Prepared Written Statement of Matthew M. Polka,
President and CEO, American Cable Association

Before the United States Senate Committee on Commerce, Science, and Transportation

"How Will the FCC's Proposed Privacy Regulations Affect Consumers and Competition?"

July 12, 2016

Thank you, Chairman Thune, Ranking Member Nelson, and Members of the Committee, for inviting me to testify on behalf of the American Cable Association (ACA) and its members about the steps we are taking to protect the privacy and security of our customers' personal information and our thoughts on the Federal Communications Commission's (FCC's or Commission's) proposed privacy and data security rules for broadband Internet access service (broadband service).

In my testimony, I will focus on four points. First, ACA members are already subject to a host of privacy and data security obligations, take those obligations seriously, and have an excellent track record of compliance. Because they too are consumers, ACA members understand consumers' expectations and the need for privacy protections. Second, to best serve the interests of broadband consumers, the FCC should adopt a privacy and data security framework that is consistent with the Federal Trade Commission's (FTC's) approach, which has proven valuable and workable for all interests. Third and most unfortunately, we fear that the FCC's proposed privacy and data security rules would impose needless, unduly burdensome

obligations on smaller broadband providers, chilling investment and innovation, all with little consumer benefit. And finally, if the FCC nonetheless proceeds and adopts rules in line with its proposals, it should ease the burdens on small providers by providing tailored exemptions, extending compliance deadlines, and streamlining its rules.

I. BACKGROUND ON ACA'S MEMBERS

ACA represents approximately 750 small and medium-sized cable operators, incumbent telephone companies, municipal utilities, and other local providers, which provide service in all fifty states. ACA members provide a variety of services to their residential and business customers, including voice, cable service, broadband, and various non-common-carrier services, such as home security, PC support, e-mail, and data center services. Eighty percent of ACA members serve fewer than 5,000 subscribers, and roughly fifty percent serve fewer than 1,000 subscribers. Half of ACA's members have ten or fewer employees, with typically just one or two engineers or individuals with technical expertise, and these employees perform many duties within their companies. Few have in-house personnel dedicated to privacy and data security compliance. Yet, they take all necessary steps to comply with today's regulatory mandates, even though it is a challenge and cuts into their ability to upgrade systems and to offer new products and services.

Consequently, ACA urges Congress and the Commission to continue to seek to balance actions that would impose new obligations with the resource capabilities of smaller providers. Skewing that balance against broadband providers—as the Commission proposes to do—imperils investments in high performance networks and information services so critical for consumers and our economy.

II. ACA MEMBERS ARE ALREADY SUBJECT TO A HOST OF PRIVACY AND DATA SECURITY RULES, TAKE THOSE OBLIGATIONS SERIOUSLY, AND HAVE AN EXCELLENT TRACK RECORD OF COMPLIANCE

ACA members must comply and have complied with numerous privacy and data security obligations, several of which were the work of this Committee. ACA members that provide cable service must comply with Section 631 of the Cable Communications Policy Act of 1984 (the Cable Act).[1] 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 of 1934, and its implementing rules related to customer proprietary network information (CPNI).[2] ACA members that provide broadband service must comply with the FCC's transparency rule (which requires disclosure of privacy policies), and since the *2015 Open Internet Order*, the FCC has asserted that they must comply with Section 222 (notwithstanding ongoing challenges to the agency's authority to do so). ACA members that provide non-common-carrier information services, a term which until recently applied to broadband service, must also comply with Section 5 of the Federal Trade Commission Act,

[1] Cable operators have been subject to Section 631 for over 30 years. Section 631 includes a robust set of requirements, including annual subscriber notices, a customer consent framework, access rights, and a private right of action.

[2] Section 222 and its implementing rules are designed to protect the confidentiality of individually identifiable CPNI, a narrow category of information that includes information about a customer's use of the network (e.g., call detail records) and information contained within customer bills. The CPNI rules include a three-tiered notice and consent regime, data security safeguards, a breach notification rule, and annual certifications. Beginning in 2014, the FCC began to read Section 222 more broadly to protect "customer proprietary information," a category of information that according to the FCC includes both CPNI as well as all personally identifiable information. ACA and others have challenged the Commission's broad interpretation of the statute as unlawful.

which prohibits "unfair or deceptive acts or practices," including those related to privacy and data security. Further, our members are subject to the laws and rules of the states in which they operate, including but not limited to data breach notification laws.[3] In addition, to the extent that they 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.

Complying with all of these privacy and data security laws is a significant burden for smaller providers, but they understand their responsibilities and have taken the necessary steps to ensure they comply. ACA members notify their subscribers of their privacy practices through welcome packages, annual notifications, and website privacy policies. Our members also provide opportunities for customers to make choices about how service providers use or share their information and give all the necessary information to make an informed choice. They 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 service companies—protect the confidentiality of customer information.

[3] Every state has a law prohibiting deceptive practices, and most have laws prohibiting unfair practices, similar to the FTC's Section 5 prohibition. *See, e.g.*, Conn. Gen. Stat. § 42-110b(a); Fla. Stat. Ann. § 501.204; Mass. Gen. Laws Ch. 93A, § 2(a); S.D. Codified Laws § 37-24-6(1). Further, 47 states have enacted data breach notification laws. *See, e.g.*, Conn. Gen Stat. § 36a-701b; Fla. Stat. §§ 501.171, 282.0041, 282.318(4)(j)(1); Mass. Gen. Laws § 93H-1 *et seq*. Moreover, several states have enacted additional privacy and data security requirements. *See, e.g.*, Fla. Stat. § 501.171; 201 CMR 17.00. For example, Massachusetts requires companies to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards," with granular requirements that every such information security program must include. *See* 201 CMR 17.00.

ACA members employ reasonable physical, technical, and administrative data security 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, our members are responsible in their duties to comply with the recordkeeping and reporting obligations of the FCC'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. We have been active in the FCC's Communications Security, Reliability and Interoperability Council Working Group IV proceeding, which is intended to assist companies with implementing voluntary cybersecurity measures for the communications sector that respect the unique challenges that small and medium-sized providers face.

The privacy and data security actions described above and others that smaller providers undertake 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.

ACA members have an excellent track record in protecting the confidentiality of their customers' information and complying with privacy and data security laws and rules. Indeed, 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 smaller broadband provider for the sorts

of privacy and data security practices that the FCC seeks to regulate pursuant to its proposals. Such a long run free of major incidents reinforces the view that a new and more intrusive privacy and data security regime is not needed to protect consumers.

III. TO BEST SERVE THE INTERESTS OF BROADBAND CONSUMERS, THE FCC SHOULD ADOPT A PRIVACY AND DATA SECURITY FRAMEWORK THAT IS CONSISTENT WITH THE FTC'S APPROACH, WHICH HAS PROVEN VALUABLE AND WORKABLE FOR ALL INTERESTS

Until the FCC classified broadband service as a Title II telecommunications service in the *2015 Open Internet Order*, all industry participants in the Internet ecosystem were subject to the jurisdiction of the FTC. The FTC's approach combines a flexible statutory provision—Section 5 of the FTC Act—with heightened obligations for limited categories of sensitive information (e.g., children's information, health information, or financial information). As such, the FTC's approach has at its core the concepts of flexibility, context specificity, and technological neutrality. This framework has enabled the Internet ecosystem to flourish to the benefit of consumers, edge providers, and broadband providers alike. Further, by avoiding hyper-prescriptive rules and focusing instead on the reasonableness of providers' practices and the truthfulness and completeness of their representations to their customers, the FTC's framework lessens the compliance burdens on smaller providers.

In contrast, the FCC proposes to cleave the Internet ecosystem in two by subjecting one set of participants—broadband providers—to a different and more burdensome privacy and data security regime, while another set—including edge providers—remain subject to the FTC's approach. The FCC is proposing these rules despite the fact that the large edge providers can know more about a user's activity and, unlike broadband providers, often employ business models that depend on the collection, use, and sharing of their customers' personal information. For smaller broadband providers, which lack scale, such business models are rarely in our members' strategic plans.

In advance of the FCC issuing its proposals, ACA and several trade associations proposed a framework that would protect consumers and promote the FCC's goals of transparency, choice, and data security while retaining consistency with the FTC's framework. Such an approach would protect consumers 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, FTC staff has stated that "any privacy framework [for broadband providers, operating systems, browsers, and social media] should be technology neutral," and has argued that the FCC's failure to propose a consistent privacy regime is "not optimal."

We recommended that to maintain consistency with the FTC's framework, the FCC should adopt rules based on the following principles:

- **Transparency.** A broadband (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 broadband 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, broadband 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 broadband 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. 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.** A broadband provider 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. Broadband providers have flexibility to determine how and when to provide such notice.

Our proposal would meet consumers' privacy needs while allowing them to take advantage of products and services they expect from their service provider and would avoid inconsistent and burdensome oversight. Moreover, it would ensure a level playing field between edge providers and broadband providers, promoting an innovative and competitive broadband ecosystem.

Our proposal also would improve the ability of smaller providers to comply without incurring undue costs or other burdens. As I explained earlier, smaller providers work to ensure that they use customer information consistent with their customers' expectations. Since these providers are already familiar with the FTC framework, they would not have to incur material additional costs to bring their policies, processes, and systems into compliance if the FCC adopts rules consistent with this framework.

Our proposal also is superior because the consumer choice provisions align with consumer expectations by respecting the context of customer-carrier interactions. This will

enable small providers to offer new and innovative services to their customers, increasing consumer choice and competition.

The data security rule in our proposal also contains a robust general security standard that requires "physical, technical, and administrative" security safeguards while including the size of the company as a factor in determining whether particular safeguards are reasonable. As such, in the event that smaller providers grow, the rules will require more sophisticated processes commensurate with their larger operations. Additionally, our framework enables the FCC to establish best practices through multi-stakeholder processes.

Finally, our proposed data breach notification rule is superior to the FCC's 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.

IV. THE FCC'S PROPOSALS WOULD NEEDLESSLY IMPOSE UNDULY BURDENSOME AND COSTLY RESTRICTIONS ON SMALL PROVIDERS, CHILLING INVESTMENT AND INNOVATION WITH MINIMAL ADDITIONAL CONSUMER BENEFIT

The FCC proposes a set of privacy and data security rules that, if adopted, would be one of the most complex in the United States. Let me highlight just some of the new notice, customer approval, data security, and data breach notification obligations the FCC proposes to impose on smaller broadband providers.

- **Proposed Notification Rules.** The proposed notification rules would prescribe, in minute detail, when, where, how, and how often providers must notify their subscribers about their privacy and data security practices, which would require smaller providers incur legal costs to draft and update privacy notices, administrative costs to deliver the notices, and technical costs to post the notices "persistently" on the provider's website, mobile app, and any functional equivalent.

- **Proposed Customer Approval Rules.** The proposed customer approval rules would replace the long-standing, context-specific, and consumer-friendly opt-out regime of the FTC with an incredibly complex and restrictive three-tiered framework that would erect unnecessary barriers to collecting, using, or sharing customer information by requiring opt-in consent in many situations that are well within consumer expectations.

- **Proposed Data Security Rules.** The proposed data security rules would replace the FTC's reasonable security standard with a general strict liability rule requiring providers to "ensure" the confidentiality, security, and integrity of customer information, irrespective of the sensitivity of that information and ignoring the fact that most agencies recognize that there is no such thing as perfect security. The proposed data security rules also would impose exacting operational requirements on broadband providers, such as: requiring regular risk management assessments; appointing "senior officials" to oversee providers' privacy and data security practices; implementing third party oversight mechanisms; and conducting training for personnel, agents, and affiliates.

- **Proposed Data Breach Notification Rules.** The proposed data breach notification rules would impose a strict, seven-day turnaround time from discovery of the breach to notify the FCC and law enforcement about any data breach, and a ten-day turnaround for notifying affected customers, regardless of whether the breach was intentional or whether consumer harm is reasonably likely. The result of this proposed breach notification rule will be over-notification, often including incomplete or evolving facts, which will confuse consumers, breed unnecessary distrust in the Internet ecosystem, and work to undermine the "virtuous circle" of demand for Internet services, deployment of broadband infrastructure, and innovation.

Unlike the existing CPNI rules, the proposed rules would not be limited to "customer proprietary network information"—the narrow set of information that Section 222 was drafted to address—but rather would apply to all "customer proprietary information," a broad, amorphous term that appears nowhere in the Communications Act and covers everything from the make and model of a user's modem to an individual's public demographic information. Further, unlike the existing CPNI rules, the proposed rules would apply to all past, present, and prospective customers of a broadband provider. The FCC even seeks comment on whether to expand the definition of customer to include minors, members of a group plan, or other

individual users who can access a shared account. By extending the universe of covered information and individuals, smaller providers will need to manage significantly more information, dramatically increasing the costs and burdens of compliance.

To meet all of these new, extensive obligations, smaller broadband providers would need at least to:

- Develop and implement new data security controls, website policies, and customer approval tracking systems;
- Hire and train dedicated privacy and data security staff;
- Provide additional customer notices, including data breach notifications that would increase customer confusion and "notice fatigue";
- Retain attorneys and consultants for such activities as regulatory analysis, contract negotiation, risk management assessments, and preparing required policies, forms, training, and audits;
- Ensure compliance for call centers, billing software, and others that interface with customer proprietary information; and
- Divert scarce resources from innovation and infrastructure deployment to regulatory compliance.

These new costs would be most burdensome for smaller providers, decreasing their ability to innovate, upgrade systems, and compete while increasing costs, confusion, and inconvenience for their customers. Indeed, the Office of Advocacy for the Small Business Administration (SBA) told the FCC that its "proposed rules will be disproportionately and significantly burdensome for small Broadband Internet Access Service (BIAS) providers," arguing that "the FCC failed to comply with the [Regulatory Flexibility Act's] requirement to quantify or describe the economic impact that its proposed regulations might have on small entities," and "[t]he FCC has provided no estimate of the paperwork hours required to comply with the regulations."

V. IF THE FCC ADOPTS ITS PROPOSED RULES, IT SHOULD TAKE STEPS TO EASE THE BURDEN ON SMALLER PROVIDERS THROUGH EXEMPTIONS TO THE MORE ONEROUS ELEMENTS OF THE RULES, EXTENSIONS OF THE APPLICABLE COMPLIANCE DEADLINES, AND STREAMLINED REGULATIONS

If the FCC rejects our proposal in favor of its prescriptive, *ex ante* privacy and data security framework, it should, consistent with similar privacy regimes:

- Exempt smaller providers from prescriptive specific data security requirements (while maintaining a flexible general data security standard) and add "the size of the BIAS provider" to the factors that the FCC must consider when assessing the reasonableness of a BIAS provider's security program;

- Exempt smaller providers from the more onerous elements of its customer approval framework by grandfathering existing customer consents and exempting smaller providers from the requirement to obtain additional approval where they do not share sensitive personal information with third parties for marketing purposes;

- Exempt smaller providers from several elements of the FCC's proposed data breach notification rule (as applied to voice and broadband services) by exempting smaller providers from the specific notification deadlines in favor of an "as soon as reasonably practicable" standard; and

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

These exemptions address and reduce the burdens that the proposed privacy rules would have on smaller providers, and align with the SBA Advocacy Office's request that the FCC adopt "exemptions for small BIAS providers wherever practicable."

The FCC also should extend the deadlines for smaller providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline (i.e., the date at which larger providers must comply with the rules). The FCC should commit to initiate a subsequent rulemaking together with or immediately after any order that results from this proceeding to determine whether to further extend the deadline and/or establish additional exemptions, and should further commit to rule on whether to extend the deadline or

establish additional exemptions prior to the expiration of the general compliance deadline. The FCC often has extended effective dates for small entities in the context of its consumer protection regulations, including: (1) a three-year waiver for certain analog-only cable systems to comply with the emergency information rule; (2) a two-year delay to comply with the User Guide Requirements of the FCC's accessibility rules; (3) a one-year extension of the compliance deadline for the FCC's open Internet enhanced transparency rule, which it subsequently extended for another year; and (4) a six-month extension to implement requirements of the *2007 CPNI Order*.

Moreover, the FCC should rationalize and streamline its proposed rules to ensure that they are not too burdensome for smaller broadband providers by:

- Developing, with industry and other stakeholders, standardized notices with safe harbor protection that small providers can use to reduce enforcement risks, as well as the need to pay for outside counsel, consultants, and developers;
- Streamlining its proposed customer approval requirements to better align with consumer expectations and avoid disrupting existing customer relationships;
- Adopting a general data security standard and working with industry to establish and update best practices rather than imposing prescriptive data security rules;
- Tailoring any data breach notification requirements to ease burdens on broadband 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; and
- Harmonizing its rules *within* Section 222, but not across statutory provisions including Section 631 of the Cable Act, which would undermine consumer expectations and would upend providers' existing compliance regimes.

While a suite of extensions, exemptions, and rationalized rules would not be as effective as adopting rules consistent with the FTC framework, it would address the concerns of smaller

providers and many others in the record—including the SBA—that the FCC's proposed rules go too far without adequately considering the burdens of its proposals on smaller providers.

ACA members have a strong record of protecting consumer data and complying with myriad state and federal privacy and data security laws. Based on this experience, we urge the Commission to adopt the time-tested privacy framework employed by the FTC. It has proven valuable for consumers and imposes important but reasonable obligations on smaller broadband providers. We look forward to working with the Committee and the Commission as this process moves forward.