sup>47</sup> that is defined as "private information that customers have an interest in protecting from public disclosure," including both: 1) CPNI, and 2) PII collected by providers through their provision of broadband service.<sup>48</sup> The rules adopted for voice service pursuant to Section 222 were limited by the statute to CPNI,<sup>49</sup> and those rules do not separately define customer proprietary information or PII.<sup>50</sup> Neither does Section 222. In fact, the term "customer proprietary information" appears nowhere in the Communications Act. Thus, the proposed inclusion of PII in the definition of customer proprietary information is a *significant expansion* of the information currently covered under Section 222, and the rules implementing that statutory provision for voice. Notably, the *NPRM* makes no effort to quantify the costs a provider would need to expend in order to protect this broader set of both sensitive and non-sensitive information.

The Commission further attempts to justify its definition by relying on the *TerraCom NAL*,<sup>51</sup> where it "recognized the obligation of providers to protect the confidentiality of customer proprietary information pursuant to Section 222(a) in the enforcement context."<sup>52</sup> In fact, the parties subject to the *TerraCom NAL* were not broadband providers or even traditional landline providers, but providers of Lifeline services. Moreover, the Commission's enforcement action was predicted on a breach of Sensitive PII, such as social security numbers, driver's license

---

<sup>47</sup> The Commission abbreviates this term to "Customer PI" in the *NPRM*, although "PI" is generally understood to mean "personal information" and not "proprietary information." Notwithstanding, the term "customer proprietary information" is used in these Comments in order to discuss the contents of the Commission's proposal.

<sup>48</sup> *NPRM* ¶ 57.

<sup>49</sup> *Id.* ¶ 56.

<sup>50</sup> *Id.* ¶ 59.

<sup>51</sup> See *TerraCom, Inc., & Yourtel Am., Inc.*, Order and Consent Decree, 30 FCC Rcd 7075 (Enf. Bur. 2015).

<sup>52</sup> *NPRM* ¶ 56.

numbers, state ID cards, state and federal tax returns, and social security benefit statements for citizens with lower incomes less likely to have the resources to help defend and recover from an egregious privacy breach.<sup>53</sup> The Commission should not use this case as justification to apply new rules to all broadband providers that would result in a vast expansion of the types of information subject to privacy and security protection.

The Commission’s proposed reliance on the definition of “material change” in the *2015 Open Internet Order* also lacks applicability in the privacy protection context. There, the Commission defined “material change” as “any change that a reasonable consumer or edge provider would consider important to their decisions on their choice of provider, service, or application.”<sup>54</sup> In the *NPRM*, the Commission asks whether this definition should be changed.<sup>55</sup> Yes, WISPA believes that the definition of “material” should be changed. The definition adopted in the *2015 Open Internet Order* is a poor fit for a privacy regime because it is not directly applicable to the purpose of a privacy policy, which is to inform a consumer of how his or her PII will be collected, used, disclosed, and retained. Instead, a “material change” for a privacy policy requiring express “opt-in” consent should be one that changes the customer’s rights and/or the responsibilities of the provider pertaining to the collection, use, disclosure and retention of the customer’s PII, particularly when such changes are retroactive.

It is a longstanding bedrock principle in the privacy world that “companies should provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection.”<sup>56</sup> Materiality will vary

---

<sup>53</sup> See *TerraCom NAL*, 30 FCC Rcd 13325 (2014).

<sup>54</sup> *NPRM* ¶ 35, citing to *2015 Open Internet Order*, at 5671-2.

<sup>55</sup> *NPRM* ¶ 57.

<sup>56</sup> FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012) (“FTC 2012 Privacy Report”), at 57, available at: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses->

depending on whether the customer is an existing customer or a new customer. A provider should be encouraged to update its privacy policy regularly to reflect the introduction of new services, features, technology, and/or business practices. Arguably, the addition of such new provisions are material to the privacy policy overall, but not necessarily material to an existing customer if the provider will not change the way it collects, uses, discloses or retains that customer's PII. Only new customers, or existing customers that subscribe to the new service separate and apart from the then-current service being provided, will be subject to the new collection, use and disclosure of PII. And the privacy policy would reflect what is required of the business and customer rights for its new service(s).

In this instance, there should be no requirement to notify or secure the "opt-in" consent to the new services from existing customers because there is no retroactive change in the collection, use, disclosure or retention of their PII already submitted to the provider.<sup>57</sup> Under the *NPRM's* proposed definition of material, a provider would be required to notify every customer every time it made a material change to its privacy policy, which discourages timely updates and the introduction of new services and features. It also increases customer confusion and the very real potential for a provider to lose existing customers if customers were required to re-opt in to a revised privacy policy, whether or not their rights changed.<sup>58</sup> Consequently, the reasonable course of action is for the Commission to retain the longstanding principle of what is deemed to be a "material change" in the privacy context and require express "opt-in" consent only when the

---

policymakers (last visited May 23, 2016); *see also In re Facebook, Inc.*, FTC File No. 092-3184 (Nov. 29, 2011) (proposed consent order), available at <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>. and *In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), available at <http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf>.

<sup>57</sup> For material changes that benefit consumers, such as a shorter retention period for certain PII, an "opt-out" regime would be practical. *See* FTC 2012 Privacy Report, at 57 and n.227.

<sup>58</sup> The provider should still be required to post its revised privacy policy clearly and conspicuously.

customer's rights change for PII already collected by the provider, and afford the provider the discretion to provide notice in whatever reasonable and comprehensive way that corresponds to its business practices and its customers' expectations.

If the Commission adopts prescriptive and specific privacy notice regulations, WISPA does not oppose the adoption of a "safe harbor" notice template that could be developed through a multi-stakeholder group in much the same way the Community Advisory Committee ("CAC") developed a "safe harbor" template for open Internet network management disclosures to consumers.<sup>59</sup> Like the "nutrition label" presented by the CAC and approved by the Commission, a layered privacy policy notice that includes both a plain language and more in-depth disclosure<sup>60</sup> should be considered. WISPA participated in the CAC's development of the "safe harbor" template and looks forward to working in similar fashion with any multi-stakeholder group the Commission may authorize for privacy disclosure purposes in the future.

In the near term, WISPA expects that trade associations will develop best practices to complement the Industry Framework. Until there is a market failure or existing laws, regulations and best practices have proved inadequate, the better policy choice for the Commission is to exercise restraint to enable industry self-regulation that has some mechanism for enforcement by the Commission.

WISPA does agree with the Commission that a provider that offers bundled service such as a "triple play" should have the flexibility to combine privacy notices, which is a standard practice for businesses that offer varying products and services.<sup>61</sup> A combined privacy policy would provide more clarity and less confusion to customers. For providers combining privacy

---

<sup>59</sup> *NPRM* ¶ 91.

<sup>60</sup> *Id.* ¶ 94.

<sup>61</sup> *Id.* ¶ 105.

policies, it would reduce the administrative burdens and costs of developing and maintaining separate policies, especially for small carriers that do not have sufficient resources.

**C. In Contrast to the Commission’s Proposal, The Industry Framework Promotes Consumer Choice Mechanisms Available To All Entities In The Internet Ecosystem.**

WISPA agrees with the Industry Framework principle regarding choice: “A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider’s actions are not unfair or deceptive.”<sup>62</sup> As examples, customer choice could be inferred from: product and service fulfillment, fraud prevention, compliance with the law, responses to government requests, network management, first-party marketing and affiliate sharing where the affiliate relationship is clear to consumers. The Industry Framework explains that this principle is consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem.

By contrast, the *NPRM* proposes three tiers of customer approval for the use and sharing of customer proprietary information: 1) consent implied by the provider-customer relationship; 2) “opt out” consent; and 3) “opt in” consent.<sup>63</sup> The application of the Commission’s proposed system would force broadband providers to reevaluate all of their current policies and potentially rewrite privacy policies and seek different customer approvals. By contrast, adopting the Industry Framework’s proposal will provide for a more seamless transition, with less burden on providers, and will retain the same consumer protections.

The Industry Framework constitutes a more flexible approach that complements the FTC “unfair and deceptive trade practice” standard and allows the provider to consider the sensitivity

---

<sup>62</sup> Industry Framework.

<sup>63</sup> *NPRM* ¶ 109.

of the data and the context it was collected when determining the appropriate choice mechanism. WISPA supports implied consent and “opt out” consent mechanisms, but opposes any “opt in” approach, unless it pertains to material changes in a privacy policy as WISPA describes above. Consistent with the Industry Framework, WISPA agrees that providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where failure to provide choice would be deceptive or unfair.<sup>64</sup> This goal can be accomplished with an “opt-out” regime. Conversely, an “opt-in” regime would impair the ability of companies to develop new uses for information – cutting them off before ever exploring the possibilities of marketplace benefits – that could provide additional revenue streams that customers might find useful.

Further, it is patently unfair and discriminatory for broadband providers to receive “opt-in” consent for the use of information, and to not require edge providers to obtain the same “opt-in” approval. Broadband providers will be stymied in their efforts to develop new business models, while edge providers will remain unrestricted in their ability to generate revenues from user data they receive from the same Internet platforms.

WISPA agrees with the Commission’s proposal in the *NPRM* to allow broadband providers to use, disclose, and permit access to aggregate customer proprietary information under certain conditions.<sup>65</sup> Consistent with the Industry Framework, WISPA believes that the Commission should allow broadband providers to continue to use aggregated data for analytics, network management and to improve customer service, so long as that information does not disclose a known individual.

---

<sup>64</sup> Industry Framework.

<sup>65</sup> *NPRM* ¶ 154.

**D. In Contrast to the Commission’s Proposal, The Industry Framework Promotes A Reasonable Approach To Data Security.**

WISPA agrees with the Industry Framework data security principle: “a telecom provider should establish, implement and maintain a CPNI data security program that is *neither unfair nor deceptive* and includes *reasonable* physical, technical and administrative security safeguards to protect CPNI from unauthorized access, use and disclosure.”<sup>66</sup> The Industry Framework security principle also proposes a flexible approach in stating that providers’ CPNI data security programs should provide reasonable protections in light of the nature and the scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.<sup>67</sup>

**1. The Commission’s Proposed Definition Of “Breach” Is Overinclusive.**

In the CPNI rules, Section 64.2011(e) states that a “breach” occurs “when a person, without authorization or exceeding authorization, has *intentionally* gained access to, used, or disclosed CPNI.”<sup>68</sup> Contrary to this definition, the Commission’s proposal would not differentiate between intentional breaches and unintentional breaches, but would treat them the same. This proposal substantially broadens the liability for providers. For example, an employee that accidentally stumbles across CPNI in its employer’s system would create a breach, even if the information including non-sensitive PII, was never disclosed. Further, the proposed definition would cover all customer proprietary information not just CPNI.<sup>69</sup> Here again, the Commission is proposing to extend its rules well beyond the limits of CPNI, an

---

<sup>66</sup> Industry Framework (emphases added).

<sup>67</sup> *Id.* See, e.g., *In re TRENDnet, Inc.*, FTC Decision and Order, Docket No. C-4426 (Jan. 16, 2014), at p. 6 (requiring a professional assessment to “explain how such safeguards *are appropriate to respondent’s size and complexity*, the nature and scope of respondent’s activities, and the sensitivity of the Covered Device Functionality or Covered Information”), *available at*: <https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf> (last visited May 27, 2016)..

<sup>68</sup> 47 C.F.R. § 64.2011(e) (emphasis added).

<sup>69</sup> See *NPRM* ¶ 75.

unnecessary overreach given that breaches of PII are already regulated by state data statutes and other consumer protection laws.<sup>70</sup>

The Commission's proposal to require notification of any breach of customer proprietary information would be harmful to consumers, too, by potentially resulting in an exponential increase of "notice fatigue."<sup>71</sup> Consumers should not be overwhelmed with inconsequential notices that potentially create unwarranted distrust of its providers. Breach notices should be reserved for situations where a consumer's CPNI is the most vulnerable to actual mis-use.<sup>72</sup>

The Commission's proposed definition also suffers from a number of defects. First, the inclusion of the term "access" is too imprecise and will result in notifications of alleged or suspected breaches in circumstances that really do not pose any harm or threat to consumer privacy, security or well-being, such as the accidental internal access illustrated above.<sup>73</sup> The trigger for any notification should focus on intentional acquisition or disclosure because there is no risk of harm to consumers from mere "access" without acquisition, use or disclosure. WISPA thus recommends eliminating the word "access" from the definition of breach.

Second, the various types of customer proprietary information that would be subject to security breach notification are considerably more broad than the definition of "Personal Information" that govern 47 states, three U.S. Territories and the District of Columbia's security

---

<sup>70</sup> See, e.g., Press Release, "Ohio Attorney General Sues Over Customer Data Theft, Ohio Attorney General's Office" (Jun. 16, 2005), *available at*: <http://www.e-commercealert.com/article690.shtml> (last visited May 26, 2016). In the absence of a state security breach notification law, the Attorney General filed suit alleging that DSW, Inc.'s "failure to contact each customer was an 'unfair or deceptive act or practice' in violation of section 1345.02(A) of the Ohio Revised Code." *Id.*

<sup>71</sup> See NPRM, ¶ 22 ("recognizing the harms inherent in over-notification").

<sup>72</sup> With the increased use of RFID chips in credit cards by retailers that will reduce credit card fraud, it is anticipated that SSNs will become an increased target by criminal elements. Kamala D. Harris, Attorney General, California Dept. of Justice, California Data Breach Report at iv (2012-2015) (Feb. 2016); *available at*: <https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>? (last visited May 23, 2016) ("Cal. Data Breach Report").

<sup>73</sup> See NPRM ¶ 75.

breach notification laws.<sup>74</sup> The state security breach laws were designed to protect consumers from identity theft and financial harm, as well as provide customers with the ability to take measures to protect themselves in a timely manner.<sup>75</sup> The state laws focus on PII that is more sensitive or confidential by nature such as social security number, driver’s license number and financial account information. In fact, the vast majority of the state security breach laws define the core PII subject to notification as an individual’s first name or first initial and last name *in combination with any one or more of certain data elements* (when either the name or the data elements are *not encrypted*): social security number; driver’s license number or state issued identification card; and account number, credit card or debit account number in combination with any security code, access code or PIN. Many states have expanded on this definition to include additional sensitive or confidential information such as medical information and health insurance records.<sup>76</sup>

Although WISPA recognizes that the types of sensitive or confidential Personal Information have been expanded since the first security breach law was adopted by California in 2003, such expansion has been in response to emerging threats and rapid changes in technology, but still calibrated to ensure that any such notice had a measurable impact on consumer security.<sup>77</sup> For example, based on “evidence that criminal organizations were targeting online account credentials,”<sup>78</sup> California amended its security breach notification law in 2013 to also

---

<sup>74</sup> See National Council of State Legislators database, *available at*: <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (last visited May 27, 2016).

<sup>75</sup> “[V]ictims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person’s personal information is imperative.” Sec.1(c), S.B. 1386 (enacted Sept. 25, 2002) (codified at Cal. Civ. Code §§ 1798.29 and 1798.82).

<sup>76</sup> See, e.g., Cal. Civ. Code 1798.82(h)(1)(D) and (E).

<sup>77</sup> See Cal. Data Breach Report.

<sup>78</sup> *Id.* at 2 (emphasis added).

include a user name or email address, *in combination with a password or security question and answer that permits access to an online account.*<sup>79</sup>

The *NPRM* offers no explanation of why an expansion of the very broad types of customer proprietary information is necessary or what emerging threat the proposal is supposed to address, or how such notices of a breach that have little consequence of real consumer harm will protect customers or help law enforcement. Not all customer proprietary information will subject a consumer to identity theft or similar harms. Compelling a broadband provider to notify consumers when an IP address or stand-alone email address has been accessed (but not necessarily acquired, used or disclosed) does not protect consumers from identity theft, nor can the consumer take preventative measures such as credit blocks or credit monitoring of his or her credit reports. A breach of an IP address, or stand-alone user ID, or email address is quite benign when compared to a breach of a social security number, driver's license number or financial account information.

Third, the Commission's proposed rules and definitions do not differentiate between Sensitive PII ("Sensitive PII") and non-sensitive PII, a distinction that many federal agencies make.<sup>80</sup> The U.S. Department of Homeland Security has defined Sensitive PII as "personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."<sup>81</sup> The Commission's rules should therefore distinguish between PII and Sensitive PII and recognize the

---

<sup>79</sup> See SB 46 (codified at Cal. Civ. Code § 1798.82(h)(2)).

<sup>80</sup> For example, information on a business card is PII, but in most cases is not Sensitive PII because it is widely available information.

<sup>81</sup> See Department of Homeland Security, Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012 at 4 *available at*: [https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII\\_march\\_2012\\_webversion.pdf](https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf) (last visited May 27, 2016).

relative harms attendant to each category. Protection and breach of non-sensitive PII should not be subject to the same regulatory obligations as Sensitive PII.

Compounded with the absence of an “intent” trigger,<sup>82</sup> a “risk of harm” trigger<sup>83</sup> and/or a “good faith employee access” safe harbor,<sup>84</sup> customers would, under the Commission’s regime, receive notices that have no bearing on whether a breach is likely to subject the consumer to identity theft or other similar harms. The Commission’s proposal to require security breach notification to customers, to the Commission, and to law enforcement should therefore be limited only to sensitive or confidential personally identifiable information that is not encrypted, and not accessed under circumstances that carry no measureable risk of harm, such as a “[g]ood faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.”<sup>85</sup>

## **2. The Commission’s Proposed Definition Of “Customer” Is Overinclusive.**

The Commission proposes to define a “customer” as a *current or former*, paying or non-paying subscriber to broadband service; and 2) an *applicant* for such service.<sup>86</sup> Yet, under Section 222 and existing Commission rules, a “customer” is a person or entity to which a

---

<sup>82</sup> See, e.g., 47 CFR § 64.3022(e).

<sup>83</sup> See, e.g., Ind. Code §24-4.9 (Notice is required only “if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception ... identity theft, or fraud affecting the Indiana resident.” (§24-4.9-3-1(a)); Iowa Code §715C.1 *et seq.*

(“[N]otification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach.” (§715C.2(6)).

<sup>84</sup> See NPRM, ¶ 76 n. 149 (citing to Haw. Stat. Rev. § 487N-1).

<sup>85</sup> *Id.*; see also Ga. Code Ann. 10-1-911(2015).

<sup>86</sup> NPRM ¶ 31.

telecommunications company is *currently* providing service.<sup>87</sup> The Commission attempts to rationalize its proposal by stating that broadband providers “have the ability to retain and reuse applicant and former customer proprietary information long after the application process is over, or the former customer has discontinued its service.”<sup>88</sup> The Commission apparently does not appreciate that it is the nature of the economy for any type of business to maintain relationships with existing customers so that they can offer them new and improved products and services over time, and to re-engage former customers. Every day, window-shopping customers provide their phone numbers and email addresses to department stores and auto dealers with the expectation that they will receive a follow-up. Here, the Commission would treat broadband providers, and only broadband providers, differently by restricting their use of this information. Moreover, an applicant has the ability to review a broadband provider’s privacy policy on-line *before* it decides to furnish the provider with any covered information. For these reasons, the term “applicant” should not be included in the definition of “customer.”

With respect to former customers, there are already other federal and state laws that govern these business relationships,<sup>89</sup> and there is no need for the Commission to create redundant and confusing regulations here.

---

<sup>87</sup> *Id.* ¶ 32, citing 47 C.F.R. § 8.2(a); and 2015 *Open Internet Order*, 30 FCC Rcd at 5682-86, ¶¶ 187-93.

<sup>88</sup> *NPRM* ¶ 32.

<sup>89</sup> *See, e.g.*, FCC Do Not Call regulations under TCPA that restrict the ability of a business to contact a customer after a purchase, transaction, inquiry or application. 47 U.S.C. § 64.1200(f)(5) (“The term *established business relationship* for purposes of telephone solicitations means a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a residential subscriber with or without an exchange of consideration, on the basis of the subscriber’s purchase or transaction with the entity within the eighteen (18) months immediately preceding the date of the telephone call or on the basis of the subscriber’s inquiry or application regarding products or services offered by the entity within the three months immediately preceding the date of the call, which relationship has not been previously terminated by either party”).

#### **E. The Commission Should Not Expand The Scope Of Its CPNI Rules For Voice.**

The *NPRM* also opens the door to vastly expanding the scope of the existing CPNI rules that apply to voice providers.<sup>90</sup> Here again, the Commission suggests the wrong approach, one that would increase compliance burdens by requiring providers to spend an inordinate amount of time and undetermined cost to adapt their existing policies and procedures. While some WISPA members offer interconnected VoIP, many have elected not to do so because even the existing regulatory obligations for Universal Service Fund contributions and reporting and CPNI compliance are deemed to be too onerous – it simply is not worth it for small providers to hire accountants, lawyers and consultants to help them understand and comply with USF, TRS, CPNI, outage reporting and a host of additional alphabet soup regulations. For those that have determined that the benefits of offering interconnected VoIP outweigh these costs, adding new privacy rules for their voice service may tip the scales in the opposite direction. It would be the epitome of irony and contrary to the public interest if increased CPNI and privacy regulations forced voice providers to discontinue that service.

Consistent with the Industry Framework, “[i]n no event should the prescriptive outdated CPNI rules designated for legacy voice services apply to broadband services.”<sup>91</sup> Rather, in order to cover all types of broadband providers as well as any future technologies, the CPNI rules should set forth principles rather than prescriptive rules dictating the methods by which privacy policies must be communicated and the means by which it must be protected, retained and divulged in the case of a security breach. The Commission should adopt “a common set of flexible policies that allow providers to keep up with their customers’ expectations and evolving

---

<sup>90</sup> See *NPRM* ¶ 27.

<sup>91</sup> Industry Framework.

technology should apply to both types [voice and broadband] of service.”<sup>92</sup> It should not expand the scope of the voice rules to impose new requirements on existing voice providers, but should instead amend those rules only as necessary to meet the flexible Industry Framework approach.

**III. SMALL PROVIDERS SHOULD BE AFFORDED ADDITIONAL TIME TO COMPLY WITH ANY NEW RULES THE COMMISSION ADOPTS AND SHOULD BE EXEMPT FROM CERTAIN OTHER OBLIGATIONS.**

**A. Small Businesses Lack The Resources To Comply With A Prescriptive And Detailed Regulatory Scheme.**

Whether it adopts the Industry Proposal, its own prescriptive and demanding regulatory regime or some other construct, the Commission must acknowledge and address the substantial increase in costs and compliance burdens that small broadband providers will face. Existing privacy policies may need to be revised to change “opt-in” and “opt-out” categories, with the assistance of legal counsel. Employees will need to be retrained, at the expense of lawyers, accountants or consultants. Someone will have to learn how to be a compliance officer, or have to hire a privacy professional to serve in that capacity. And someone will have to know when a data breach occurs, who to notify and when.

All of these new obligations would have two things in common: they take time and cost money. For small providers, the costs of compliance are no lower, and, in fact, probably higher, than they are for large companies. For example, large companies with in-house lawyers and compliance officers can rely on those existing resources to re-write privacy policies, but small providers do not have in-house lawyers or regulatory departments and must hire outside counsel to advise on the new rules, draft new privacy policies, and conduct training.<sup>93</sup> Companies either will need to draft training manuals or re-write them, again requiring the service of lawyers expert

---

<sup>92</sup> *Id.*

<sup>93</sup> See WISPA PRA Comments at 4-5; Comments of the American Cable Association, GN Docket No. 14-28 (filed July 20, 2015).

in privacy law. In the event reporting to the Commission is required, small broadband providers – which may not have ever been required to file annual CPNI certifications – will need sufficient time to incorporate practices that will make the certifications accurate and complete.

Small providers, especially those with a handful of employees that serve a few hundred customers, cannot be expected to simply tackle these new obligations as a part of their jobs, or find the money to pay for the expertise and documentation that would be required. These additional compliance costs cannot be absorbed by small businesses and will likely be passed on to consumers in the form of higher prices. Of critical importance, the Commission provides absolutely no economic analysis to document support for its prescriptive plan, but it is easy to imagine that those costs will be extremely burdensome. Although in the *1998 CPNI Order* the Commission concluded that different CPNI rules were not necessary for small or rural carriers,<sup>94</sup> the rules proposed in the *NPRM* would be far more expansive and would create significantly more burdensome requirements.<sup>95</sup>

#### **B. Small Businesses Should Have Two Years To Comply With The New Rules.**

As a threshold matter, WISPA recommends that a “small provider” be defined much more broadly than the 5,000 subscriber limit the Commission suggests in light of the significant additional burdens proposed rules would require.<sup>96</sup> In the *2015 Open Internet Order*, the Commission defined small businesses for the purposes of the transparency exemption, as providers “with 100,000 or fewer broadband [connections], as per their most recent Form 477,

---

<sup>94</sup> See, e.g., *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8196 (1998) (“*1998 CPNI Order*”).

<sup>95</sup> Also, in the *1998 CPNI Order*, the Commission noted that carriers could seek a waiver of the CPNI rules if they could show that the rules would be unduly burdensome. See *1998 CPNI Order*, at 8196. Because the substantial burdens here are obvious, deferral of compliance time and exemptions for a class of providers is a better option, and will save scarce administrative resources and time it would take to review and process waivers.

<sup>96</sup> See *NPRM* ¶ 151.

aggregated over all of the providers' affiliates."<sup>97</sup> Recently, the House of Representatives unanimously passed the Small Business Broadband Deployment Act, defining small businesses as "any provider of broadband Internet access service that has not more than 250,000 subscribers."<sup>98</sup> Although a 250,000 limit can accommodate all of WISPA's members at this time, WISPA does not oppose a higher number such as 500,000 subscribers, which would be consistent with the definition used by the Small Business Administration for small telecommunications carriers – non-dominant providers with 1,500 or fewer employees or carriers with 500,000 or fewer subscribers.<sup>99</sup> Regardless of what new rules the Commission may adopt, and especially if the Commission adopts rules along the lines of its proposals, it must afford small providers additional time to comply with the new rules.<sup>100</sup>

At a minimum, small providers should be given up to two years after the effective date of any rules to meet any applicable new regulatory requirements. This additional time will enable small providers to assess their obligations, budget for lawyers, consultants, train personnel, and establish internal systems to ensure compliance. In general, deferred compliance approach will spread out the costs of compliance so that small providers are better able to manage the expenses and reduce the regulatory risk. Small providers also may be able to adopt models developed by larger providers that are required to meet an earlier compliance date. Overall, affording small providers additional time will help meet the Commission's goal of greater compliance, and

---

<sup>97</sup> *2015 Open Internet Order; Protecting and Promoting the Open Internet*, Report and Order, GN Docket No. 14-28 (CGB, Dec. 15, 2015) ("*Small Provider Extension Order*") (Consumer and Governmental Affairs Bureau extends the temporary exemption for small providers from the *2015 Open Internet Order* enhanced transparency rules until December 15, 2016).

<sup>98</sup> H.R. 4596, 114<sup>TH</sup> Cong. (2016). The "Small Business Broadband Deployment Act" passed in the House of Representatives on March 16, 2016.

<sup>99</sup> See E911 Stay Order, *supra* note 6 (citing to 15 U.S.C. § 632; 13 C.F.R. § 121.201).

<sup>100</sup> WISPA does not oppose a higher ceiling such as 500,000 subscribers, which would be consistent with the definition used by the SBA for the "Tier III" wireless classification as a small business size standard. See E911 Stay Order, *supra* note 6.

decrease the degree of enforcement for violations of rules that small providers cannot be prepared to meet. Stated another way, the Commission should not be creating an enforcement regime, but rather a set of flexible rules with which all providers, large and small, can reasonably comply.

It is common practice for the Commission to extend compliance periods for small businesses. In adopting the *2015 Open Internet Order*, the Commission granted small providers a short-term exemption from enhanced transparency rules.<sup>101</sup> In the *2007 CPNI Order*,<sup>102</sup> small providers were given a six-month extension to comply with new authentication rules. Other examples of small business exemptions and relief also can be found in the broadcast and MVPD equal opportunity requirements;<sup>103</sup> the 1992 Cable Act rate reductions<sup>104</sup> and abbreviated Cost of Service filings;<sup>105</sup> Commercial Advertisement Loudness Mitigation Act waiver request process;<sup>106</sup> the Twenty-first Century Communications and Video Accessibility Act implementation requirements;<sup>107</sup> and the Hearing Aid Compatibility Act *de minimis* exception

---

<sup>101</sup> *2015 Open Internet Order; Small Provider Extension Order*.

<sup>102</sup> *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6980 (2007) (*2007 CPNI Order*).

<sup>103</sup> See 47 C.F.R. § 73.2080(c)(2); see also *Review of the Commission's Broadcast and Equal Opportunity Rules and Policies*, Second Report and Order and Third Notice of Proposed Rulemaking, 17 FCC Rcd 24018, 24069 (2002).

<sup>104</sup> See *Implementation of Sections of the Cable Television Consumer Protection and Competition Act of 1992: Rate Regulation*, Second Order on Reconsideration, Fourth Report and Order, and Fifth Notice of Proposed Rulemaking, 9 FCC Rcd 4119, 4221-26 (1994).

<sup>105</sup> See *Implementation of Sections of the Cable Television Consumer Protection and Competition Act of 1992: Rate Regulation*, Report and Order and Further Notice of Proposed Rulemaking, 9 FCC Rcd 4527, 4671 (1994).

<sup>106</sup> See *Implementation of Commercial Advertisement Loudness Mitigation (CALM) Act*, MB Docket No. 11-93, Report and Order, FCC 11-182, 26 FCC Rcd 17222, 17244-45, 17253-54 (2011) ("*CALM Act Report and Order*"); see also 47 C.F.R. §§ 73.682(e)(3)(iii) and 76.607(a)(3)(iii).

<sup>107</sup> See *Accessibility of User Interfaces, and Video Programming Guides and Menus*, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 17330, 17334, 17401-2 (2013) (For purposes of the CVAA, mid-sized and smaller MVPDs are defined as: (1) MVPD operators with 400,000 or fewer subscribers (*i.e.*, MVPD operators other than the top 14), and (2) MVPD systems with 20,000 or fewer subscribers that are not affiliated with an operator serving more than 10 percent of all MVPD subscribers); Pub. L. No. 111-260, 124 Stat. 2751 (2010) (as codified in various sections of the Act). See also Amendment of the Twenty-first Century Communications and Video Accessibility Act, Pub. L. No. 111-265, 124 Stat. 2795 (2010) (making technical corrections to the CVAA).

for small businesses.<sup>108</sup> These examples often illustrate the Commission’s acknowledgement that small businesses may need more time to comply with new requirements and should be exempt from certain rules.<sup>109</sup>

Further, the FTC has taken business size into account when adopting privacy recommendations. In its 2012 Report, the FTC established a framework for consumer privacy and exempted small businesses from its framework for non-sensitive consumer data.<sup>110</sup> Because the proposals in the *NPRM* would impose significantly greater burdens than either CPNI rules or non-sensitive consumer data rules, a longer compliance period is warranted so that small providers can budget and plan for activities such as rewriting privacy policies, revamping security and data retention practices and hiring new personnel.

A two-year compliance deferral will also give the Commission and the Office of Management and Budget (“OMB”) an opportunity to more accurately assess and determine compliance burdens applicable to the specific information collections ultimately adopted. As the Commission discovered in its Paperwork Reduction Act proceeding for the enhanced disclosure rules adopted in the *2015 Open Internet Order*, undertaking an analysis to accurately estimate compliance burdens can take a substantial amount of time. In fact, more than 15 months after the enhanced disclosure rules are adopted, those rules are not effective because broadband providers questioned the Commission’s burden estimates and OMB has not approved the rules. Here, where the potential privacy protection burdens, especially for small providers, could extend far beyond the burdens estimate for the enhanced disclosure rules, the need for public

---

<sup>108</sup> See 47 CFR § 20.19(e). Manufacturers or service providers that offer two or fewer digital wireless handsets in an air interface in the United States are exempt from the hearing-aid compatibility requirements in connection with that air interface, except for the reporting requirements. *Id.*

<sup>109</sup> See also WISPA Open Internet Comments at 9.

<sup>110</sup> See FTC 2012 Privacy Report at 15-16. The FTC “acknowledge[d] the need for flexibility for businesses that collect limited amounts of non-sensitive information” and that “some business practices create fewer potential risks to consumer information.” *Id.*

input and informed decision-making is even more important. That process can run concurrently with the two-year deferral period WISPA recommends.

### **C. Small Providers Should Be Exempt From Onerous Notice And Data Security Obligations.**

In addition to a two-year compliance deferral, and if the Commission adopts rules similar to those proposed in the *NPRM*, WISPA urges the Commission to adopt specific exemptions to certain of those rules. *First*, in response to the Commission’s request for comment “on ways to minimize the burden of our proposed customer choice framework” on small providers,<sup>111</sup> small providers should be permitted to grandfather existing customer approvals for the use and disclosure of proprietary information. Small providers should not be compelled to obtain new consents, whether implied or explicit, from its customers. The time and expense to accomplish that task, coupled with the great potential for customer confusion, would not benefit the provider, which has a legal obligation to honor the consent of the customer who already has an expectation of how its private information will be handled.

*Second*, if the Commission adopts proposed Section 64.7005, small providers should only be required to comply with the first sentence stating that “A BIAS provider must ensure the security, confidentiality, and integrity of all customer proprietary information the BIAS provider receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, or uses exceeding authorization.”<sup>112</sup> Small providers should not be subject to proposed subsections (1)-(5), which describe specific requirements that will be difficult, if not impossible, for them to meet. If the Commission adopts proposed Section 64.7005(b), a new subsection should be added to ensure that, together with the “nature and scope” of the provider’s

---

<sup>111</sup> *NPRM* ¶ 151.

<sup>112</sup> *Id.* ¶ 109-10.

activities and the “sensitivity” of the information held by the provider, the Commission takes into account the provider’s size in determining whether data security measures are “reasonably implement[ed].”

*Third*, if the Commission adopts proposed Section 64.7006, small businesses should not be subject to the same notification deadlines that it otherwise would apply to larger providers. Instead, small providers should be required to provide notice of data breaches as soon as practicable under the circumstances, again taking into account the size of the provider and the resources it has available to it to detect data breaches. The proposed deadlines would require notification to Federal law enforcement and customers much more quickly than nearly all state laws require such that it may be difficult for even larger providers to comply with the Commission’s proposals.<sup>113</sup>

The small business relief urged in this Section also would be consistent with the RFA. Section 603 of the RFA requires the Commission to prepare and make available for public comment an initial regulatory flexibility analysis (“IRFA”) that describes the significant economic impact of the proposed rules on small entities subject to those proposed rules.<sup>114</sup> An IRFA must include “a description of the projected reporting, recordkeeping and other compliance requirements of the proposed rules, including an estimate of the classes of small entities which will be subject to the requirement . . . .”<sup>115</sup> An IRFA “*shall* also contain a description of any significant alternatives . . . which accomplish the stated objectives of

---

<sup>113</sup> For example, Ohio, Vermont and Wisconsin have 45 day notice windows. *See, e.g.*, Ohio Rev. Code Ann. §1349.19; Vt. Stat. Ann. Tit. 9, §2430, *et seq.*; Wis. Stat. §134.98.

<sup>114</sup> *See* 5 U.S.C. § 603(a).

<sup>115</sup> *Id.* at § 603(b)(4).

applicable statutes and which minimize any significant economic impact of the proposed rule on small entities.”<sup>116</sup> The required discussion of these alternatives includes:

- (1) the establishment of *differing compliance or reporting requirements or timetables* that take into account the resources available to small entities;
- (2) the clarification, consolidation, or *simplification of compliance and reporting requirements* under the rule for small entities;
- (3) the use of performance rather than design standards; and
- (4) *an exemption from coverage of the rule, or any part thereof, for such small entities.*<sup>117</sup>

The Final Regulatory Flexibility Analysis must, among other things, provide “a *description of the steps the agency has taken to minimize the significant economic impact on small entities* consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.”<sup>118</sup>

The Commission thus has legal obligations to consider alternatives, specifically including “differing compliance or reporting requirements or timetables” and exemption from certain rules. Although the Commission resorted to asking for comment on the impact its proposed rules would have on small providers, the Commission cannot avoid considering WISPA’s specific proposals in the record of this proceeding. WISPA urges adoption of the two-year compliance deferral and the exemptions described above.

---

<sup>116</sup> *Id.* at § 603(c) (emphasis added).

<sup>117</sup> *Id.* (emphases added). WISPA notes that the IRFA in this proceeding makes no mention of the thousands of fixed broadband providers that rely on *unlicensed* spectrum to provide service to the public. The IRFA recites various licensed and “lightly licensed” spectrum bands, but does not offer any analysis of the WISP industry that serves 3,000,000 people. Although WISPA explained this same IRFA defect in connection with the proceeding leading to adoption of the *2015 Open Internet Order*, the Commission continues to shirk its legal responsibilities. *See* WISPA IRFA Comments.

<sup>118</sup> 5 U.S.C. § 604(a)(6) (emphasis added).

#### **IV. THE COMMISSION SHOULD ADOPT A CLEAR AND STREAMLINED ENFORCEMENT PROCESS.**

The Commission asks if the “current informal complaint process for alleged violations of the Communications Act is sufficient to address customer concerns or complaints with respect to the collection, use, and disclosure of customer information covered by [the Commission’s] proposed rules.”<sup>119</sup> The Commission also seeks comment on whether the informal complaint process is adequate.<sup>120</sup>

WISPA hereby provides a number of specific recommendations regarding the complaint process.<sup>121</sup> First, arbitration and informal complaints should be the only methods by which customers can seek resolution of their disputes. Customers should not be permitted to file complaints or class action lawsuits in civil court that will cripple small providers, regardless of the merits of a case. Even the mere possibility of having to defend lawsuits will have a chilling effect on deployment, investment and competition because small providers will need to establish substantial cash reserves in the event they need to defend themselves.

Second, before any informal complaint is filed, the prospective complainant should be required to disclose the alleged basis of its potential complaint to its broadband provider. Both parties should be required to attempt to resolve the dispute in good faith for 30 days, and should be obligated to retain all correspondence. This gating process could lead to resolution of many disputes that would otherwise occupy Commission resources, and would allow the parties to consider private remedies.<sup>122</sup>

---

<sup>119</sup> *NPRM* ¶ 273.

<sup>120</sup> *Id.*

<sup>121</sup> *Id.*

<sup>122</sup> As an additional means to avoid Commission or civil litigation, broadband providers should be able to require arbitration as a means to resolve disputes. Arbitration clauses provide certainty to both customers and providers.

Third, all complaints should be filed within one year of the alleged rule violation. One year is a sufficient period of time for any party to register its complaint with the Commission. Any complaint filed against a small provider subject to deferred compliance with the rules should be immediately dismissed.

Fourth, unless it requires further information is required, the Commission should render a decision on any complaint within 60 days of the filing of the answer or any required supplemental information. A 60-day shot clock provides certainty and mitigates the risk from long and indefinite inquiries.

Fifth, the rules should expressly prevent the filing of complaints regarding notices where the broadband provider is using any “safe harbor” notice template that the Commission may authorize. The Commission should make clear that “safe harbor” practices are not complaint-worthy, which in turn should eliminate the filing of frivolous complaints, and should enforce its policies against the filing of frivolous complaints.<sup>123</sup> There is an inherent unfairness in penalizing broadband Internet access providers that make good faith efforts to comply with the rules only to fall short because of an honest misunderstanding of the Commission’s requirements.

Finally, if after review of the record the Commission imposes financial penalties on the provider, it should establish a clear schedule of forfeitures similar to the table in Section 1.80 of the Commission’s Rules. Broadband providers should know whether a potential violation is subject to an admonishment, a citation, a \$1 forfeiture or a \$1 million forfeiture. Moreover, any sanction must account for the size of the broadband provider. A small broadband provider will be less able to pay a large forfeiture than a large provider. Under Section 1.80, an inability to

---

<sup>123</sup> See, e.g., *Public Notice*, “Commission Taking Tough Measures Against Frivolous Pleadings,” 11 FCC Rcd 3030 (Feb. 9, 1996).

pay is considered to be a mitigating factor in the assessment of any forfeiture, and the same principles should apply with respect to any forfeiture schedule the Commission may wish to establish for violations of its privacy rules.

### **Conclusion**

The Commission lacks authority to create the prescriptive and expansive broadband privacy regime it describes in the *NPRM*. Even if it has that authority, it should exercise restraint in imposing it, and incorporate the FTC-based Industry Framework that promotes flexibility and innovation. In any event, small providers should have two years to comply with any new regulations, and should be exempt from specific data security and data breach notification requirements. WISPA also supports the development of a “safe harbor” for any required notices and streamlined complaint procedures that are focused on dispute resolution and not on extracting damages from those least likely to afford them.

Respectfully submitted,

### **WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION**

By: */s/ Alex Phillips, President*  
*/s/ Mark Radabaugh, FCC Committee Chair*  
*/s/ Jack Unger, Technical Consultant*

4417 13th Street #317  
St. Cloud, Florida 34769  
(866) 317-2851

Stephen E. Coran  
S. Jenell Trigg  
Deborah J. Salons  
Lerman Senter PLLC  
2001 L Street, N.W., Suite 400  
Washington, DC 20036  
(202) 429-8970  
*Counsel to the Wireless Internet Service Providers Association*

May 27, 2016