

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, DC 20554**

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

**COMMENTS**



Matthew M. Polka  
President and Chief Executive Officer  
American Cable Association  
Seven Parkway Center, Suite 755  
Pittsburgh, PA 15220  
(412) 922-8300

Thomas Cohen  
John J. Heitmann  
Jameson J. Dempsey  
Kelley Drye & Warren LLP  
3050 K Street, NW  
Washington, DC 20007  
(202) 342-8518

Ross J. Lieberman  
Senior Vice President of Government Affairs  
American Cable Association  
2415 39th Place, NW  
Washington, DC 20007  
(202) 494-5661

May 27 , 2016

## **EXECUTIVE SUMMARY**

In this proceeding, the Commission proposes a set of privacy and data security rules that, if adopted, would be one of the most sweeping, complex, and burdensome in the United States. American Cable Association (ACA) members—750 small and medium-sized providers of voice telephony, cable video, and broadband Internet access service (BIAS)—take seriously their obligation to protect the privacy and security of their subscribers’ personal information, and to that end have implemented reasonable controls to meet their customers’ expectations and the requirements of federal and state privacy laws and rules. However, ACA and its members are concerned that the Commission discounts these controls and does not fully appreciate the tremendous costs and burdens that the Commission’s proposed rules would impose on small BIAS providers. We submit these comments to challenge the Commission’s authority to impose its proposed rules, to describe the burdens that the new rules would impose, and to propose alternatives that would ease the burdens placed on small providers while still achieving the Commission’s goals of transparency, consumer choice, data security, and data breach notification.

The Commission does not have authority to adopt its proposed BIAS privacy and data security rules. As ACA and others have argued before in the still-pending appeal before the D.C. Circuit, the Commission lacks authority to classify BIAS as a Title II common carrier service. Consequently, the Commission cannot impose privacy and data security rules under Section 222 of Title II on BIAS providers. Even if the court were to rule that the Commission could subject BIAS to Title II regulation, the statutory language and legislative history of Section 222 demonstrate that that provision applies to voice services, not BIAS. Further, as ACA and others have argued, even if the Commission had authority under Section 222 to impose privacy and data

security rules on BIAS, Section 222(a) does not provide the Commission with blanket authority to regulate the recently invented category of “customer proprietary information.” Congress purposely limited Section 222 to the narrow category of CPNI, and it would contravene congressional intent to expand the scope of Section 222 to all “customer proprietary information.” Similarly, the Commission lacks authority under Sections 201 and 202 of the Communications Act to implement its rules. Sections 201 and 202 of the Communications Act neither impose nor authorize the Commission to impose privacy and data security rules. Had Congress intended for these provisions to reach the privacy and data security practices of common carriers, it would not have enacted the “comprehensive” privacy regime set forth in Section 222. The other statutory provisions the Commission cites for its authority—including Section 631 of the Cable Act, Section 705 of the Communications Act, and Section 706 of the 1996 Telecommunications Act—similarly do not provide the Commission with the requisite authority to enact the proposed rules.

Moreover, the Commission’s proposals would impose tremendous burdens on small providers. These burdens include, but are not limited to, attorney and consultant costs associated with regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits; development and implementation costs associated with data security controls, website policies, and customer approval tracking systems; personnel costs associated with dedicated privacy and data security staff; costs associated with all aspects of providing required notices and follow-up; third-party costs associated with modifying contracts and ensuring compliance for call centers, billing software, and others that interface with customer proprietary information; and opportunity costs associated with diverting scarce resources from innovation and infrastructure deployment to regulatory compliance.

Rather than impose the unnecessary and heavy-handed rules proposed in the NPRM, the Commission should adopt rules consistent with the successful “unfair or deceptive acts or practices” standard of Section 5 of the FTC Act and as set forth in the Industry Proposal submitted to the Commission in advance of this proceeding. Like the Commission’s proposal, the Industry Proposal focuses on the core values of transparency, consumer choice, data security, and data breach notification. Unlike the Commission’s proposal, however, the Industry Proposal will promote consistency across the entire Internet ecosystem, flexibility consistent with provider needs and consumer expectations, and innovation to drive the virtuous circle. Further, it will do so without overburdening small providers with micro-managerial, one-size-fits-all regulations. Moreover, it would comport with consumers’ expectations that their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used regardless of which entity in the Internet ecosystem uses that data.

Alternatively, if the Commission pursues a prescriptive, *ex ante* privacy and data security framework as proposed in the NPRM, it should adopt the following targeted exemptions for small providers consistent with similar privacy regimes:

- Exempt small providers from the specific “minimum” data security requirements that it sets forth in proposed Section 64.7005(a) and add “the size of the BIAS provider” to the factors that the Commission must consider when assessing the reasonableness of a BIAS provider’s security program;
- Exempt small providers from the more onerous elements of its customer approval framework by grandfathering existing customer consents and exempting small providers from the requirement to obtain additional approval where they do not share sensitive personal information with third parties for marketing purposes;
- Exempt small providers from several elements of the Commission’s proposed data breach notification rule (as applied to both voice services and BIAS) by exempting small providers from the specific notification deadlines in favor of an “as soon as reasonably practicable” standard; and

- Exempt small providers from any customer dashboard requirements that it adopts pursuant to its notice and choice regulations.

Not only are these exemptions consistent with existing privacy regimes, they also would directly address and reduce the burdens that the proposed privacy rules would have on small providers. Further, regardless of the exemptions that the FCC adopts, it should extend the deadlines for small providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline, with a subsequent rulemaking to determine whether to further extend the deadline and/or establish additional exemptions.

Further, if the Commission does not adopt an “unfair or deceptive acts or practices” framework consistent with the Industry Proposal, it should rationalize and streamline its proposed rules to ensure that the rules are not too burdensome for small BIAS providers. Specifically, the Commission should develop, with industry and other stakeholders, standardized notices that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and developers. Moreover, the Commission should streamline its proposed customer approval requirements to better align with consumer expectations and avoid disrupting existing customer relationships. Additionally, the Commission should adopt a general data security standard and work with industry to establish and update best practices rather than imposing prescriptive data security rules. Finally, the Commission should tailor any data breach notification requirements to ease burdens on BIAS providers, including by adopting flexible deadlines for breach notification, limiting notifications to situations where consumer harm is reasonably likely, creating a one-stop-shop for breach reporting, and preempting state breach notification laws.

Finally, while ACA supports the concept of streamlining privacy and data security regulations for providers of multiple services, it is concerned that, in practice, a single set of rules across different statutory regimes could increase the burdens on small providers, heighten consumer confusion, and contravene statutory language and legislative intent. For this reason, the Commission should only harmonize its rules *within* Section 222 and should not use this rulemaking proceeding to impose new and unfamiliar rules on cable video service pursuant to Section 631.

## TABLE OF CONTENTS

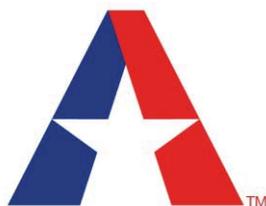
I.	INTRODUCTION AND OVERVIEW .....	2
II.	ACA MEMBERS TAKE PRIVACY AND DATA SECURITY OBLIGATIONS SERIOUSLY.....	4
III.	THE COMMISSION LACKS AUTHORITY TO IMPOSE ITS PROPOSED PRIVACY AND DATA SECURITY RULES.....	9
A.	The FCC lacks authority under Title II to impose privacy and data security rules on BIAS providers.....	10
B.	The FCC does not have authority under Section 222 to impose privacy and data security rules on BIAS .....	10
C.	The FCC does not have authority under Sections 201 and 202 to impose its proposed privacy and data security rules .....	15
D.	The FCC does not have authority under Section 631 to extend or impose additional privacy requirements on BIAS provided by cable operators .....	18
E.	The FCC does not have authority under Section 706 to impose privacy rules, which hurt, not help, the virtuous circle by hindering innovation and partnerships and slowing investment and deployment.....	19
IV.	EVEN IF THE COMMISSION DOES HAVE AUTHORITY TO IMPOSE RULES FOR BIAS CUSTOMER PROPRIETARY INFORMATION, THE PROPOSED RULES WOULD IMPOSE SIGNIFICANT AND DISPROPORTIONATE COSTS AND BURDENS ON SMALL PROVIDERS .....	22
A.	The proposed data security requirements are unduly prescriptive and impractical .....	23
B.	The proposed customer approval requirements are complex, restrictive, and impractical.....	29
C.	The proposed data breach notification requirements are unnecessarily prescriptive.....	34
D.	The proposed notice requirements are burdensome and unnecessary.....	37
V.	THE COMMISSION SHOULD ADOPT A PRIVACY AND DATA SECURITY FRAMEWORK CONSISTENT WITH THE FTC’S SUCCESSFUL “UNFAIR OR DECEPTIVE ACTS OR PRACTICES” APPROACH AS SET FORTH IN THE INDUSTRY PROPOSAL.....	39
VI.	IF THE FCC ADOPTS A PRESCRIPTIVE, <i>EX ANTE</i> FRAMEWORK, IT SHOULD ADOPT TAILORED EXEMPTIONS FROM SPECIFIC RULES, EXTEND IMPLEMENTATION TIMEFRAMES FOR SMALL PROVIDERS, AND STREAMLINE AND RATIONALIZE ITS SECTION 222 RULES .....	42

A.	The Commission should adopt targeted exemptions to its proposed BIAS privacy and data security rules.....	43
B.	The Commission should extend the compliance deadlines for small providers by at least one year, with a subsequent rulemaking to determine whether to further extend the deadline and/or establish additional exemptions.....	46
C.	The Commission should rationalize and streamline its proposed BIAS privacy and data security rules .....	49
VII.	THE COMMISSION SHOULD HARMONIZE ITS PRIVACY AND DATA SECURITY REQUIREMENTS FOR VOICE AND BIAS, BUT SHOULD NOT HARMONIZE ITS CABLE PRIVACY RULES .....	57
VIII.	CONCLUSION.....	59

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, DC 20554**

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

**COMMENTS**



**AMERICAN CABLE  
ASSOCIATION**

The American Cable Association (ACA) hereby submits its comments in response to the Notice of Proposed Rulemaking adopted by the Federal Communications Commission (Commission) in the above-referenced dockets.<sup>1</sup> ACA represents approximately 750 small and medium-sized cable operators, incumbent telephone companies, municipal utilities, and other local providers. In aggregate, these providers pass nearly 19 million homes and serve nearly seven million homes. The vast majority of ACA members have fewer than 5,000 subscribers, and half have fewer than 1,000 subscribers. These smaller providers are characterized by a number of attributes that are relevant for the Commission to consider as it deliberates on

---

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

adopting new and modified privacy and data security regulations for broadband Internet access service (BIAS) providers and whether to amend existing privacy and data security rules for voice and cable services.

ACA focuses its initial comments on the *Broadband Privacy NPRM* on a discrete set of issues of most importance to smaller providers. ACA anticipates entering additional commentary in the record on other issues raised in the *Broadband Privacy NPRM* and addressed by other commenters in its reply comments and *ex parte* submissions.

## **I. INTRODUCTION AND OVERVIEW**

In this NPRM, the Commission proposes a set of privacy and data security rules that, if adopted, would be one of the most sweeping, complex, and burdensome in the United States. This proposal is not occasioned by any major market failure, such as repeated and serious data breaches pertaining to the services that would be subject to these regulations. Not only does the Commission propose specific rules under Section 222 of the Communications Act of 1934, as amended (the Act),<sup>2</sup> for providers of BIAS, it also seeks comment on whether and how to “harmonize” its existing privacy rules for voice, cable, and satellite services to match—to the extent possible—its new proposals. ACA members are concerned that the Commission discounts small BIAS providers’ excellent track record in protecting the confidentiality of their customers’ information, the existing robust controls they utilize to protect their customers’ privacy, and the tremendous costs and burdens that the Commission’s proposed rules would impose on these providers. ACA submits these comments to describe the burdens that the new rules would impose and, should the Commission proceed with its proposal, to propose

---

<sup>2</sup> See 47 U.S.C. § 222.

alternatives that would ease the burden on small providers while still achieving the Commission's goals of transparency, consumer choice, data security, and data breach notification.

ACA's comments proceed as follows: Section II demonstrates that ACA members take privacy and data security seriously and describes ACA members' current privacy and data security compliance efforts pursuant to federal and state law. Section III argues that the Commission lacks statutory authority to impose privacy and data security rules for BIAS providers, at least to the degree that it proposes to do so here. Section IV provides evidence showing that the Commission's proposed privacy and data security rules would be extremely burdensome for small providers, which lack the resources of large providers. Section V proposes that the FCC adopt a flexible privacy and data security regime built on an "unfair or deceptive acts or practices" framework, which will create a level playing field for the Internet ecosystem while protecting consumers and promoting innovative products and services. Section VI submits that if the FCC rejects the proposed "unfair or deceptive acts or practices" framework in favor of a prescriptive *ex ante* regime, it should adopt targeted small provider exemptions, establish at least a one-year implementation extension (with a subsequent rulemaking to decide whether and how to further extend the deadline or adopt additional exemptions), and streamline and rationalize its rules to ease compliance burdens. Section VII argues that the Commission should harmonize its Section 222 rules, but should not harmonize its cable service privacy rules with existing or proposed rules for voice service and BIAS. Section VIII provides concluding remarks.

## II. ACA MEMBERS TAKE PRIVACY AND DATA SECURITY OBLIGATIONS SERIOUSLY

ACA members take their obligations to protect the privacy and security of their customers' data seriously and devote considerable resources to informing their customers about their privacy policies, providing them with choices about how customer data is used, and protecting their networks and their customers from data security threats and breaches.

As providers of voice, cable service, broadband, and various non-common-carrier services—e.g., home security, PC support, e-mail, and data center services—ACA members and their agents, affiliates, and contractors are subject to a thicket of federal and state privacy and data security obligations. ACA members that provide voice services—whether traditional circuit-switched voice or interconnected voice over Internet Protocol (VoIP)—must comply with Section 222 of the Communications Act and its implementing rules.<sup>3</sup> ACA members that provide cable service must comply with Section 631 of the Cable Communications Policy Act of 1984 (the Cable Act).<sup>4</sup> ACA members that provide BIAS services must comply with the Commission's transparency rule (which requires disclosure of privacy policies), and since the *2015 Open Internet Order*, the Commission has argued that they must comply with Section 222 (notwithstanding ongoing challenges to the agency's authority to do so).<sup>5</sup> ACA members that

---

<sup>3</sup> See 47 U.S.C. § 222; 47 C.F.R. § 64.2001 *et seq.*

<sup>4</sup> See 47 U.S.C. § 551.

<sup>5</sup> See 47 C.F.R. § 8.3; *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, ¶¶ 164, 462-67 (rel. Mar. 12, 2015) (2015 Open Internet Order); *FCC Enforcement Advisory: Open Internet Privacy Standard—Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps To Protect Consumer Privacy*, Public Notice, DA 15-603 (EB May 20, 2015). See *infra* Section III.

provide non-common-carrier services must also comply with Section 5 of the Federal Trade Commission Act, which until recently applied to BIAS.<sup>6</sup> Further, ACA members are subject to the laws and rules of the states in which they operate, including a panoply of privacy and data security laws and rules (e.g., data breach notification laws).<sup>7</sup> In addition, to the extent that ACA members interact with institutions handling sensitive information such as banks, hospitals, and schools, they often must assume obligations—by statute, rule, or contract—to protect such information.

ACA members have taken reasonable steps to comply with the myriad privacy regulations to which they are subject. ACA members notify their subscribers of their privacy practices through welcome packages, annual notifications, and website privacy policies. ACA members also provide opportunities for customers to make choices about how service providers use or share their information. While ACA members generally do not use their customers' information for purposes requiring opt-in consent—often because they lack the incentive or resources to do so—ACA members provide customers with the opportunity to opt-out of specific uses and disclosures of customer information, to the extent required by law. ACA members also understand the importance of effective personnel training, as well as the need to ensure that agents and independent contractors—e.g., billing and customer services companies—protect the confidentiality of customer information.

ACA members recognize that trust is foundational to the customer-carrier relationship, and for that reason they employ reasonable physical, technical, and administrative data security

---

<sup>6</sup> See 15 U.S.C. § 45.

<sup>7</sup> See, e.g., *infra* at n.99-101 (citing various state data breach notification laws).

practices to protect against breaches of customer information. For example, ACA members have established robust authentication requirements, such as password protection for access to customer information or, for small-town providers, requiring customers to authenticate themselves in person with proper identification. In addition, ACA members take reasonable steps to comply with the recordkeeping and reporting obligations of the Commission's existing privacy and data security rules, including obligations to keep records of customer approval status and marketing campaigns, as well as annual certification obligations.

ACA members acting through ACA have also been active in the Commission's CSRIC Working Group IV proceeding to assist companies to implement workable voluntary cybersecurity measures for the communications sector that respect the unique challenges that small and medium-sized providers face.<sup>8</sup> In fact, in response to an FCC Public Notice seeking comment on the CSRIC recommendations, ACA, at the direction of its members, supported the recommendation for voluntary meetings of communications sector companies, subject to liability and other protections, to provide "the Commission and the public assurances that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise."<sup>9</sup> ACA members acting through ACA even advised the Commission that

---

<sup>8</sup> See Comments of the American Cable Association, *CSRIC IV Cybersecurity Risk Management and Assurance Recommendations*, PS Docket No. 15-68, (May 29, 2015) (hereinafter ACA CSRIC Voluntary Assurance Comments).

<sup>9</sup> *Id.* at 11, 13 (citing Communications Security, Reliability and Interoperability Council, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*, 4 (Mar. 2015), [https://transition.fcc.gov/pshs/advisory/csric4/CSRIC\\_IV\\_WG4\\_Final\\_Report\\_031815.pdf](https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf) (CSRIC IV Report)). ACA is disappointed that the Commission has moved away from addressing data security through the voluntary public-private partnership mechanisms set forth in the CSRIC IV Report, which were widely embraced both inside the Commission and in the

the ACA “stands ready to act as an intermediary” with respect to small and medium-sized companies. Similarly, ACA members directed ACA to take an active role in supporting the development of cybersecurity information sharing in a way that is accessible to and effectively and meaningfully benefits small and medium-sized companies, filing comments with the Department of Homeland Security regarding the Standards for Information Sharing and Analysis Organizations and successfully supporting passage of the Cybersecurity Act of 2015.<sup>10</sup>

ACA members have had an excellent track record in protecting the confidentiality of their customers’ information and complying with the privacy and data security laws and rules to which they are subject. This is true even though the sophistication and scope of ACA members’ privacy and data security practices necessarily varies depending on the size of each operator and the resources available to them. Eighty percent of ACA members serve fewer than 5,000

---

private sector. That comprehensive groundbreaking report was developed by more than 100 participants in only one year. More than a year has passed since that monumental task was completed, and the FCC has failed to implement the cooperative voluntary approach it lauded and has instead moved on to propose a far-reaching, burdensome set of prescriptive rules. *See also, e.g.*, Remarks of FCC Chairman Tom Wheeler, As Prepared For Delivery, RSA Conference, 8 (Apr. 21, 2015), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-333127A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-333127A1.pdf) (“When fully developed and properly implemented, I believe that CSRIC’s assurance model will provide much-needed accountability for network security, while avoiding top-down prescriptive regulation of industry practices. A cooperative and collaborative approach is the FCC’s preferred means of engagement.”); *id.* at 1 (“For more than a year, the Commission and key stakeholders have been working together to develop a strategy to enhance the security of our wired and wireless broadband networks. Last month we all agreed on that plan.”).

<sup>10</sup> Comments of the American Cable Association, *Notice of Public Meeting Regarding Standards for Information Sharing and Analysis Organizations*, Docket No. DHS-2015-0017, (November 9, 2015). This proceeding followed up on President Obama’s February 13, 2015, Executive Order entitled “Promoting Private Sector Cybersecurity Information Sharing.” Exec. Order No. 13691, 80 Fed. Reg. 9347 (Feb. 13, 2015) (Promoting Private Sector Cybersecurity Information Sharing Executive Order), available at <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

subscribers, and roughly fifty percent serve fewer than 1,000 subscribers. Further, margins and levels of free cash flow differ significantly among these member companies.<sup>11</sup> Most ACA members have few employees: half of ACA's members have ten or fewer employees,<sup>12</sup> with typically just only one or two engineers or individuals with technical expertise, and these employees perform many duties within their companies. Moreover, very few of these providers have in-house technical or compliance personnel with extensive expertise in privacy and data security compliance. Some are forced to outsource some of their security functions to outside vendors at a significant cost. To address regulatory compliance matters, they use personnel dedicated to operational and other activities and often must turn to outside consultants and counsel.

While ACA members have developed robust and effective privacy and data security procedures to protect the confidentiality of their customers' proprietary information, compliance with the existing privacy and data security rules still presents considerable burdens, particularly for those ACA members that provide multiple regulated services (e.g., voice, video, and broadband). Further, these privacy and data security costs do not exist in a vacuum—they are just one part of an increasingly complex web of legal and regulatory obligations with which providers must comply, including law enforcement, disabilities access, copyright, emergency alert service, universal service, and open Internet obligations, as well as a variety of state and local regulations. As explained below in Section IV, the Commission's proposed rules would

---

<sup>11</sup> See American Cable Association, *High and Increasing Video Programming Fees Threaten Broadband Deployment*, (Apr. 2015), <http://www.americancable.org/node/4728>.

<sup>12</sup> See American Cable Association, *Connecting Hometown America: How the Small Operators of ACA Are Having a Big Impact*, 13 (Mar. 2014), available at [http://www.americancable.org/files/140328%20ACA\\_Whitepaper\\_PDF%20\(FINAL\).pdf](http://www.americancable.org/files/140328%20ACA_Whitepaper_PDF%20(FINAL).pdf).

add another layer of complexity to the existing rules, with significant and unique burdens for small providers and without sufficient countervailing benefits for consumers.

Despite these resource challenges and compliance burdens, ACA members have an excellent track record in protecting the confidentiality of their customers' personal information. In fact, based on numerous interviews with ACA members, it appears that the most common complaint from customers about privacy and data security is that the existing rules—which require consumers to receive, read, and respond to multiple notices and approval forms based on each service—are too confusing and burdensome, with few, if any, complaints about the sufficiency of ACA members' practices.

### **III. THE COMMISSION LACKS AUTHORITY TO IMPOSE ITS PROPOSED PRIVACY AND DATA SECURITY RULES**

In the NPRM, the Commission argues that it has ample statutory authority to adopt its proposed rules pursuant to Section 222 of the Communications Act of 1934, as amended, as well as Sections 201, 202, and 705 of the Act, Section 631 of the Cable Act, and Section 706 of the Telecommunications Act of 1996 (the 1996 Act).<sup>13</sup> ACA respectfully submits that the Commission does not have authority to adopt its proposed BIAS privacy and data security rules under any of the statutory provisions on which it purports to rely, and even if it did, the scope of its authority is not broad enough to adopt all of the rules proposed in the NPRM. This section addresses each of the proposed sources of statutory authority in turn.

---

<sup>13</sup> See NPRM ¶¶ 294-309. See also 47 U.S.C. §§ 201, 202, 222, 551, 705, 1302.

**A. The FCC lacks authority under Title II to impose privacy and data security rules on BIAS providers**

As a preliminary matter, ACA reiterates its argument that the Commission lacks authority to impose Title II obligations on BIAS providers. The instant NPRM stems from the Commission's *2015 Open Internet Order*, in which the Commission improperly reclassified broadband Internet access service as a telecommunications service under Title II of the Communications Act. A number of parties, including ACA, have appealed the *2015 Open Internet Order* to the D.C. Circuit, and we incorporate here our arguments in the appeal by reference.<sup>14</sup> If the D.C. Circuit vacates the Commission's reclassification of broadband Internet access service, the Commission will not have authority under Title II—including Sections 201, 202, 222, and 705—to impose privacy and data security rules on BIAS.

**B. The FCC does not have authority under Section 222 to impose privacy and data security rules on BIAS**

Even if the D.C. Circuit upholds the Commission's authority to classify BIAS as a Title II service, the Commission lacks authority to impose privacy and data security rules on BIAS under Section 222. The statutory language and congressional intent of Section 222 confirm that the provision applies to telephone *voice* services, not BIAS. Moreover, even if Section 222 could be read to apply to BIAS, it does not provide the Commission with authority to regulate non-CPNI personally identifiable information.

---

<sup>14</sup> See Joint Brief for Petitioners USTelecom, NCTA, CTIA, ACA, WISPA, AT&T, and CenturyLink, *United States Telecom Ass'n v. FCC*, Case No. 15-1063 (July 30, 2015); Joint Reply Brief for Petitioners USTelecom, NCTA, CTIA, ACA, WISPA, AT&T, and CenturyLink, *United States Telecom Ass'n v. FCC*, Case No. 15-1063 (October 5, 2015).

**1. Section 222 does not provide the Commission with authority to regulate the privacy or data security practices of BIAS providers**

The Commission lacks authority under Section 222 to impose privacy or data security rules on BIAS providers, as evidenced by the statutory language of Section 222 and its legislative history.

The statutory language of Section 222 clearly focuses on the protection of information related to telephone service and not BIAS. Section 222 cabins key provisions with words such as “call,” “call location information,” and “telephone exchange service,” with no reference to broadband service.<sup>15</sup> Indeed, the only reference to the Internet in Section 222 relates to IP-enabled *voice* services, a category that was added to the statute in 2008.<sup>16</sup> The fact that Congress saw the need to add a specific provision dealing with IP-enabled services demonstrates that it did not intend Section 222 to apply to any other IP-enabled services, such as BIAS. The lack of an explicit reference to the Internet or broadband in Section 222 stands in stark contrast with Section 230 of the Act, which explicitly addresses Internet access services. Section 230, for its part, limits the liability of providers and users of “interactive computer services”—i.e., “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides *access to the Internet*”<sup>17</sup>—and applies to Internet content delivered over “packet switched networks,” as opposed to telephone exchange services. In short, Congress knows how

---

<sup>15</sup> See 47 U.S.C. § 222.

<sup>16</sup> See NET 911 Improvement Act of 2008, Pub. L. No. 110-283, § 301(1) (2008).

<sup>17</sup> 47 U.S.C. § 230(f)(2) (emphasis added).

to include the terms “Internet” and “broadband” when it intends for a provision to apply to Internet-related services (e.g., BIAS) and did not do so when it drafted Section 222.

Second, the legislative history of Section 222 demonstrates that Congress did not intend for that provision to apply to BIAS. As the Commission has recognized, Section 222 was drafted to protect certain information to which *telephone* providers had unique access, while at the same time promoting competition in the telephone services market.<sup>18</sup> The information that Section 222 protects—customer proprietary network information (CPNI)—includes information that is voice-service specific and made available to the customer’s carrier “solely by virtue of the carrier-customer relationship,” such as call detail records and billing information. Section 222 excludes public and non-sensitive information, such as subscriber list information and basic subscriber information (e.g., name, address, and telephone number).<sup>19</sup> The Internet ecosystem presents dramatically different circumstances. Specifically, unlike CPNI in the telephone context, “customer proprietary information,” as the Commission defines it, often is not uniquely available to BIAS providers. Indeed, when consumers use the Internet, their information necessarily is shared with numerous entities throughout the Internet ecosystem, including edge providers, advertisers, and countless intermediaries.<sup>20</sup> This fact alone demonstrates that

---

<sup>18</sup> See *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*, CC Docket Nos. 96-115, 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, ¶ 37 (rel. Feb. 26, 1998) (1998 CPNI Order).

<sup>19</sup> See 47 U.S.C. § 222(h)(1)(A).

<sup>20</sup> See generally, Peter Swire, et al., *Online Privacy and ISPs*, Working Paper, The Institute for Information Security & Privacy at Georgia Tech, (Feb. 11, 2016), <http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf>.

Congress did not intend Section 222 to apply to BIAS. Therefore, the Commission may not use Section 222 to promulgate its proposed BIAS privacy and data security rules.

**2. Section 222(a) does not provide the Commission with authority to regulate non-CPNI personally identifiable information**

Even if the FCC had authority to impose Section 222 on BIAS, the terms of Section 222 protect a class of information defined as CPNI and Section 222(a) does not provide authority to regulate the recently invented and much broader category of “customer proprietary information.”<sup>21</sup>

In the NPRM, the Commission once again improperly seeks to leverage Section 222(a) of the Communications Act to impose broad privacy and data security rules on “customer proprietary information,” a term that does not appear anywhere in the Communications Act but that the Commission apparently invented in its 2014 Notice of Apparent Liability against TerraCom and YourTel.<sup>22</sup> As ACA argued in an earlier challenge to the Commission’s authority under Section 222(a), the statutory language, structure, purpose, and legislative history of Section 222 make clear that CPNI is the only customer data that Section 222 protects, and that the Commission’s reading of Section 222(a) as establishing broad privacy and data security obligations cannot be squared with the clear and more specific provisions of Sections 222(b) and

---

<sup>21</sup> ACA’s use of the term “customer proprietary information” in these comments is solely for purposes of addressing the merits of the Commission’s proposals in the NPRM and is not intended to waive any of its legal challenges to the Commission’s authority to establish its authority or promulgate rules pursuant to Section 222, or to otherwise legitimate the term.

<sup>22</sup> See *TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture*, File No.: EB-TCD-13-00009175, Notice of Apparent Liability, 29 FCC Rcd 13325 (2014).

222(c) of the statute.<sup>23</sup> Rather than establish a separate category of protected “customer proprietary information,” the language of Section 222(a) sets forth a general duty to protect that takes its force and effect only through the specific provisions that follow detailing precisely the type of information to be protected and how it is to be protected.

Moreover, there are many instances in which Congress has drafted statutory provisions to protect the type of “personal information” or “personally identifiable information” at issue here,<sup>24</sup> but it used the term “proprietary information” in Section 222 to serve a different and more limited purpose—preventing incumbent carriers from leveraging CPNI already in their possession to control CPNI derived “in one market to perpetuate their dominance as they enter other service markets.”<sup>25</sup> The NPRM impermissibly ignores Congress’ choice of terminology, incorrectly conflating “proprietary information” as used in Section 222(a) with “personally identifiable information.”

---

<sup>23</sup> See Comments in Support of Petition for Partial Reconsideration of the American Cable Association, *Lifeline and Link Up Reform and Modernization, et al.*, WC Docket Nos. 11-42, 09-197, 10-90, (Oct. 8, 2015) (ACA Comments in Support of CTIA Petition). ACA incorporates in full here the arguments it made in its comments in support of CTIA’s Petition for Partial Reconsideration. To the extent that ACA’s arguments in those comments focused on data security obligations, ACA makes clear here that the Commission does not have authority under Section 222(a) to impose *any* of its proposed rules—privacy or data security—on non-CPNI “proprietary information.”

<sup>24</sup> Provisions in the Communications Act include Section 631, protecting the privacy of cable subscribers’ “personally identifiable information,” 47 U.S.C. § 551, and a similar provision, Section 338(i), protecting the privacy of satellite subscribers’ “personally identifiable information,” 47 U.S.C. § 338(i).

<sup>25</sup> *1998 CPNI Order* ¶ 37.

The Supreme Court has made clear that “[a]n agency has no power to ‘tailor’ legislation to bureaucratic policy goals”<sup>26</sup> by interpreting a statute to create a regulatory system “unrecognizable to the Congress that designed” it.<sup>27</sup> Because Congress purposely cabined Section 222 to CPNI, the FCC cannot now expand its interpretation of the statute to cover information that Congress clearly did not intend it to address.

Although the Commission may wish to protect the privacy and security of consumers’ personally identifiable information, Congress simply has not tasked the Commission with this particular mandate under Section 222. As such, even if the D.C. Circuit upholds reclassification of BIAS under Title II, the Commission does not have authority to impose privacy and data security rules on non-CPNI “customer proprietary information.”

**C. The FCC does not have authority under Sections 201 and 202 to impose its proposed privacy and data security rules**

While the NPRM primarily relies on Section 222 for its proposed rules, the Commission also asserts that Sections 201 and 202 of the Communications Act provide it with the requisite authority to adopt its proposed privacy and data security rules.<sup>28</sup> Sections 201 and 202 do not confer upon the Commission the authority claimed in the NPRM.

As ACA has argued, Section 201(b) neither imposes privacy or data security requirements nor gives the Commission authority to impose them.<sup>29</sup> Had Congress granted the

---

<sup>26</sup> *Util. Air Reg. Group v. EPA*, 134 S. Ct. 2427, 2445 (2014).

<sup>27</sup> *Id.* at 2444 (citing Prevention of Significant Deterioration and Title V Greenhouse Gas Tailoring Rule, 75 Fed. Reg. 31514, 31555 (June 3, 2010)).

<sup>28</sup> See NPRM ¶¶ 305-06.

<sup>29</sup> See ACA Comments in Support of CTIA Petition at 7-9. As we stated above, ACA incorporates here its earlier arguments challenging the Commission’s authority over data security

Commission authority under Section 201(b) broad enough to reach privacy and data security practices of common carriers, it would not have needed to enact subsequently the very detailed set of prescriptions over this same subject matter in Section 222. The fact that it did so alone suggests the Commission overreaches in attempting to broadly regulate customer privacy and data security under Section 201(b). Indeed, not only did Congress recognize that the Commission lacked authority under Section 201(b) over privacy and data security when it enacted Section 222 in 1996, it again confirmed this lack of broad authority when it later added “location” to the definition of CPNI, explaining that had it not done so, “there [would have been] no protection for a customer’s location information.”<sup>30</sup>

Section 202, similarly, cannot be read so broadly as to impose privacy and data security requirements on BIAS providers. Section 202 prohibits carriers from “mak[ing] any unjust or unreasonable discrimination”; “mak[ing] or giv[ing] any undue or unreasonable preference or advantage”; or “subject[ing] any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage.”<sup>31</sup> These provisions have nothing to do with privacy and data security obligations; indeed, we are unaware of a single instance in which the Commission has ever used Section 202 in a case involving alleged privacy or data security violations.

---

pursuant to Section 201(b). To the extent that those arguments focused on the Commission’s authority to impose data security practices under Section 201(b), ACA makes clear here that the Commission lacks authority to impose *any* of the rules it proposes in the NPRM pursuant to Section 201(b).

<sup>30</sup> See Floor Statement Concerning the Wireless Communications and Public Safety Act of 1999, 145 Cong. Rec. H9861 (Oct. 12, 1999) (statement of Rep. John Shimkus).

<sup>31</sup> See 47 U.S.C. § 202(a).

It is utterly inconsistent with this legislative history and the structure of the Communications Act as a whole to read the Commission's authority under Sections 201 and 202 to overcome the later and more specific limitations on its authority under Section 222. Such a limitless view of the Commission's authority would render much of the rest of Title II, with its minutely detailed statutory provisions and related rules, exceptions and exemptions, largely if not completely superfluous.<sup>32</sup> Notably, the Commission found as much in its *1999 CPNI Order on Reconsideration*, when it stated that “the specific consumer privacy and consumer choice protections established in [S]ection 222 supersede the general protections identified in [S]ection 201(b) and 202(a).”<sup>33</sup> Absent any legislative history suggesting an alternative interpretation, the Commission's 1999 interpretation is the correct one. Indeed, the Commission has long viewed Section 222 as a “comprehensive” privacy framework.<sup>34</sup> For these reasons, the Commission lacks authority under Sections 201 and 202 to adopt privacy and data security rules for BIAS.

---

<sup>32</sup> Further, the Commission's suggestion that Section 222(a) is designed to serve as a privacy and data security catch-all renders Section 201(b) wholly duplicative.

<sup>33</sup> *See 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*, CC Docket Nos. 96-115, 96-149, Order on Reconsideration and Petitions for Forbearance, FCC 99-223, ¶ 152 (rel. Sept. 3, 1999) (1999 CPNI Order on Reconsideration). For a similar reason, the Commission lacks authority to impose its proposed privacy and data security rules pursuant to Section 705 of the Communications Act. As with Sections 201 and Section 202, the broad prohibitions in Section 705 cannot be squared with the specific and nuanced terms of Section 222. Not only do the Commission's proposed rules protect different types of information from Section 705, they also set forth markedly different permissions and prohibitions. Together, these differences demonstrate that Congress did not intend for Section 705 to authorize the complex privacy and data security regime for BIAS providers the Commission proposes in the NPRM.

<sup>34</sup> *1998 CPNI Order* ¶ 14 (“Congress established a comprehensive new framework in [S]ection 222, which balances principles of privacy and competition in connection with the use and

**D. The FCC does not have authority under Section 631 to extend or impose additional privacy requirements on BIAS provided by cable operators**

In the NPRM, the Commission also seeks comment on whether it has the authority to promulgate its proposed privacy and data security rules pursuant to Section 631 of the Cable Act.<sup>35</sup> Section 631 sets forth detailed notice, choice, and security obligations for any “cable service or other service” provided through a cable system. Under the statute, “the term ‘other service’ includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service.”<sup>36</sup> The only appellate court to directly address the issue of whether Section 631 applies to BIAS held that the term “other service” in Section 631 does not apply to the broadband ISP services offered by a cable operator.<sup>37</sup> In *Klimas*, the Court found it “clear” that the term “other service” was not intended to apply to broadband Internet access in part because broadband Internet access “did not exist at the time the Cable Act was passed.”<sup>38</sup> This fact, clearly, has not changed. Moreover, even if a future court were to disagree with the Sixth Circuit, the Commission lacks authority to impose common carrier regulations—such as Section 222 or its rules—on cable operators. Indeed,

---

disclosure of CPNI and other customer information [i.e., subscriber list information and aggregate customer information].”).

<sup>35</sup> See NPRM ¶ 295 (“We welcome comment on the legal framework we offer below for this proceeding and invite commenters to offer their own legal analysis on whether the rules we propose, the alternatives on which we seek comment, and the recommendations that commenters make are consistent with and supported by the statutory authority upon which we rely, or on other statutory authority, including, for example, Sections 631 and 338(i) of the Communications Act.”).

<sup>36</sup> See 47 U.S.C. § 551(a)(2)(B).

<sup>37</sup> See *Klimas v. Comcast Cable Comms., Inc.*, 465 F.3d 271, 276 (6th Cir. 2006).

<sup>38</sup> *Id.*

Section 621 of the Cable Act prohibits the Commission from subjecting a cable system “to regulation as a common carrier or utility.”<sup>39</sup> As a result, the Commission cannot promulgate its proposed privacy and data security rules through Section 631. Further, even if the Commission somehow had authority to implement its proposed rules pursuant to Section 631, it would be unwise to do so. The Commission has never promulgated rules under Section 631, and for good reason: “[S]ection 631’s terms are enforced by the courts, and not by the Commission.”<sup>40</sup> Promulgating rules now would upset the long-standing and successful regime, on which cable operators and their customers have relied for decades. For these reasons, the Commission cannot, and should not, adopt privacy and data security rules for BIAS pursuant to Section 631.

**E. The FCC does not have authority under Section 706 to impose privacy rules, which hurt, not help, the virtuous circle by hindering innovation and partnerships and slowing investment and deployment**

The FCC’s reliance on Sections 706(a) and (b) of the 1996 Act for statutory authority for its proposed privacy and data security rules is misplaced because the proposed rules would undermine, rather than promote, the goals of those provisions.<sup>41</sup> In *Verizon v. FCC*, which

---

<sup>39</sup> 47 U.S.C. § 541(c).

<sup>40</sup> See *Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, et al.*, GN Docket No. 00-185, et al., Declaratory Ruling and Notice of Proposed Rulemaking, FCC 02-77, ¶ 112 (rel. Mar. 15, 2002); *Applications for Consent to the Transfer of Control of Licenses and Section 214 Authorizations by Time Warner Inc. and America Online, Inc., Transferors, to AOL Time Warner Inc., Transferee*, CS Docket No. 00-30, Memorandum Opinion and Order, 16 FCC Rcd 6547, ¶ 279 (2001).

<sup>41</sup> 47 U.S.C. § 1302(a) and (b). Section 706(a) states that “[t]he Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure

reversed in part the Commission’s 2010 *Open Internet Order*, the D.C. Circuit held that Sections 706(a) and 706(b) were independent grants of authority to the Commission and accepted the Commission’s reasoning that the Commission could adopt rules pursuant to Section 706 that promote the so-called “virtuous circle” of edge provider innovation, consumer demand, and broadband infrastructure deployment.<sup>42</sup> However, the *Verizon* Court also noted that Section 706(a) had “at least two limiting principles”: (1) the section must be read in conjunction with other provisions of the Communications Act to ensure that any regulatory action under Section 706(a) fell within the Commission’s subject matter jurisdiction, and (2) regulations must be “designed to achieve a particular purpose: to ‘encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.’”<sup>43</sup>

Here, the proposed rules will not promote the virtuous circle, especially with respect to the deployment of broadband infrastructure by small providers. Specifically, contrary to the Commission’s pronouncements,<sup>44</sup> no evidence indicates that consumers would use broadband more should the Commission supplant the successful FTC privacy and security framework with

---

investment.” Section 706(b) provides that if the Commission finds that advanced telecommunications capability is not being deployed to all Americans in a reasonable and timely fashion, “it shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market.”

<sup>42</sup> See *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

<sup>43</sup> *Id.* at 639-40 (internal citations omitted).

<sup>44</sup> See NPRM ¶ 309 (“[T]he proposed transparency, choice, and security requirements further align with the virtuous cycle of Section 706, since they 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.”).

the onerous privacy and data security regulations it has proposed in this proceeding.<sup>45</sup> Further, no compelling evidence suggests that broadband providers today are not sufficiently protecting their customers' information. In the decade during which the FTC exercised its authority over broadband providers—conducting innumerable investigations and actions against companies related to privacy and data security—we are not aware of a single action against a small BIAS provider for the sorts of privacy and data security practices that the FCC seeks to regulate in the NPRM. A 20-year run free of major incidents simply does not support the argument that prescriptive privacy and data security regulations are needed to promote broadband usage and deployment.

In fact, the proposed rules are more likely to shove a stick in the spokes of the virtuous circle than to perpetuate it. First, a poll of ACA members indicated that across the board, the proposed rules will divert scarce resources from deployment, network improvement, and customer service to regulatory compliance. This will have an outsized impact on small providers, raising their costs and reducing their ability to compete and innovate in the broadband market. For example, the NPRM proposal to narrow the definition of “communications-related services”<sup>46</sup> could make it more difficult for small providers to share information among affiliates and to market and provide ancillary services such as “connected home” solutions that consumers increasingly demand. Second, the Commission’s proposed rules will undermine trust in the broadband ecosystem by, among other things, fatiguing customers through a deluge of customer

---

<sup>45</sup> See *Verizon*, 740 F.3d at 643 (“[W]e must uphold the Commission’s factual determinations if on the record as a whole, there is such relevant evidence as a reasonable mind might accept as adequate to support [the] conclusion”) (citing *Secretary of Labor, MSHA v. Fed. Mine Safety & Health Review Comm’n*, 111 F.3d 913, 918 (D.C. Cir. 1997)).

<sup>46</sup> NPRM ¶ 71.

notifications and opt-out/opt-in choices, and creating an uneven playing field for BIAS providers and edge providers. Third, the drag on broadband deployment and consumer demand will slow edge provider innovation (i.e., the virtuous circle in reverse). Fourth, the proposed rules also will raise barriers to edge provider innovation by requiring BIAS providers to obtain opt-in consent from their customers before sharing any customer proprietary information with edge providers. Finally, the Commission's proposed rules ultimately will harm consumers by raising costs for service (which will reduce their disposable income to pay for edge services), overwhelming them with notifications and approvals, and imposing unnecessary friction in the broadband ecosystem.

#### **IV. EVEN IF THE COMMISSION DOES HAVE AUTHORITY TO IMPOSE RULES FOR BIAS CUSTOMER PROPRIETARY INFORMATION, THE PROPOSED RULES WOULD IMPOSE SIGNIFICANT AND DISPROPORTIONATE COSTS AND BURDENS ON SMALL PROVIDERS**

In the NPRM, the Commission seeks comment on the impact that its proposals would have on small providers.<sup>47</sup> The Commission's proposals would impose tremendous burdens on small providers. These burdens include, but are not limited to:

- attorney and consultant costs associated with regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits;
- development and implementation costs associated with data security controls, website policies, and customer approval tracking systems;
- personnel costs associated with hiring or training dedicated privacy and data security staff;

---

<sup>47</sup> See *id.* ¶ 89 (seeking comment on the burdens of the proposed privacy notice framework for BIAS providers); *id.* ¶ 95 (seeking comment on the burdens of a consumer-facing privacy dashboard); *id.* ¶ 101 (seeking comment on the burdens of the proposed material change notice requirements); *id.* ¶ 131 (seeking comment on the burdens of the proposed opt-in framework); *id.* ¶¶ 177, 194, 212, 219 (seeking comment on the burdens of the proposed data security obligations); *id.* ¶¶ 241, 247 (seeking comment on the burdens of the proposed data breach notification requirements).

- costs associated with all aspects of providing required notices and follow-up;
- third-party costs associated with modifying contracts and ensuring compliance for call centers, billing software, and others that interface with customer proprietary information; and
- opportunity costs associated with diverting scarce resources from innovation and infrastructure deployment to regulatory compliance.

Below, we describe the burdens associated with the Commission’s most problematic proposals.

**A. The proposed data security requirements are unduly prescriptive and impractical**

The Commission’s proposed prescriptive data security requirements would impose overwhelming costs and burdens on small providers.<sup>48</sup> Among the most onerous of the Commission’s proposed data security rules is the requirement to establish and perform regular risk management assessments. While obtaining a suitable form of risk management assessment may in many circumstances be a best practice, requiring that small providers establish and perform “regular” risk management assessments through binding regulations would be costly, time-consuming, and operationally disruptive. To comply, most small providers would need to hire a team of outside experts—including consultants, attorneys, and technical specialists—to design and conduct the assessment. Further, these risk management assessments would divert core staff from their day-to-day responsibilities to support the audit process through interviews, walk-throughs, system tests, and similar activities. To the extent that small providers use third

---

<sup>48</sup> *See id.* ¶¶ 167-232. As the Communications Security, Reliability and Interoperability Council (CSRIC) recognized in its 2015 Working Group 4 Final Report, “Small and Medium Businesses (SMBs) have unique circumstances and challenges that may influence their approach to implementing the [NIST Cybersecurity] Framework and providing macro-level assurances,” and “there is no one-size fits all approach to cybersecurity risk management.” *See The Communications Security, Reliability and Interoperability Council IV, Working Group 4, Final Report*, 25, 375 (Mar. 2015).

parties to handle billing, customer service, network maintenance, security, and other functions, risk management assessments would be extremely complicated and disruptive, particularly where existing contracts do not provide for audit rights or where they prescribe data security standards different from those that the Commission proposes here. Moreover, any specific frequency requirement—e.g., one risk management assessment per year—would impose disproportionate burdens on smaller providers.

Moreover, the proposal to require BIAS providers to “promptly address any weaknesses in the provider’s data security system identified” in the risk management assessments would impose significant burdens and lead to unintended consequences, including weakened security. While addressing “any” weakness “promptly” would be nice to do, often it is not feasible to do so based on the interrelationship and interdependencies of some of the weaknesses, the limited resources and expertise available, and the need to prioritize the most serious risks and threats. It is a fundamental principle of risk management to prioritize. To the extent companies, especially smaller ones with limited resources and expertise, “promptly” try to address “any weaknesses” that are identified, they are likely to make choices that divide, disperse and misallocate their resources, resulting in less protection and security in the most important places. This language and other parts of this rule may also potentially become a major and costly generator of litigation and liability.<sup>49</sup>

---

<sup>49</sup> In addition, no BIAS provider can “ensure the security... of all customer PI,” something they “must” do as stated in proposed rule 64.7005(a). To the extent that the Commission may intend section 64.7005(b), which mentions the sensitivity of the customer information and the BIAS provider’s activities, to cut back in some way on the requirements of (a), it should revise and clarify the proposed rule.

The Commission’s proposed requirement that BIAS providers designate a senior official “with responsibility for implementing and maintaining the BIAS provider’s information security program” also would impose substantial and disproportionate burdens on smaller providers.<sup>50</sup> To be sure, the existing voice-centric rules already require small providers to have an officer with personal knowledge of the company’s compliance with the CPNI rules. However, the proposed rules would supersize the responsibility of the designated point of contact, requiring them not only to have personal knowledge of the company’s policies and procedures, but to be responsible for “implementing and maintaining” those policies. This would effectively require a full-time staff member to manage privacy and data security compliance, which is well beyond the means of most small providers.<sup>51</sup> Moreover, training privacy and information security officers is expensive. Today, many dedicated privacy and data security positions require or recommend one or more professional certifications, which can cost hundreds or thousands of dollars to prepare for, obtain, and maintain.<sup>52</sup> Further, the Commission’s proposal is not only costly, it is also unwise. Large organizations tend to have separate roles for privacy (e.g., a Chief Privacy Officer responsible for legal and regulatory compliance) and information security (e.g., a Chief Information Security Officer responsible for implementing security programs). These

---

<sup>50</sup> See NPRM ¶¶ 188-90.

<sup>51</sup> According to Indeed.com, the average salary for a Chief Privacy Officer in the United States is \$95,000. See Chief Privacy Officer Salary, Indeed.com, <http://www.indeed.com/salary?q1=Chief+Privacy+Officer&l1=USA>.

<sup>52</sup> Indeed, the Commission itself has required that privacy officers be “privacy certified.” See *In the Matter of AT&T Services, Inc.*, File No.: EB-TCD-14-00016243, Order and Consent Decree, DA 15-399, ¶ 17 (rel. Apr. 8, 2015); *In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, File No.: EB-TCD-14-00017601, Order and Consent Decree, DA 16-242, ¶ 17 (rel. Mar. 7, 2016).

separate roles exist because they require largely different skillsets and training, and as such should not be combined within a single individual.

Small providers also would struggle to comply with the Commission’s proposal that BIAS providers “provide their customers with access to all customer [proprietary information] in their possession, including all CPNI, and a right to correct that data.”<sup>53</sup> As the FTC has recognized, “consumer access [to data] should be proportional to the sensitivity and the intended use of the data at issue,” with more limited access rights for non-sensitive information and in situations where the information is not used for consumer reporting purposes covered under the Fair Credit Reporting Act.<sup>54</sup> For example, “[f]or data used solely for marketing purposes, . . . the costs of providing individualized access and correction rights would likely outweigh the benefits.”<sup>55</sup> Moreover, small providers generally store customer proprietary information in multiple locations throughout their organization, on different and incompatible systems, and in both paper and electronic form. Rendering all of this information accessible to customers would be a herculean effort, requiring providers to build new systems to store all customer proprietary information in their possession and create mechanisms for consumers to access and correct the information. Moreover, such a system would increase security risk by opening systems

---

<sup>53</sup> See NPRM ¶ 205.

<sup>54</sup> See 2012 FTC Privacy Report at 65. Distinguishing between non-sensitive and sensitive information, or between types of sensitive information, makes sense from an economic standpoint. The Federal Bureau of Investigation (FBI), in an April 2014 bulletin, noted that cybercriminals can sell partial electronic health records on the black market for \$50 each, but sell stolen social security card numbers or credit card numbers for \$1 each. See FBI Cyber Division Private Industry Notification, (U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, PIN #: 140408-009 (Apr. 8, 2014).

<sup>55</sup> See 2012 FTC Privacy Report at 65.

previously designed for internal use only. Further, the benefit to consumers is unlikely to offset the extreme burden in making the information available, since, in general, customers are not clamoring for access to their customer proprietary information. As a result, the effort and cost of making the information available in all likelihood will be for naught.

The Commission's proposal to require training for all personnel, agents, and affiliates that handle customer proprietary information would also impose significant burdens on small providers.<sup>56</sup> As above, for those small providers that lack dedicated compliance staff, the Commission's proposed rule would effectively require them to pay attorneys or consultants to conduct the training. Further, unlike the existing rules, which do not require training of affiliates or other third parties, this proposed rule would require small providers to pay for and oversee training for a much broader group. Indeed, neither HIPAA, the GLBA, nor the existing CPNI rules require covered entities to train affiliates, and for good reason: not only is additional training costly, but it may conflict with the affiliate's existing training models.<sup>57</sup>

Other proposals in the NPRM could place undue burdens on small providers. For example, if the Commission were to require small providers to pass through data security requirements to third parties by contract, small providers may need to renegotiate existing contracts or to add unnecessary transaction costs to future contract negotiations. For small providers that lack bargaining power over their vendors, it may be impossible to pass through such requirements. Finally, even if a vendor were to agree to specific privacy and data security

---

<sup>56</sup> See NPRM ¶¶ 185-87.

<sup>57</sup> See *id.* ¶ 186.

terms, small BIAS providers often lack the resources and staff to monitor these third parties' compliance.<sup>58</sup>

Similarly, the requirement to adopt “robust customer authentication requirements”<sup>59</sup> could impose significant burdens if the Commission were to require multi-factor authentication or other prescriptive rules. Requiring multi-factor authentication could require expensive specialized equipment and would require small providers to overhaul existing authentication systems at significant cost, e.g., by distributing dongles to customers. Further, requiring multi-factor authentication could raise liability issues under the Telephone Consumer Protection Act (TCPA), particularly for fixed BIAS providers that would rely on text messages to conduct multi-factor authentication.<sup>60</sup> Moreover, multi-factor authentication is burdensome for some consumers, particularly the elderly and those without smartphones who are not used to the system. As a result, a multi-factor authentication requirement could require costly consumer education and customer service training, both of which would be costly for small providers.

---

<sup>58</sup> For these reasons, ACA also opposes the Commission's proposal to require small providers to contractually prohibit entities receiving aggregate customer data from re-identifying such information, and to monitor those entities' compliance. *See id.* ¶¶ 161-62.

<sup>59</sup> *See id.* ¶ 191.

<sup>60</sup> *See In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, FCC 12-21 ¶ 28 (rel. Feb. 15, 2012).

**B. The proposed customer approval requirements are complex, restrictive, and impractical**

The Commission’s proposal to adapt its existing three-tiered customer approval framework<sup>61</sup> to the BIAS context would impose significant burdens on small providers that outweigh any customer benefit.

First, and most importantly, because the new rules are different from both the flexible FTC Section 5 approach and the existing customer approval framework for voice services, complying with the proposed customer approval rules would require providers to engage attorneys to understand the new rules and what they mean for existing and planned collection, use, and sharing of customer proprietary information. Specifically, these attorneys would be required to assist small providers with classifying their services as “communications-related” or “non-communications-related” and determining whether particular uses of customer proprietary

---

<sup>61</sup> The FCC’s proposed customer approval framework establishes three levels of customer approval: no additional customer consent, opt-out approval, or opt-in approval. *See* NPRM ¶¶ 106-33. Specifically, the first tier requires no additional consent for uses that are statutorily exempted or for which consent is implied by virtue of the customer-carrier relationship. The second tier requires providers to give a customer the opportunity to opt-out of the use or sharing of her customer PI prior to the BIAS provider (1) using the customer’s PI to market other communications-related services to the customer; or (2) sharing the customer’s PI with affiliates that provide “communications-related services,” in order to market those communications-related services to the customer. The third tier requires opt-in approval from a customer before using customer PI for any other purpose before disclosing customer PI to (1) affiliates that do not provide communications-related services and (2) all non-affiliated third parties. The Commission also proposes to narrow the definition of the term “communications-related services,” effectively subjecting more types of services and uses to an opt-in consent requirement. *See id.* ¶¶ 71-73. In addition to the proposed consent framework, the NPRM proposes to adopt requirements for soliciting consent, including a requirement that BIAS providers obtain consent after the point of sale but before the first time that they seek to use customer PI for a purpose that would require consent, as well as a persistently available means of denying or granting approval. *See id.* ¶ 82. Moreover, the NPRM proposes to require BIAS providers to document their compliance with the rules through recordkeeping requirements, training requirements, supervisory review processes, and notice to the Commission. *See id.* ¶¶ 185-90, 252-53.

information fall within the established exemptions under Section 222(d) or require additional consent. After making the initial classification determinations, attorney assistance would be necessary to draft consent forms and compliance plans, and help train employees, agents, and partners on the permissible uses of customer proprietary information. In all, these requirements could cost thousands of dollars in legal fees.

Second, the proposal effectively will require small providers to build systems for obtaining and tracking BIAS consumer consents. Small providers that already have internal systems in place would need to upgrade them, likely hiring outside developers to assist. Small providers that rely on third-party solutions likely would need to negotiate statements of work or new contracts to upgrade systems, with weeks to months of development time and thousands of dollars in expenses. As for small providers that do not have consent tracking systems in place for BIAS customers (e.g., small providers that run their BIAS operations as a separate affiliate), the proposal would require them to build, purchase, or license new systems. Importantly, small providers would need to undertake these steps even if they already comply with the Commission's existing CPNI rules, since the proposed rules cover all customer proprietary information and impose new limitations on the collection, use, and sharing of that information.

Third, the proposed approval framework could require providers to obtain new approvals from consumers at a substantial cost. For example, today small BIAS providers generally obtain customer approval through an opt-out mechanism, which usually is presented to consumers on the provider's website, at the time of enrollment, and periodically thereafter. If the Commission were to require opt-in for existing uses, these providers would need to go back to their consumers to obtain a new approval. Further, if the Commission were to void existing consents, it could undermine existing contractual relationships that BIAS providers have with third parties

or affiliates with respect to the use and sharing of customer proprietary information, inadvertently leading to contractual breaches.

Fourth, the proposed rules will have a significant impact on the ability of BIAS providers to offer and market innovative services to their subscribers. Until the *2015 Open Internet Order*, BIAS providers were subject to the FTC's flexible privacy framework, which sensibly uses opt-out approval as a default approval mechanism. This framework has allowed providers, including small providers, to explore, market, and deploy innovative, value-added services to their consumers, including home security and home automation services that will drive the "Internet of Things." The Commission's proposal flips the FTC's successful approach on its head, defaulting to an "opt-in" framework that is out of step with the market and customer expectations. ACA members have said that this framework would make it extremely difficult—if not impossible—to effectively market and deploy innovative products to their consumers. As more customers expect their BIAS providers to offer these value-added services—and choose their BIAS provider based on those services—the Commission's proposal will impose a significant drag on innovation and business growth. Because small providers often will avoid services that require obtaining opt-in consent before marketing or offering them to consumers, the result would be less consumer choice and less consumer value—and fewer revenue opportunities that could support the deployment of broadband infrastructure.

Fifth, because of the way that many BIAS providers are structured, with separate affiliates for different verticals and different regions, the NPRM's approval framework necessarily will make opt-in approval unavoidable. For example, under the proposed framework, a BIAS provider could not share basic customer information with an IP-enabled home security affiliate for purposes relating to the provision of the home security product (e.g.,

customer service or troubleshooting) without obtaining opt-in consent from the consumers. This shift would impose dramatic costs for small BIAS providers that have relied on the FTC's flexible Section 5 regime and the ease of operating without obtaining opt-in approval.

Finally, the proposed customer approval framework could lead to unintended consequences, particularly with respect to voluntary cybersecurity information sharing. The Commission proposes to interpret Section 222(d)(2) to permit BIAS providers to "use or disclose CPNI whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities" and asks about expanding the exceptions in Section 222(d) in the broadband context.<sup>62</sup> Encouraging more entities to share information relating to cybersecurity threats and defensive measures voluntarily and to do so faster, potentially in real time, is a major U.S. cybersecurity priority, reflected by Executive Orders of the President, the Cybersecurity Act of 2015, Pub. L. No. 114-113 (CISA), and the activities of the Commission and numerous other entities.<sup>63</sup> Unfortunately, without additional clarity or a different approach, this and other proposals could inadvertently raise questions about and potentially deter sharing.<sup>64</sup>

---

<sup>62</sup> NPRM ¶¶ 117, 120.

<sup>63</sup> See Promoting Private Sector Cybersecurity Information Sharing Executive Order; the Communications Security, Reliability and Interoperability Council IV, Working Group 4, Final Report (Mar. 2015); FCC Chairman Tom Wheeler, Remarks at the American Enterprise Institute (June 12, 2014); Exec. Order No. 13718, 81 Fed. Reg. 7441 (Feb. 9, 2016) (Commission on Enhancing National Cybersecurity Executive Order); Exec. Order No. 13719, 81 Fed. Reg. 7959 (Feb. 9, 2016) (Establishment of the Federal Privacy Council); Communications Security, Reliability and Interoperability Council V, Federal Communications Commission, <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability> (last visited May 27, 2016); Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113.

<sup>64</sup> As noted above, ACA has advocated the importance of developing standards that facilitate effective voluntary cybersecurity information by small and medium size businesses, and its members have participated in the CSRIC. ACA also actively supported passage of CISA

For example, sharing cybersecurity information pursuant to CISA is voluntary. An entity that is engaged in doing so pursuant to that law can receive liability protection even if it shares information about specific persons that is not part of a cyber threat indicator if it is not known at the time of sharing that it is included.<sup>65</sup> In contrast, the Commission proposes that BIAS providers may disclose CPNI whenever “reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities.”<sup>66</sup> If a BIAS provider, engaged in cybersecurity threat information sharing inadvertently discloses customer proprietary information that is not part of a threat indicator, would that disclosure fall within the Commission’s exemption? If not, would Commission’s proposal require a BIAS provider to provide the Commission or consumer with a data breach notification? The result could be fewer companies, especially small providers, sharing threat information in the first place. Smaller providers, for example, may also view themselves as at greater risk than bigger businesses of making an inadvertent mistake if engaged in sharing information in near or real time, and as having few resources with which to engage with the Commission. In this way, the costs, complexity, and uncertainty of the

---

because it believes that CISA encourages information sharing by providing clear liability and certain regulatory protections that lessen some of the concerns of small businesses. Businesses are protected from liability if, for example, among other things: (1) they share personal information that is not part of a threat indicator but don’t know at the time of sharing that they have done so; and (2) if they fail to act on a threat indicator they receive through information sharing. They are also protected against certain regulatory activities related to shared information. Guidance from the Department of Homeland Security and the Department of Justice makes clear that at least some information on the FCC’s list of PI can properly be shared voluntarily even under CISA as a part of certain “threat indicators.” *See e.g.*, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, February 16, 2016 at p. 6-7.

<sup>65</sup> *See* CISA, Pub. L. No. 114-113, § 104(d)(2) (2015).

<sup>66</sup> NPRM ¶ 117.

Commission’s proposals and proposed exemption, if not satisfactorily addressed, could undermine information sharing and efforts to improve the security of customer proprietary information, as the Commission defines it.

**C. The proposed data breach notification requirements are unnecessarily prescriptive**

The Commission’s proposal to impose heavy-handed breach notification obligations creates several burdens that would disproportionately impact small providers.<sup>67</sup>

First, by expanding the definition of “breach,” the Commission unnecessarily increases the number of situations in which a breach notification would be required. In the NPRM, the Commission proposes to define “breach” as “any instance in which a person, without

---

<sup>67</sup> In the NPRM, the Commission seeks comment on its proposal to adopt a modified and expanded version of its data breach notification requirements for both voice service and BIAS. *See id.* ¶¶ 233-255. Specifically, the data breach notification rules would require a BIAS provider or voice provider to notify the Commission and law enforcement within seven days of discovery of a breach of customer PI, and to notify customers within ten days, unless law enforcement directs otherwise. *See id.* ¶ 246. As written, the proposed rules would require a notification to law enforcement of any breach except where the breach involves fewer than 5,000 customers. *See id.* ¶ 247. Strangely, the Commission pitches this limited exemption as a way to reduce the burden on providers, when in fact the Commission *added* two notifications, which will be required regardless of breach size. *See id.* ¶ 247. Rather than require that every breach affecting even one individual be reported to the Commission, it ought only to require breach notification to the Commission, law enforcement, and customers where a reasonable number of parties are affected. This would save expenses and reduce the burden on small businesses, reflect the approach of the states, and provide ample data to the Commission to recognize and address important trends. The Commission sets reasonable thresholds to trigger reporting in other important areas where it seeks to track trends and help improve performance, rather than require reporting of every event, as in the case of the triggers it has set for reporting outages through the Network Outage Reporting System (“NORS”). *See* 47 C.F.R. § 4.9; *Amendments to Part 4 of the Commission’s Rules Concerning Disruptions to Communications, New Part 4 of the Commission’s Rules Concerning Disruptions to Communications*, PS Docket No. 15-80, ET Docket No. 04-35, Notice of Proposed Rulemaking, Second Report and Order and Order on Reconsideration, FCC 15-39 (rel. Mar. 30, 2015). *See also* Public Safety and Homeland Security Bureau, *Network Outage Reporting System (NORS)*, Federal Communications Commission, <http://transition.fcc.gov/pshs/services/cip/nors/nors.html>.

authorization or exceeding authorization, has gained access to, used, or disclosed customer [PI].”<sup>68</sup> This definition expands the current definition of breach to cover all personally identifiable information and all CPNI. Moreover, the definition of breach does not have an intent or harm component—even unintentional breaches causing no consumer harm would trigger notification obligations, at least to the Commission and consumers. As a result, the proposed rules would dramatically expand the situations in which a breach notification would be required, increasing the total costs of compliance, as well as the risk of costly enforcement actions. Moreover, the costs of providing notifications and associated breach costs are sky high—one recent estimate was well over \$130 per person.<sup>69</sup>

Second, the Commission fails to provide adequate time for BIAS providers to investigate breaches and provide meaningful and complete notifications. ACA members have indicated that while it is possible to respond to some breaches within seven days, in many situations—particularly with respect to more complex security incidents—seven days simply is not enough time. If small BIAS providers were required to comply with a seven-day timeline, they would need to divert senior and technical staff solely to data breach response for the duration of the

---

<sup>68</sup> NPRM ¶ 75.

<sup>69</sup> Thus, the FCC’s proposed combination of an expansive definition of breach, a very broad definition of personal information, and a requirement of customer notification even where there is no likelihood of harm is economically toxic, especially to small businesses, even without the additional requirement of a company having to engage with the FCC through reporting and possibly otherwise on *every* breach no matter how small. *See generally* Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals*, Richard Kissel, Hyunjeong Moon, U.S. Department of Commerce, 2 (December 2014) (“The average estimated cost for these notifications and associated security breach costs is well over \$130 per person. If you have 1000 customers whose data was/*or might have been* compromised in an incident, then your expected minimum cost would be \$130,000, per incident.”) (emphasis added).

breach response period, and to hire a data breach response team including outside attorneys, IT experts, and crisis management specialists. In most cases, small providers could not afford to do so, and as a result, would simply do their best to comply, risking costly enforcement action for timely, but incomplete, breach reporting. Neither option is affordable for small providers. Moreover, even President Obama proposed a much more generous single, national 30 day standard for notification to customers if their information has been stolen.<sup>70</sup>

Finally, an over-inclusive data breach notification rule would have a negative consumer impact. Under the majority of state-level data breach notification rules, companies are only required to notify their customers about breaches of sensitive information that are likely to cause consumer harm (e.g., fraud, crime, or identity theft).<sup>71</sup> As a result, when a consumer receives a breach notification, he or she understandably concludes that something serious has happened. In the Commission’s proposed framework, however, even unintentional breaches of public information with no risk of consumer harm would require a breach notification.<sup>72</sup> This

---

<sup>70</sup> President Barack Obama, Remarks at the Cybersecurity and Consumer Protection Summit, Stanford University, February 13, 2015 (“We’ve called for a single national standard so Americans know within 30 days if your information has been stolen.”) <https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>. Not only is the FCC’s proposed timetable much faster and different than that of the President, it does not replace existing law across the country with a single national standard.

<sup>71</sup> See, e.g., *infra* at n. 100.

<sup>72</sup> Exacerbating the potential costs is the Commission’s pronouncement in the *TerraCom/YourTel NAL* that carriers be “over inclusive” in their breach notifications. *In the Matter of TerraCom, Inc. and YourTel America Inc. Apparent Liability for Forfeiture*, File No.: EB-TCD-13-00009175, Notice of Apparent Liability for Forfeiture, FCC 14-173, ¶ 43 (Oct. 24, 2014) (“[W]e find that TerraCom and YourTel acted unjustly and unreasonably by failing to notify all customers whose Lifeline enrollment information was exposed to *actual and potential data security breaches* . . . . We expect carriers to act in an *abundance of caution—even to the extent of being overly inclusive*—in their practices with respect to notifying consumers of

framework would cause significant customer confusion and distrust in BIAS providers, leading to less broadband usage and undermining the virtuous circle.

Such a standard invariably would lead to notice fatigue, consumer aggravation and inconvenience, and distrust in the broadband ecosystem. Based on existing database breach laws, rules, and standards consumers have come to expect only to receive notifications if there has been a breach of sensitive information or if consumer harm is reasonably likely. An over-inclusive or non-harm-based breach standard at first will create a false sense of danger. As a consequence, consumers might respond in ways that are unnecessary and inconvenient for them, and likely would flood small providers' customer service lines, cancel accounts due to distrust in their provider, or bring law suits against their provider, each of which would be extremely costly. Over time, as consumers learn that the breach notifications more often than not relate to inadvertent breaches with little or no risk of consumer harm, it will become less likely that they will pay attention to any data breach notification (including those with an actual likelihood of consumer harm). This would have a ripple effect throughout the entire broadband ecosystem, as consumer reduce their vigilance to breach notifications across the board.

**D. The proposed notice requirements are burdensome and unnecessary**

The Commission's proposal to require BIAS providers to "provide customers with clear and conspicuous notice of their privacy practices at the point of sale and on an on-going basis through a link on the provider's homepage, mobile application, and any functional equivalent,"<sup>73</sup>

---

security breaches.") (emphasis added), [https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-14-173A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf). Should the Commission adopt a breach notification standard in line with its proposal, it should clarify that its misguided "over inclusive" notification standard no longer applies.

<sup>73</sup> See NPRM ¶ 82.

as well as its proposal to require updates for “material” changes to such policies, also would impose substantial burdens on small providers.

To comply with the proposed notice rule, small providers would need to hire counsel to review and update existing privacy policies or to draft new BIAS-specific privacy policies. Preparing such notices can cost a provider thousands of dollars up front, and incremental amounts as services, policies, and practices (and rules) evolve. Further, for any changes to a privacy policy, small providers would need to rely on outside counsel to determine if a given change is “material” in the Commission’s eyes, and to draft compliant notices for consumers. In addition to legal costs, the proposed notice requirements also would impose technical costs associated with posting the notice “persistently” on the provider’s website, mobile app, and any functional equivalent. While some ACA members have in-house web development expertise, others do not, and as such would need to have vendors prepare the policy for publication online in the manner that the Commission proposes.

Above all other costs, however, the most burdensome for small providers would be a requirement to develop a customer dashboard. Universally, the ACA members we interviewed indicated that developing a customer dashboard to view and manage customer proprietary information and choices would be a near-impossible task. If these providers were required to make available customer proprietary information, policies, and approval status through a dashboard, ACA members estimate, they would need to pull together multiple systems that hold customer proprietary information and approval status information, a task that itself could take years to accomplish, if they could afford the project at all. After providers brought all of the information together, they would need to develop the internal and customer-facing systems to provide customers with access to that information. Because ACA members generally do not

have the technical expertise in house, such a project would require hiring outside consultants and IT experts at an enormous cost. Further, if such a system needed to include all customer proprietary information in one place, it necessarily would make the dashboard a target for attackers, and consequently would require extremely high levels of security to prevent breaches. Importantly, a customer dashboard would provide almost no added consumer value. Consumers already have access to most of their customer proprietary information—as the Commission defines it—through their web browsers and the various edge services that they use, and have access to information about BIAS providers’ privacy practices through those providers’ privacy notifications. For these reasons, the proposed customer dashboard would present an extreme burden on small providers, outweighing any consumer benefit, and should not be adopted.

**V. THE COMMISSION SHOULD ADOPT A PRIVACY AND DATA SECURITY FRAMEWORK CONSISTENT WITH THE FTC’S SUCCESSFUL “UNFAIR OR DECEPTIVE ACTS OR PRACTICES” APPROACH AS SET FORTH IN THE INDUSTRY PROPOSAL**

In the NPRM, the Commission seeks comment on “any alternative approaches we can take to protect customer privacy, preserve customer control, and promote innovation . . . .”<sup>74</sup> As ACA stated in its proposal with several other industry groups, “[w]e believe it is important to maintain a consistent privacy framework for the Internet” based on the successful “unfair or deceptive acts or practices” standard of Section 5 of the FTC Act, under which BIAS providers have complied without incident for over a decade.<sup>75</sup> Such an approach will protect consumers

---

<sup>74</sup> *See id.* ¶ 292.

<sup>75</sup> *See* Letter from Matthew M. Polka, President & CEO, American Cable Association, et al., to Tom Wheeler, Chairman, Federal Communications Commission (Mar. 1, 2016) (Industry Proposal). ACA continues to believe that the Industry Proposal reflects the best way forward for the Commission’s privacy and data security rules, and for that reason adopts the Industry Proposal in its entirety here.

and avoid entity-based regulation that would create consumer confusion and stifle innovation. Consumers expect their data will be subject to consistent privacy standards based upon the sensitivity of the information and how it is used, regardless of which entity in the Internet ecosystem uses that data. Indeed, the FTC itself has stated that “any privacy framework [for BIAS providers, operating systems, browsers, and social media] should be technology neutral.”<sup>76</sup>

The Industry Proposal focuses on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. Specifically, we recommend that the Commission adopt the following enforceable principles:

- **Transparency.** A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- **Respect for Context and Consumer 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. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- **Data Security.** A telecommunications service 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>76</sup> See 2012 FTC Privacy Report at 56.

Providers' CPNI data security programs should provide reasonable protections in light of the nature and 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.

- **Data Breach Notifications.** Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

A consistent privacy framework for the Internet also will continue to provide Internet service providers with the flexibility to update their practices in ways that meet the evolving privacy and data security needs of their customers and ensure they can provide their customers new products and customized services. Such a framework would identify privacy or security goals, and afford providers, including smaller providers with limited resources, flexibility in achieving those goals. Rules dictating specific methods—like those proposed in the NPRM—quickly become out of date and out of step with constantly changing technology, and will only hamper innovation and harm consumers.

The Industry Proposal would dramatically improve the ability of small providers to comply without incurring undue cost or burden. As explained in Section II above, small providers dutifully comply with all of the privacy and data security laws and rules that apply to them. As such, small providers would not have to incur additional costs to bring their policies, processes, and systems into compliance. Further, the consumer choice provisions in the Industry Proposal are superior for small providers because they align with consumer expectations by respecting the context of customer-carrier interactions, and provide flexibility that will enable small providers to offer new and innovative services to their customers, increasing consumer

choice and competition. Moreover, the proposed data security rule maintains a robust general security standard that requires “physical, technical, and administrative” security safeguards while appropriately including the size of the company as a factor in determining whether particular safeguards are reasonable. As such, in the event that small providers grow into medium or large providers, the rules naturally will require more sophisticated processes commensurate with their larger operations. Further, to the extent that the Commission would like to establish best practices, this framework would not preclude multi-stakeholder processes to do so. Finally, the proposed data breach notification rule is superior to the proposed rule because it provides flexible deadlines that will not overburden small providers, and a safety valve for good faith disclosures so that small providers can avoid counterproductive strict liability enforcement actions associated with inflexible and overly prescriptive regimes.

A flexible “unfair and deceptive” approach as outlined in the Industry Proposal would meet consumers’ privacy needs while allowing them to take advantage of innovative products and services, and would avoid inconsistent oversight. Moreover, it would ensure a level playing field between edge providers and BIAS providers, promoting an innovative *and* competitive broadband ecosystem. Lastly, if adopted in its entirety, it would avoid overburdening small providers and would reduce or eliminate the need for special exemptions. For these reasons, the FCC should adopt a flexible approach consistent with the Industry Proposal.

**VI. IF THE FCC ADOPTS A PRESCRIPTIVE, *EX ANTE* FRAMEWORK, IT SHOULD ADOPT TAILORED EXEMPTIONS FROM SPECIFIC RULES, EXTEND IMPLEMENTATION TIMEFRAMES FOR SMALL PROVIDERS, AND STREAMLINE AND RATIONALIZE ITS SECTION 222 RULES**

If the Commission pursues a prescriptive, *ex ante* privacy and data security framework, it should adopt targeted exemptions and implementation extensions for small providers consistent

with similar privacy regimes.<sup>77</sup> Moreover, the Commission should rationalize and streamline its proposed rules to ease the burden on small providers.

**A. The Commission should adopt targeted exemptions to its proposed BIAS privacy and data security rules**

Throughout the NPRM, the Commission seeks comment on ways that it can ease the burdens of its proposed rules on small providers, including exemptions from generally applicable rules or other means to ease the burdens on those providers and their customers.<sup>78</sup> ACA applauds the Commission for recognizing the unique burdens that small providers face.<sup>79</sup> As explained in Section IV above, many of the Commission’s proposed prescriptive regulations would be unduly burdensome for smaller providers, which lack the staff, internal expertise, and

---

<sup>77</sup> To the extent that the Commission adopts new or modified rules for voice or cable service, ACA submits that the Commission should adopt consistent exemptions, extensions, and streamlined rules for those services as well.

<sup>78</sup> See NPRM ¶ 89 (“Are there any alternatives [to the proposed notice requirements] that would reduce the burdens on BIAS providers, particularly small providers, while still ensuring that BIAS providers’ privacy practices are sufficiently transparent?”); *id.* ¶ 95 (“We seek comment on the costs and benefits of requiring the creation of such a dashboard, and any alternatives that Commission should consider to minimize the burdens of such a program on small providers”); *id.* ¶ 101 (“Is there any way to modify our proposed material change rules so as to lessen the burden on these requirements on small providers while still achieving the Commission’s stated goals of increasing transparency in the BIAS market and keeping consumers well-informed of their BIAS providers’ privacy practices?”); *id.* ¶ 151 (“We seek comment on ways to minimize the burden of our proposed customer choice framework on small BIAS providers. In particular, we seek comment on whether there are any small-provider-specific exemptions that we might build into our proposed approval framework.”); *id.* ¶ 177 (“We . . . seek comment on whether there are alternative actions that BIAS providers could employ to meet” the goals of the proposed data security requirements.”); *id.* ¶ 241 (“Should the commission consider establishing any exceptions” to its proposed data breach notification rules?”).

<sup>79</sup> See also FCC, *Cybersecurity for Small Business*, <https://www.fcc.gov/general/cybersecurity-small-business>; FCC, *Cyberplanner*, <https://www.fcc.gov/cyberplanner>.

legal resources to implement such highly prescriptive regulations.<sup>80</sup> If the Commission declines to adopt the Industry Proposal in favor of prescriptive, *ex ante* rules, ACA respectfully calls on the Commission to adopt several targeted exemptions that will ease burdens on smaller providers while continuing to promote the Commission’s goals of transparency, choice, and security.

First, the Commission should exempt small providers from the specific “minimum” data security requirements that it sets forth in proposed Section 64.7005(a), and add “the size of the BIAS provider” to the factors that the Commission must consider when assessing the reasonableness of a BIAS provider’s security program. As demonstrated above, even the proposed minimum data security standards would impose tremendous costs on small providers, which typically lack the resources and expertise of larger providers. Rather than unnecessarily force these burdens on small providers, the Commission should adopt a flexible approach that reflects the FTC’s well-established framework. As the Commission notes in the NPRM, the FTC’s general privacy framework takes into consideration the size of the business when determining whether privacy practices are reasonable.<sup>81</sup> The FTC framework also “does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties.”<sup>82</sup> Similarly, the GLBA permits entities to

---

<sup>80</sup> See e.g., National Institute of Standards and Technology, *Small Business Community: Detailed Overview*, NIST Computer Security Division: Computer Security Resource Center, <http://csrc.nist.gov/groups/SMA/sbc/overview.html> (“SMBs cannot always justify an extensive security program, or often a single full time expert... The difficulty for these organizations is to identify needed/cost-effective security mechanisms and obtain training that is practical and cost effective.”)

<sup>81</sup> See 2012 FTC Privacy Report at 9.

<sup>82</sup> See *id.* at 15.

develop security plans “appropriate to [the company’s] size and complexity.”<sup>83</sup> Oddly, the Commission cites these flexible standards, but nevertheless does not include company size as a factor in determining the reasonableness of a BIAS provider’s data security plan.<sup>84</sup> The Commission should take the opportunity to harmonize its rules with the existing FTC approach, and exempt small providers from the specific minimum data security standards and add company size as a consideration in determining the reasonableness of a provider’s data security practices.

Second, the Commission should exempt small providers from the more onerous elements of its customer approval framework. As explained above, the proposed customer approval framework—which differs substantially not only from the FTC’s more flexible approach, but also from the Commission’s existing approach under the CPNI rules—would disrupt existing agreements between carriers and their customers, as well as between affiliates or other third parties and their customers. To avoid this result, the Commission should grandfather all existing consents between small BIAS providers and their customers, including those that permit sharing of customer information with third parties. Such an exemption will not negatively impact these customers, who have already provided their approval to the BIAS providers, and will ensure that small BIAS providers can fulfill their contractual obligations with any agents, affiliates, or third parties with whom they share customer proprietary information. Moreover, the Commission also should exempt small providers from the requirement to obtain additional customer approval to use, disclose, or make available customer proprietary information, provided they do not share sensitive customer proprietary information with unaffiliated third parties for marketing purposes.

---

<sup>83</sup> 16 C.F.R. § 314.3.

<sup>84</sup> *See* NPRM ¶ 219.

Because this proposed exemption is consistent with the FTC's approach and is more sensitive to the context of consumer interactions with their carriers, it should be adopted.

Third, the Commission should adopt exemptions to several elements of the Commission's proposed data breach notification rule (as applied to both voice and BIAS services). The Commission should exempt small providers from the specific notification deadlines in favor of an "as soon as reasonably practicable" standard. ACA members we surveyed explained that the Commission's proposed timelines are too short to conduct a meaningful investigation and to provide complete and accurate notifications to affected customers. To avoid the undue consumer confusion and significant burden on small providers that the proposal rule would cause, an exemption from the specific notification deadlines is warranted.

Fourth, the Commission should exempt small providers from any customer dashboard requirements that it adopts pursuant to its notice and choice regulations. These dashboards would impose significant costs on providers to develop and maintain them, with marginal, if any, resulting consumer benefit. Further, we are not aware of any U.S. laws or rules that mandate such a dashboard. In addition, to the extent that the dashboard would require BIAS providers to make available customer proprietary information to customers (e.g., to enable them to access the information and request corrections or deletions), the customer dashboard proposal would significantly raise the risk of a breach of customer proprietary information by creating a new one-stop shop for hackers and pretexters.

**B. The Commission should extend the compliance deadlines for small providers by at least one year, with a subsequent rulemaking to determine whether to further extend the deadline and/or establish additional exemptions**

Regardless of the exemptions that the FCC adopts, it should extend the effective dates for small providers to comply with any new privacy and data security rules by at least one year

beyond any general compliance deadline, with a subsequent rulemaking to determine whether to further extend the deadline and/or establish additional exemptions. Because small providers have fewer resources, they require additional time to comply, particularly with a new comprehensive regime that differs in significant ways from the FTC's approach. Not only would these new rules impact providers, these new policies and procedures have the potential to disrupt customer expectations, particularly as customers are bombarded with new notifications and consent forms.

The FCC often has extended effective dates for small entities in the context of its consumer protection regulations. Last year, the Commission granted with conditions ACA's request to give certain analog-only cable systems more than a three-year waiver of the emergency information rule's compliance deadline.<sup>85</sup> In 2013, the Commission delayed compliance with the User Guide Requirements by two years, at which point certain mid-sized and smaller MVPD operators and small MVPD systems must comply with the requirements of Section 205.<sup>86</sup> In the *2015 Open Internet Order*, the FCC extended the compliance deadline for the enhanced transparency rule for small providers by one year, and subsequently granted a

---

<sup>85</sup> *Accessible Emergency Information, and Apparatus Requirements for Emergency Information and Video Description: Implementation of the Twenty-First Century Communications and Video Accessibility Act of 2010, Video Description: Implementation of the Twenty-First Century Communications and Video Accessibility Act of 2010*, MB Docket Nos. 12-107 and 11-43, Memorandum Opinion and Order, 30 FCC Rcd 5012 (rel. May, 26, 2015) (delaying the compliance deadline from May 26, 2015 to June 12, 2018).

<sup>86</sup> *See Accessibility of User Interfaces, and Video Programming Guides and Menus*, MB Docket No. 12-108, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 17330, ¶ 114 (2013). The extension applied to MVPD operators with 400,000 or fewer subscribers and MVPD systems with 20,000 or fewer subscribers not affiliated with an operator serving more than 10 percent of all MVPD subscribers. *See id.*

further one-year extension, after which it will determine whether to grant a permanent exemption from the rule.<sup>87</sup> Similarly, in the *2007 CPNI Order*, the FCC granted a six month extension to small providers to implement requirements in the order “to avoid disruption and inconvenience to consumers.”<sup>88</sup> In addition, the FCC granted extensions for smaller providers from its disabilities access rules, implementing a six-month extension for providers of advanced communications services to adopt technical, recordkeeping, and certification requirements required under the Communications and Video Accessibility Act.<sup>89</sup>

Here, the Commission is proposing to enact perhaps the most sweeping privacy and security regime in the U.S. regulatory landscape. These rules have the potential to be significantly more complex than the Open Internet enhanced transparency rule and the Commission’s *2007 CPNI Order*. While some of the proposed rules draw inspiration from existing rules, in whole, the proposed rules present something new, complex, and challenging for small providers. It will take a significant amount of time for these providers to hire or retrain staff; develop updated notifications, policies, and procedures; revisit and potentially modify existing relationships with agents, affiliates, vendors, and other third parties to comply with the rules; and comply with other aspects of the rules. It is vital that the Commission provide enough

---

<sup>87</sup> *2015 Open Internet Order* ¶ 24; *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, DA 15-1425 (rel. Dec. 15, 2015).

<sup>88</sup> *See in the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (2007 CPNI Order).

<sup>89</sup> *See In the Matter of Implementation of Sections 716 and 717 of the Communications Act of 1934, as Enacted by the Twenty-First Century Communications and Video Accessibility Act of 2010 et al.*, CG Docket No. 10-213 et al., Second Report and Order, 28 FCC Rcd 5957 (2013).

time for these entities to bring themselves into compliance. Therefore, an extension of at least one year from the adoption of new privacy and data security regulations is warranted.

Moreover, immediately following the adoption of any order and during the pendency of the one-year extension, the Commission should launch a rulemaking to examine whether one year is enough time and whether exemptions are necessary in some cases based on data and information provided by smaller entities about the specific rules as adopted. In this way, the Commission can revisit cost and burden questions in light of an adopted order, a refreshed record, and with the benefit of time and experience.

**C. The Commission should rationalize and streamline its proposed BIAS privacy and data security rules**

If the Commission does not adopt an “unfair or deceptive acts or practices” framework consistent with the Industry Proposal, it should rationalize and streamline its proposed rules to ensure that the rules are not too burdensome for small BIAS providers. Specifically, the Commission should (1) develop, with industry and other stakeholders, standardized notices that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and developers; (2) streamline its customer approval requirements to better align with consumer expectations and avoid disrupting existing customer relationships; (3) adopt a general data security standard and best practices rather than prescriptive data security requirements; and (4) tailor data breach notification requirements to ease burdens on BIAS providers.

**1. The Commission should develop standardized notices through a multi-stakeholder process that includes small provider representatives**

The Commission should develop standardized notices that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and

developers. These notices should include, at a minimum: privacy policy notices and material change notices; opt-out and opt-in customer approval forms; account change notifications; and data breach notifications. For providers that use the standardized forms, the Commission should provide a safe harbor from enforcement, to the extent such notices are not unfair or deceptive. By developing such notices, the Commission will reduce the need for small providers to rely on outside counsel to develop such policies, and by extension the cost of compliance.

The FCC has developed such standardized forms in the past. For example, the Commission has issued an easy-to-use standard template for its annual CPNI certifications<sup>90</sup> and developed standardized “nutrition label”-style forms for providers to use to comply with the Commission’s open Internet transparency rule.<sup>91</sup> Similarly, the National Telecommunications and Information Administration (NTIA) has undertaken several multi-stakeholder processes to develop standard privacy notices for mobile application privacy notices, cybersecurity, facial recognition, and unmanned aerial systems.<sup>92</sup> Moreover, the FTC has long used industry

---

<sup>90</sup> See Annual 47 C.F.R. ¶ 64.2009(e) CPNI Certification Template EB Docket 06-36, <http://apps.fcc.gov/eb/CPNI/>.

<sup>91</sup> See FCC, “FCC Unveils Consumer Broadband Labels to Provide Greater Transparency to Consumers, News Release (Apr. 4, 2016).

<sup>92</sup> See NTIA, Multistakeholder Process: Unmanned Aerial Systems (May 18, 2016), <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems>; NTIA, Privacy Multistakeholder Process: Facial Recognition Technology (Mar. 24, 2016), <https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology>; NTIA, Multistakeholder Process: Cybersecurity Vulnerabilities (Apr. 8, 2016), <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities>; NTIA, Privacy Multistakeholder Process: Mobile Application Transparency (Nov. 12, 2013), <https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency>.

workshops and information guidance to aid regulated entities in their compliance with Section 5 and its sector- and data-specific rules.

The Commission should develop these standardized notices through a multi-stakeholder process that includes small providers with a dedicated working group to address the issues of small and medium-sized providers. Due to limited resources, small providers are more likely than larger providers to avail themselves of standardized forms, and as such should play an integral role in any multistakeholder process. Further, the Commission should ensure that any resulting forms are flexible and tailored to the needs and unique obligations of small providers (i.e., reflecting any exemptions that the Commission adopts for small providers).

**2. The Commission should streamline its customer approval framework to align with customer expectations and promote innovation**

The Commission should streamline its customer approval requirements to better align with customer expectations and to promote innovative service offerings without burdening small providers.<sup>93</sup>

First, the Commission should abandon the artificial distinction between “communications-related services” and non-communications-related services in favor of a standard permitting the use and sharing of consumer data in any context consistent with consumer expectations. For well over a decade, BIAS providers have operated under the FTC’s Section 5 authority, which establishes a flexible privacy and data security framework. The FTC’s approach sets opt-out approval as the standard, and requires opt-in approval only for the most sensitive consumer data (e.g., health, financial, and children’s information). This framework has enabled all members of the Internet ecosystem to develop and provide innovative

---

<sup>93</sup> See NPRM ¶¶ 131, 151.

services to their customers. Indeed, the FTC itself recommends a more contextual approach than that proposed in the NPRM.<sup>94</sup> For BIAS providers, including ACA members, the FTC approach has enabled a proliferation of value-added services to the home, including home security systems, home automation systems, and other “connected” products that transit the BIAS network. Over time, consumers have come to expect that BIAS providers will offer them these services in conjunction with their BIAS service. For this reason, the Commission should permit BIAS providers to use customer proprietary information to provision (themselves or through their affiliates) non-BIAS data services and similar over-the-top services without obtaining additional customer approval, and to use or share customer proprietary information to market non-BIAS data services and similar over-the-top services subject to opt-out approval.

Second, the Commission should enable BIAS providers to obtain opt-out or opt-in customer approval at a time and in a manner that makes sense in context, including at the point of sale, at the point of installation, or before first use of the data for a purpose requiring consent. Under today’s CPNI rules, broadband providers may obtain customer consent to use CPNI at any time before they use the information, including at the point of sale. The FTC has recognized that the manner in which companies gain consent may differ in different contexts.<sup>95</sup> ACA members obtain consent in a variety of ways. Some prefer obtaining consent at the point of sale when the consumer has an opportunity to ask questions. In other cases—e.g., when enrollment occurs online or over the phone—it makes more sense to obtain approval during installation of BIAS equipment. The Commission’s proposal, however, would eliminate this flexibility, imposing a

---

<sup>94</sup> See 2012 FTC Privacy Report at 38.

<sup>95</sup> See *id.* at 50.

rigid rule that is inconsistent with current industry practices and consumer expectations. The Commission should return to a more flexible, context-based and consumer-friendly approach and continue to allow, but not mandate, customer approval at the point of sale and any other time that is consistent with customer expectations.

**3. The Commission should streamline its data security and data breach notification requirements through flexible standards**

It is axiomatic that there is no such thing as “perfect security.” For this reason alone, it is alarming that the Commission adopts rigid data security requirements with a “strict liability” breach notification standard that does not take into account consumer harm or reasonableness in light of company size and resources. If the Commission rejects the Industry Proposal, it should better align its proposed rules with those of other federal and state standards through flexible data security and data breach rules.

With respect to its data security requirements, the Commission should replace its specific data security rules (i.e., 64.7003(a)(1)-(5)) with best practices developed in conjunction with industry. Prescriptive rules quickly become obsolete, as security techniques evolve and new threats emerge to surmount them. Overly prescriptive rules raise, rather than reduce, the risk of a data security incident by requiring procedures that—in time—will be viewed as inadequate. A prime example of this phenomenon is the Commission’s 2007 authentication regime. While at the time the Commission viewed password protection as an adequate means of protecting user privacy, today it recognizes that such requirements may no longer be adequate.<sup>96</sup> Prescriptive data security rules will also harm consumers. For instance, prescriptive data security rules will harm competition and consumer choice by diverting limited resources from network deployment

---

<sup>96</sup> See NPRM ¶¶ 196-97.

and innovative service offerings to compliance. Further, the fact that the Commission’s proposal neglects the size of the company in its reasonableness determination effectively imposes a “strict liability” standard, which, when coupled with headline-grabbing enforcement actions, would ultimately hurt, rather than help, consumers.<sup>97</sup> An approach based on public-private partnership, best practices and voluntary action, coupled with the possibility of enforcement action if a company behaves unreasonably and this leads to consumer harm, provides the flexibility for companies to marshal their limited resources to adapt and respond effectively and efficiently to changing threats and privacy and security priorities.<sup>98</sup>

As for its data breach notification proposal, the Commission should take guidance from state legislatures and adopt flexible timeframes and limit breach notifications to situations where consumer harm is reasonably likely. First, the Commission should adopt an “as soon as

---

<sup>97</sup> As FTC Commissioner Maureen Ohlhausen stated in a recent speech, “[i]f an enforcement action imposes costs disproportionate to the actual consumer harm, that enforcement action may make consumers worse off if prices rise or innovation slows.” *See* FCC Commissioner Maureen K. Ohlhausen, *FTC-FCC: When is Two a Crowd?*, Remarks at 33<sup>rd</sup> Annual Institute on Telecommunications Policy & Regulation (Dec. 4, 2015).

<sup>98</sup> *See, e.g., NIST Cybersecurity Framework*, February 12, 2014 at p. 5 (discussing the importance of organizations prioritizing and making adjustments to their cybersecurity activities and expenditures, determining risk tolerance, and understanding the likelihood that an event will occur and the resulting impact). The information on the FCC’s overbroad list of customer proprietary information includes information that varies greatly. For example, the Federal Bureau of Investigation (FBI), in an April 2014 bulletin, noted that cybercriminals can sell partial electronic health records on the black market for \$50 each, but sell stolen social security card numbers or credit card numbers for \$1 each. *See* FBI Cyber Division Private Industry Notification, (U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, PIN #: 140408-009 (Apr. 8, 2014). It would be prudent for a company to take account of differences relevant to information the Commission identifies as customer proprietary information in setting priorities and determining how to proceed with its available resources. This is also a further reflection of why the FCC’s comparisons in the NPRM to a statute like HIPAA, which largely addresses some of the most highly sensitive and valuable personal information anywhere, is frequently inapposite.

reasonably practicable” standard for data breach notifications to promote complete and accurate breach reports to the Commission, law enforcement, and consumers. This standard would comport with the breach notification standards of the vast majority of states. Today, only eight states require notification within a specific time frame, and most of those states provide 45 days or more to provide notice.<sup>99</sup> These time frames recognize that breach response is a time- and cost-intensive activity, and for that reason puts the emphasis on getting it right rather than settling for an incomplete and potentially inaccurate picture of the breach (as the Commission’s rule would do).

Second, the Commission should limit breach notification to situations where there is a reasonable likelihood of consumer harm. This too aligns with the approach taken by the vast majority of states (41), which limit breach notification requirements to situations where there is actual harm or harm is reasonably likely.<sup>100</sup> Under this standard, good faith acquisition by an

---

<sup>99</sup> Conn. Gen. Stat. § 36a-701b(b)(1); Fla. Stat. § 501.171(3)(a); Me. Rev. Stat. Tit. 10, § 1348; Ohio Rev. Code § 1349.19(B)(2); 11 R.I. Gen. Laws § 11-49.3-4 [effective July 2, 2016]; Vt. Stat. tit. 9, § 2435(b)(1); Wash. Rev. Code § 19.255.010(16); Wis. Stat. § 134.98(3)(a).

<sup>100</sup> Alaska Stat. § 45.48.010(c); Ariz. Rev. Stat. § 44-7501(G); Ark. Code Ann. § 4-110-105 (2015); Colo. Rev. State. § 6-1-716 (2015); Conn. Gen. Stat. § 36a-701b(b)(1); Del. Code Ann. tit. 6, § 12B-102(a); Fla. Stat. § 501.171(4)(c); Haw. Rev. Stat. § 487N-1; Idaho Code § 28-51105; Ind. Code § 24-4.9-3-1; Iowa Code § 715C.2(6); Kan. Stat. § 50-7a01(h); Ky. Rev. Stat. § 365.732(1)(a); La. Stat. § 3074(G); Me. Rev. Stat. Tit. 10, § 1348(1)(B); Md. Code, Com. Law § 15-3504(b); Mass. Gen. laws ch. 93H, § 3; Mich. Comp. Laws § 445.72; Miss. Code Ann. § 75-24-29(3); Mo. Rev. Stat. § 407.1500(2)(5); Mont. Code Ann. § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-803; Nev. Rev. Stat. § 603A.220; N.H. Rev. Stat. Ann. § 359-C:20(I)(a); N.J. Stat. § 56:8-163(a); N.Y. Gen. Bus. Law § 899-aa(c); N.C. Gen. Stat. § 75-61(14); Ohio Rev. Code § 1349.19(B)(1); Okla. Stat. tit. 24, § 163(a); Or. Rev. Stat. § 646A.604(7); 73 Pa. Stat. Ann. § 2302; 11 R.I. Gen. Laws § 11-49.3-4(a)(1); S.C. Code Ann. § 39-1-90(A); Tenn. Code Ann. § 47-18-2107(a)(1); Utah Code § 13-44-202(1)(a); Vt. Stat. tit. 9, § 2435(d)(1); Va. Code Ann. § 18.2-186.6 (A); Wash. Rev. Code § 19.255.010(1); W. Va. Code § 46A-2A-102(a); Wis. Stat. § 134.98(2)(cm); Wyo. Stat. § 40-12-502(a).

employee, agent, or third party where there is no likelihood of consumer harm would not trigger a breach notification obligation, provided there is no reasonable likelihood that the disclosure will result in consumer harm. Moreover, limiting breach notifications to situations where consumer harm exists would benefit consumers. Specifically, limiting notifications in this way will decrease the chance of consumer notice fatigue while tying breach notifications with colorable actions that the consumer should take, including contacting credit agencies, banks, and other entities to reduce the risk of crime, fraud, or identity theft. Relatedly, the Commission should clarify that its breach notification rules do not apply to encrypted customer proprietary information, which is in line with the approach that 47 states and three territories have taken.<sup>101</sup>

Finally, the Commission should take steps to reduce the number of notifications that BIAS providers need to make. Specifically, it should create a one-stop shop for Commission and law enforcement notifications to avoid the need to duplicative notifications, and should preempt

---

<sup>101</sup> Alaska Stat. § 45.48.090(7); Ariz. Rev. Stat. § 44-7501(L)(6)(a); Ark. Code Ann. § 4-110-103(7); Cal. Civ. Code § 1798.82(h)(1); Colo. Rev. State. § 6-1-716(1)(d) (2015); Conn. Gen. Stat. § 36a-701b(a); Del. Code Ann. tit. 6, § 12B-101; Fla. Stat. § 501.171(1)(g)(2.); Haw. Rev. Stat. § 487N-1; Idaho Code § 28-51104(5); Ind. Code § 24-4.9-3-1; Iowa Code § 715C.1(11)(a); Kan. Stat. § 50-7a01(g); Ky. Rev. Stat. § 365.732(1)(a); La. Stat. § 3073(4)(a); Me. Rev. Stat. Tit. 10, § 1347(6); Md. Code, Com. Law § 15-3501(d)(1); Mass. Gen. laws ch. 93H, § 1; Mich. Comp. Laws § 445.72; Minn. Stat. § 325E.61(e); Miss. Code Ann. § 75-24-29(2)(a); Mo. Rev. Stat. § 407.1500(1)(9); Mont. Code Ann. § 30-14-1704(4)(b)(i); Neb. Rev. Stat. § 87-802(5)(a); Nev. Rev. Stat. § 603A.040, N.H. Rev. Stat. Ann. § 359-C:19(IV)(a), N.J. Stat. § 56:8-161, N.Y. Gen. Bus. Law § 899-aa(b); N.C. Gen. Stat. § 75-61(14); N.D. Cent. Code § 51-30-01(4)(a); Ohio Rev. Code § 1349.19(A)(7)(a); Okla. Stat. tit. 24, § 162(6); Or. Rev. Stat. § 646A.604(11)(a); 73 Pa. Stat. Ann. § 2302, 11 R.I. Gen. Laws § 11-49.3-3(a)(8) [Effective July 2, 2016]; S.C. Code Ann. § 39-1-90(D)(3); Tenn. Code Ann. § 47-18-2107(a)(3)(A); Tex. Bus. & Com. Code § 521.002(a)(1); Utah Code § 13-44-102(3)(a); Vt. Stat. tit. 9, § 2430(5)(A); Va. Code Ann. § 18.2-186.6 (A); Wash. Rev. Code § 19.255.010(1); W. Va. Code § 46A-2A-101(6); Wis. Stat. § 134.98(1)(b); Wyo. Stat. § 40-12-501(a)(vii); 9 Guam Code Ann. § 48.20(f); P.R. laws Ann. tit. 10, § 4051(a); and V.I. Code Ann. tit 14 § 2208(e).

state data breach notification laws entirely. By reducing the number of government-level notifications that BIAS providers must make from over 50 notifications to a single notification, the Commission will significantly reduce the costs that BIAS providers must assume in the event of a breach while preserving the benefits of notifications to the customer.

## **VII. THE COMMISSION SHOULD HARMONIZE ITS PRIVACY AND DATA SECURITY REQUIREMENTS FOR VOICE AND BIAS, BUT SHOULD NOT HARMONIZE ITS CABLE PRIVACY RULES**

At several points in the NPRM, the Commission seeks comment on whether and how to “harmonize” its proposed BIAS privacy and data security rules with its existing privacy regimes for voice, cable, and satellite services.<sup>102</sup> While ACA supports the concept of creating a single privacy and data security framework for providers of multiple services as a means of reducing compliance burdens and consumer confusion, it is concerned that, in practice, a single set of rules could increase the burdens on small providers, heighten consumer confusion, and contravene statutory language and legislative intent. For this reason, the Commission should only harmonize *within* specific statutory provisions, and not *across* statutory provisions; and should avoid any rule changes that would increase the burdens of existing rules on small providers or their customers. Specifically, the Commission should limit its harmonization to Section 222 of the Act, and should not use this rulemaking proceeding to impose new and unfamiliar rules on cable service.

With respect to Section 222, the Commission should adopt a single set of rules that apply to voice and broadband service. As explained above, while ACA members diligently comply with Section 222 and its regulations, the existing voice requirements already are enormously

---

<sup>102</sup> See NPRM ¶¶ 103-105, 152, 254.

complex and burdensome. Superimposing yet another regulatory framework on Section 222 would only add to the significant legal, administrative, and technical costs that small providers face, particularly if the rules would require them to obtain separate approvals, provide separate notices, and conduct separate or more nuanced trainings to differentiate between the voice and BIAS rules. For that reason, ACA submits that the Commission should harmonize its Section 222 voice and BIAS rules by adopting the Industry Proposal for both voice and BIAS service. In this way, the Commission can bring its voice rules in line with the existing and successful FTC framework, which consumers have come to expect for the rest of the innovation economy. Moreover, adopting the Industry Proposal for voice services will further reduce compliance costs for small providers while continuing to promote the values underlying this proceeding. Alternatively, if the Commission declines to adopt the Industry Proposal, it should harmonize its voice rules and BIAS rules by adopting targeted exemptions and exceptions consistent with ACA's proposals in Sections V and VI above.

At the same time, the Commission should not harmonize its proposed BIAS rules under Section 222 with the separate and distinct requirements of Section 631. Like Section 222, Section 631 is a comprehensive, standalone privacy framework. Unlike Section 222, however, Section 631 imposes very specific notice, consent, access, disposal and enforcement rights and duties, which are interpreted and enforced by the courts, not by the Commission. Under this framework, Section 631 has protected the rights of cable subscribers for over 30 years without the need for regulatory intervention. The Commission should not now undermine established business practices and consumer expectations by imposing new regulations on cable service, particularly if the result would be to impose the Commission's heightened notice, consent, and data security requirements on cable operators.

## **VIII. CONCLUSION**

ACA members have worked strenuously to preserve the trust of their consumers through reasonable privacy and data security protections, and have achieved an excellent record of compliance. The Commission's proposals would impose onerous, costly, and unnecessary privacy and data security regulations that would harm competition, investment, innovation, and the customer-carrier relationship.

To ease the burdens on small providers and their customers, the Commission should adopt rules consistent with the FTC's successful and flexible "unfair or deceptive acts or practices" framework, as set forth in the Industry Proposal.

If the Commission instead adopts an *ex ante*, prescriptive framework more in line with the NPRM proposal, it should mitigate the costs and burdens of compliance through targeted small provider exemptions and extensions, streamlined and rationalized rules, and harmonization of voice and broadband rules under Section 222.

Respectfully submitted,



By: \_\_\_\_\_

Matthew M. Polka  
President and Chief Executive Officer  
American Cable Association  
Seven Parkway Center  
Suite 755  
Pittsburgh, PA 15220  
(412) 922-8300

Thomas Cohen  
John J. Heitmann  
Jameson J. Dempsey  
Kelley Drye & Warren LLP  
3050 K Street, NW  
Washington, DC 20007  
(202) 342-8518

Ross J. Lieberman  
Senior Vice President of Government Affairs  
American Cable Association  
2415 39th Place, NW  
Washington, DC 20007  
(202) 494-5661

May 27, 2016