BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
WASHINGTON, DC

Developing the Administration's Approach to Consumer Privacy	))))	Docket Number 180821780-8780-01 RIN 0660-XC043

COMMENTS OF THE AMERICAN CABLE ASSOCIATION ON THE PUBLIC NOTICE

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

Thomas Cohen
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
(202) 342-8518
Counsel to American Cable Association

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

November 9, 2018

TABLE OF CONTENTS

BEFORE THE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
WASHINGTON, DC

Developing the Administration's Approach to Consumer Privacy	))))	Docket Number 180821780-8780-01 RIN 0660-XC043

COMMENTS OF THE AMERICAN CABLE ASSOCIATION
ON THE PUBLIC NOTICE

I. Introduction and Summary

The American Cable Association ("ACA") hereby comments on the Notice issued by the National Telecommunications and Information Administration ("NTIA") requesting comments on "Developing the Administration's Approach to Consumer Privacy."[1] ACA represents more than 700 smaller providers of broadband, video, and telephony services passing some 18 million households and serving almost 7 million.[2] Half of ACA members serve fewer than 1,000 subscribers and have 10 or fewer employees. In offering these services, smaller providers are subject to a number of federal privacy statutes.[3] For video and telephony services, they must

1 *Developing the Administration's Approach to Consumer Privacy*, NTIA, 83 Fed. Reg. 48600 (Sept. 26, 2018) ("*Notice*").

2 For additional information about ACA, *see* www.americancable.org. *See also* "Connecting Hometown America, How the Smaller Operators of ACA are Having a Big Impact" (2014), which elaborates on the characteristics and activities of smaller video and broadband providers who are ACA members, available at http://www.americancable.press/files/140328%20ACA_Whitepaper_PDF%20(FINAL).pdf.

3 Throughout these comments, when referring to privacy statutes or issues, ACA includes data security as well.

comply with, respectively, the cable services privacy and customer proprietary network information ("CPNI") provisions of the Communications Act of 1934[4] overseen by the Federal Communications Commission ("FCC"). Internet Service Providers ("ISPs") are subject to the "unfair or deceptive acts or practices" provision in Section 5 of the Clayton Act overseen by the Federal Trade Commission ("FTC"), and state (mini-FTC) privacy laws.[5]

Over the many years they have been subject to these laws, smaller providers have demonstrated an exceptional record of commitment to protecting their customers' privacy and compliance with the laws, driven in part by the fact that they live and work in the communities they serve and value protecting their neighbors' privacy. They recognize the importance of gaining their customers' trust and have spent years earning it.

Smaller ISPs also generally lack the ability to easily monetize their subscribers' information because of their limited scale (*e.g.,* customer base and financial and human resources), even if they had an interest in doing so. Thus, it is rare that any smaller ISP poses a significant threat to misusing their subscribers' information. By contrast, Internet Providers like Google and Facebook base their business models on collection from and use of their billions of users' information, often directly or by sharing it with third-party vendors.

Smaller providers also know that the way they and other providers collect, use, and share personal data from customers has changed, and will change, over time. Moreover, they have seen how a relatively light-touch regulatory regime accounts for their subscribers' privacy interests while not imposing undue burdens on smaller providers. Accordingly, they have urged federal and state governments to generally refrain from imposing highly prescriptive and

---

4 47 U.S.C. §§ 551, 222.

5 When offering broadband Internet access service, providers are referred to as "Internet Service Providers." In addition, many other firms operate in the Internet ecosystem, including upstream content, applications, and services providers, often called "edge providers." In these comments, we refer to all firms operating in the Internet ecosystem as "Internet Providers."

inflexible requirements that can become quickly outdated, imposing burdens without any benefits.

Even while recognizing consumers have a legitimate interest in protecting the privacy of their information, smaller providers find that it is a significant burden to comply with many different legal requirements and fear that federal or state governments will add to this load. Make no mistake, these laws, even when serving an important public interest, impose costs, which reduce free cash that providers can invest in infrastructure. And, at their worst, onerous or vague legal requirements can deter providers from rolling out service offerings that consumers want. Moreover, unlike larger providers, which are more able to withstand the weight of new and extensive laws and regulations, smaller providers lack the scale and resources to simply spread the cost of these additional burdens across their customer base. Thus, while smaller providers agree that consumers should have meaningful privacy protections, these protections need to be reasonable, matching the problems they are designed to solve, and scaled to the size of the provider.

In these comments, ACA addresses development of a national privacy policy from the perspective of smaller providers. In particular, ACA agrees that a national privacy framework, one that establishes rules that are competitively and technology-neutral and apply uniformly across the country, is valuable and necessary so that consumers can understand and act on their rights regardless of the entity accessing their personal information. By contrast, a patchwork of different state privacy laws will impose substantial costs on smaller providers to understand and comply with any requirements. In addition, by having uniform rules, a national framework provides businesses with greater certainty, which will facilitate investment and deployment of new services. ACA also believes that such a framework should be based on the existing risk-based approach, which will protect the reasonable privacy expectations of consumers, and recognize that collection, use, and sharing practices will constantly evolve as

innovative and beneficial services are deployed. Finally, the framework should be scaled so as not to unreasonably burden smaller providers.

II. Smaller Providers and Government Regulation of Privacy and Data Security

In the Notice, NTIA asks for comment on ways to achieve a delicate policy balance—advancing consumer privacy while protecting prosperity and innovation[6]—and to achieve that balance in an ever-changing market. Before delving into substance, there are several fundamental objectives that should shape any Internet privacy policy regime:

- The regime should apply uniformly across all jurisdictions on a competitively and technology-neutral basis.
- The regime should apply a risk-based flexible approach.
- The regime should be tailored to the more limited capabilities and resources of smaller providers and their customers.

A. Federal privacy requirements should be uniform, overseen by the Federal Trade Commission, and apply on a competitively and technology-neutral basis.

To provide consumers with a consistent "privacy" experience and to further competition, all firms operating in the Internet ecosystem ("Internet Providers")[7] should be subject to the same privacy requirements overseen only by the FTC, the federal agency that has the most experience and expertise with privacy oversight. The Internet is inherently interstate, with consumers accessing information and other content and purchasing services from firms based in other states which are transmitted over networks that traverse different states at different times.[8] And, with consumers increasingly using mobile devices to engage in Internet commerce, they often make purchases from different jurisdictions, even on the same day.

---

6 *Notice* at 48600.

7 As discussed below, the regime should be tailored for smaller firms.

8 *Restoring Internet Freedom*, Declaratory Ruling, Report and Order, and Order, FCC, 33 FCC Rcd 311, 430 (Dec. 14, 2017) ("*Restoring Internet Freedom Order*").

Moreover, many firms operating in the Internet ecosystem offer similar services to consumers and have access to similar types of consumer information regardless of whether they are ISPs or upstream edge providers. Further, given that the Internet is dynamic, firms are certain to evolve their offerings and consumers are certain to alter their behavior, both of which are virtually certain to engender, if permitted, scores of statutes and regulations that conflict in application, requirements, and enforcement. For all these reasons, it is essential to have a single, albeit evolving, set of privacy requirements that are overseen by a single federal agency.

By contrast, the FCC's *Privacy Order*,[9] which was flawed in many respects, made the fatal error of singling out ISPs for different, much more onerous oversight rather than include all Internet Providers.[10] The FCC erroneously assumed that ISPs "hold a unique position in the Internet ecosystem" that necessitates prescriptive rules to "bolster consumer trust."[11] Yet, nowhere was the FCC presented with evidence of actual consumer harm or of evidence that adopting rules that depart from the FTC's regime would bolster consumer trust. Instead, the FCC merely relied on its assumption that "consumers fearful of the loss of privacy may be less likely to use broadband connectivity,"[12] and it heavily discounted evidence demonstrating that ISPs are good stewards of their customers' data, with most simply lacking the incentives or

---

9 The Order, which was adopted in 2016, was repealed by Congress in 2017. S.J. Res. 34, Pub. L. No. 155-22, 115th Cong. (2017).

10 The FCC's rationale for singling out ISPs was based upon its *2015 Open Internet Order*'s finding that ISP are providing telecommunications services and the CPNI statute only applies to telecommunications services providers. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC, 31 FCC Rcd 13911, 13918-19 (Oct. 27, 2016) ("*Privacy Order*"). That fact, however, does not mean that the FCC could not have harmonized its regulations with the FTC's framework, which is what ISPs requested. The FCC explicitly eschewed any effort to harmonize its regulations with the FTC's framework. *See id.* at 13919.

11 *Id.* at 13924.

12 See *id.* at n.62 (citing *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion*, 2016 Broadband Progress Report, FCC, 31 FCC Rcd 699, 751-52 (Jan. 28, 2016)).

resources to engage in the sorts of sophisticated data analytics that the FCC feared.[13] Even worse, the FCC failed to attribute even these unsupported and sweeping suggestions of consumer fear about privacy to the actions of ISPs, as opposed to edge providers or other players in the Internet ecosystem.

The California Consumer Privacy Act of 2018 ("CCPA")[14] at least applies to all, but the smallest, Internet Providers. However, apart from correctly including all types of market participants, the CCPA—or for that matter, any state statute—is flawed because the Internet is inherently a national (if not international) market and not a mere aggregation of individual state and local markets. As such, having multiple state privacy regimes would confuse consumers, burden providers, and greatly increase marketplace friction, leading to higher costs for service and less innovation. Moreover, the burden of having to comply with multiple regulatory regimes would fall heaviest on smaller providers and new entrants, which lack the operational and legal resources required to comply with numerous, different regulations. Thus, if individual state regulations are permitted to override or work in conjunction with a national regime, consumers in markets served by smaller providers would likely have access to fewer services, and markets served by new entrants that operate in multiple states would likely be less competitive.[15] In both instances, larger incumbent firms, which can more easily absorb the costs of regulation, would benefit.

---

13 *See, e.g.*, *Ex Parte* Letter from Patricia Cave, Director Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2-3 (Aug. 22, 2016); Reply Comments of the Rural Wireless Association, Inc., WC Docket No. 16-106 at 2-3 (July 6. 2016).

14 Cal. Civ. Code §§ 1798.100 *et seq*.

15 Noah Phillips, Commissioner, FTC, *Keep It: Maintaining Competition in the Privacy Debate*, Prepared Remarks at the Internet Governance Forum USA at 2 (July 27, 2018) ("Phillips Speech").

In sum, any privacy regime NTIA adopts should establish a single, national regulatory regime overseen by the FTC that applies to Internet Providers regardless of their competitive position or the technology they use.[16]

B. US privacy policy should continue to be based on a risk-based approach.

The risk-based approach to privacy policy that the US Congress and federal agencies have employed for decades imposes different requirements on firms depending upon the type of information being protected, the nature in which the information is used, and the entity collecting, using, and sharing the information. For instance, the US Congress has determined that strict privacy requirements should be applied to the collection and security of health and financial-related information,[17] as well as information collected from children,[18] while the collection of less-sensitive online data warrants less rigorous rules. In effect, a risk-based approach imposes requirements where "the greatest privacy need exists, limiting such costs where the need is less."[19] The Notice explains that risk-based flexibility underlies the Administration's policy approach because it "believes that users should be able to benefit from dynamic uses of their information, while still expecting organizations will appropriately minimize risks to users' privacy."[20]

---

16 By contrast, *see* Statement of Laura Moy, Executive Director, Center on Privacy & Technology at Georgetown Law, Before the S. Comm. on Commerce, Science, & Transportation, *Hearing on Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act* at 15 (Oct. 10, 2018) ("[F]ederal legislation should a establish a floor…thus allowing states to continue to pass stronger laws on their own."). ACA opposes such an approach because it would continue to subject providers to different requirements, engendering the problems discussed above and undermining the value of having a single set of rules applicable to all Internet Providers and their customers.

17 *See e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

18 *See e.g.*, Children's Online Privacy Protect Act of 1998, 15 U.S.C. §§ 6501-6506.

19 *See* Phillips Speech at 5.

20 *Notice* at 48600.

ACA believes the risk-based approach should continue and be at the heart of a comprehensive federal policy setting forth baseline privacy protections. Such an approach will focus privacy protections and enforcement actions on those practices where misuse of consumer data will cause the greatest harm, while limiting compliance burdens where there is little benefit and enabling use of data for productive purposes. Further, any such approach would recognize the dynamic nature of data collection and use practices.[21]

C. Privacy requirements should be tailored to smaller Internet Providers and their customers.

ACA appreciates that the Notice, consistent with a risk-based approach, recognizes the benefits of imposing extensive privacy regulations on smaller providers are limited because most smaller providers do not collect, maintain, or share much, if any, personal information—let alone sensitive customer information—with third parties.[22] By contrast, Facebook and Google collect information on billions of consumers, and when their data is breached, tens of millions of consumers, if not more, are harmed. Any reasonable regulatory approach should focus on where harms are the greatest.

The costs of regulation also weigh more heavily on smaller providers, who not only have more limited resources to spend on compliance with regulations than larger providers,[23] but lack

---

21 Other stakeholders support a risk-based approach. For instance, in a recent blog post, Kathy Grillo, Senior Vice President, Verizon, stated, "Statutory requirements governing ever-evolving technology need to be flexible so that they don't become quickly outdated. The overall framework should be informed by the principle that the level of sensitivity of the person information will dictate the corresponding protections. The FTC could have a role in providing guidance on statutory requirements, such as defining 'personal information' and 'sensitive personal information.'" Kathy Grillo, *Privacy: It's Time for Congress to do right by consumers*, Verizon (Oct. 9, 2018), available at https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers.

22 *Notice* at 48600, 48603.

23 From the experiences of ACA members, the types of costs that smaller providers may incur include: 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; costs associated with all aspects of providing required

the scale and scope of larger providers upon which to spread the costs of compliance.[24] Further, by contrast with larger providers, smaller providers' employees tend to be less specialized, often performing multiple, disparate tasks, and so the costs to engage in the training and education needed to deal with regulations is impactful. In addition, smaller providers rarely have in-house counsel or personnel specializing in privacy and data security matters. As a result, the burdens to spend on understanding any requirements and then to comply with them are greater. Accordingly, the Notice appropriately seeks "solutions that support their continued ability to innovate and support economic growth,"[25] while ensuring "they make good-faith efforts to utilize privacy protections."[26]

---

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 personal information; and opportunity costs associated with diverting scarce resources from innovation and infrastructure deployment to regulatory compliance.

24 *See* Phillips Speech at 6 ("By their nature, regulatory regimes create compliance costs that are durable and may become more onerous over time. These are what economists call 'economies of scale', costs that large companies can bear more easily than their smaller competitors or new entrants."). Commissioner Phillips (at 9) also notes that "large companies can manipulate legal requirements to their own benefit more easily than smaller competitors or new entrants."

25 *Notice* at 48600.

26 *Notice* at 48603. ACA notes that the FCC, in its *Privacy Order*, failed in many instances to account for the disproportionate burdens its rules would impose on small providers and their customers. For example, nowhere did the *Privacy Order* even attempt to quantify the costs of the adopted rules, despite the overwhelming evidence in the record that prescriptive rules would be extremely burdensome for small providers. *See, e.g.*, *Privacy Order* at 14111 (highlighting part of the FCC's Final Regulatory Flexibility Analysis). The FCC also simply assumed, for instance, that its choice framework would not be burdensome because "[t]he choice rules are also significantly harmonized with existing rules, with which most small providers currently comply." *Id.* at 14078. However, in doing so, the FCC ignored that the *Privacy Order* significantly modified its existing choice framework by adopting a sensitivity-based regime, heightening consent requirements, and removing existing exemptions. *See id.* At 13913-15. As a result, the changes to the consent rules would have required modifications to an ISP's existing consumer choice policies, employee and vendor training materials, and systems for obtaining and tracking customer choices, all at substantial cost and disruption to providers' business operations. The rules also created confusion and frustration among consumers, who would have been faced with a new privacy regime out of step with their expectations and a deluge of new consent forms.

Similarly, the FCC assumed that its "reasonableness" approach to data security would mitigate small provider concerns about the cost of the data security requirements. *Id.* at 14046. However, while the FCC planned to consider the size of an ISP when analyzing whether its data security practices are reasonable, *id.* at 14010, as explained above, many small providers would have expended even more significant resources—including internal and external legal, compliance,

ACA believes NTIA should address concerns about smaller firms in two ways that would be consistent with the goal of protecting their customers' privacy. First, require the smallest firms to continue to be subject to the current FTC requirement that they refrain from engaging in unfair and deceptive acts or practices, but do not subject them to any enhanced requirements, such as ones similar to those included in the CCPA. Second, for other smaller firms, tailor any enhanced requirements to their capabilities and their customers' expectations. Regarding a complete exemption, ACA believes that the CCPA, which consumer advocates cite as a robust statute,[27] provides a template. The CCPA carves out smaller firms by applying its requirements to only firms that, among other things, have annual gross revenues of more than $25 million or that collect "the personal information of 50,000 or more consumers, households, or devices."[28] ACA submits that such an exemption addresses the burden that smaller firms—which generally collect little or no sensitive, let alone personal, information and do not share it with third parties—would face by having to comply with enhanced requirements that are oriented to concerns with collection and use practices of larger providers. Thus, ACA recommends NTIA not apply any enhanced requirements to any Internet Provider that has at least annual gross revenues of less than $25 million (as adjusted annually) or that collects customer personal information from fewer than at least 50,000 households.[29]

---

and technical personnel—on an abbreviated timeline to adopt the FCC's "exemplary practices" or face an increased risk of enforcement.

27 *See, e.g.,* Testimony of Alastair Mactaggart, Board Chair, Californians for Consumer Privacy, Before the S. Comm. on Commerce, Science, & Transportation, *Hearing on Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act* at 2:01 (Oct. 10, 2018), available at https://www.commerce.senate.gov/public/index.cfm/2018/10/consumer-data-privacy-examining-lessons-from-the-european-union-s-general-data-protection-regulation-and-the-california-consumer-privacy-act.

28 Cal. Civ. Code §1798.140(c).

29 Smaller providers in California continue to be subject to the "mini-FTC" law requiring them to refrain from engaging in deceptive or unfair acts or practices. Cal. Bus. & Prof. Code §§ 17200, 17500.

In addition, ACA recommends that NTIA, as part of the Administration's proposal, adopt data security policies that align with the risk-based framework developed by the National Institute of Standards and Technology ("NIST") through a multi-stakeholder process. The framework is designed to guide critical infrastructure companies, including ISPs, to develop data security measures that are appropriate for each company's profile, including based on the company's size and the nature of the information they collect.[30] The measures would help companies understand their risk and then protect against, identify, respond to, and recover from data breaches.[31] In any event, any data security standards NTIA adopts should account for the lower security risks of small ISPs. Holding small ISPs to a set of high data security standards that might be appropriate for large providers that collect larger amounts of customer personal information would be costly, beyond the limited resources of small providers, and unnecessary given the lower risk of smaller ISPs. The risk-based approach in the NIST framework would ensure that providers are implementing data security procedures that are effective for their operations.

Smaller providers also would struggle to implement and comply with a requirement that they provide customers with access to all their data in the provider's possession and then give customers the ability to correct that data,[32] such as the one contained in the CCPA. Smaller

---

30 *See Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*, NIST at 11 (2018).

31 *See id.* at 6-8.

32 In general, 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. *See Protecting Consumer Privacy in an Era of Rapid Change*, FTC at 65 (2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("*FTC Privacy Report*"). 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

providers generally store customer personal 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 major effort, requiring providers to build new systems to store all customer personal 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 previously designed for internal use only.

Finally, should NTIA determine that the Administration should alter any existing customer approval processes, such as that which occurred with the CCPA, smaller providers will need to engage attorneys to understand the new rules and what they mean for existing and planned collection, use, and sharing of customer information. And the more complicated the framework or the more it differs from existing frameworks, the more time attorneys and other personnel will spend on the task. In addition to the consent framework, any requirements for soliciting and documenting consent will impose additional costs. Attorneys would need to draft consent forms and compliance plans, and help train employees, agents, and partners on the permissible uses of personal information. Further, to comply with new consent requirements, smaller providers will need to build or upgrade systems, most likely by outsourcing, for obtaining and tracking consumer consents. Lastly, any different approval framework would require providers to again need to expend resources to obtain new approvals from consumers at a substantial cost.

In sum, any enhanced privacy framework for smaller providers that collect data on at least more than 50,000 households, but not so many as to be considered a large Internet Provider should generally provide them with additional time and flexibility to comply.

---

credit card numbers for $1 each. *See* Fed. Bureau of Investigation, Private Industry Notification 140408-009, FBI Cyber Division: (U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (2014).

III. ACA's Recommended Privacy Approach

In 2016, as the FCC was considering adopting privacy and data security regulations for ISPs, ACA joined with other ISPs and their trade associations to propose a privacy and data security regulatory framework that would be based on the "unfair or deceptive acts or practices" standard of Section 5 of the FTC Act, under which the FTC treats all providers in the Internet eco-system similarly.[33] Until the FCC's 2015 *Open Internet Order*, ISPs operated under the FTC's framework and complied without incident. ISPs explained their proposal would not only establish the appropriate, technology-neutral standard, but also would avoid customer confusion that would be inevitable under any entity-based regulation[34] and would lead to greater innovation and competition. ACA continues to support this approach. Given its expertise and experience in dealing with complex and evolving privacy issues, the FTC, which again oversees ISP privacy and data security activities, should be the agency to establish and enforce data collection and use practices for all Internet Providers.

ACA believes that any privacy and data security framework that NTIA develops for the Administration, with FTC as the lead agency, should be consistent with the FTC's historical oversight of these matters—and NTIA should not adopt enhanced requirements. More specifically, the following four principles should underlie privacy and data security policy: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification.

- **Transparency**. Internet Providers should provide notices that clearly, comprehensibly, and accurately describe the categories of customer data that they collect, how they will

---

33 *See* Letter from Matthew M. Polka, President & CEO, American Cable Association, *et al.*, to Tom Wheeler, Chairman, FCC (Mar. 1, 2016).

34 The FTC too has agreed that a privacy framework should be technology neutral. *See, e.g., FTC Privacy Report* at 31; Press Release, Joint Statement of Acting FTC Chairman Maureen K. Ohlhausen and FCC Chairman Ajit Pai on Protecting Americans' Online Privacy, FTC (Mar. 1, 2017), available at https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc.

use that data, and whether and for what purposes they may share that data with third parties. Privacy policies should be easily accessible, prominent, and current.

- **Respect for Context and Consumer Choice**. Internet Providers may use or disclose customer data 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, including by ensuring consumers are aware they are giving consent and the specific purposes for which they are giving consent. For example, Internet Providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their data, where the failure to provide choice would be deceptive or unfair. Internet Providers also should consider the sensitivity of the data and the context in which they were collected when determining the appropriate choice mechanism. On the other hand, the use or disclosure of customer data for the following commonly accepted data practices would not warrant a "choice mechanism" (customer consent), 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.

- **Data Security**. Internet Providers should establish, implement, and maintain a customer data security program that includes reasonable physical, technical, and administrative security safeguards to protect customer data from unauthorized access, use, and disclosure. Internet Providers' data security programs should provide reasonable protections in light of the nature and scope of the activities of the firm, the sensitivity of the data, and the size and complexity of the relevant data operations of the firm.

- **Data Breach Notifications**. Internet Providers should notify customers whose data 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. Internet Providers should have flexibility to determine how and when to provide such notice.[35]

ACA believes this framework, based on the current FTC regime, will provide Internet Providers with the ability 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 with new products and customized services. By contrast, rules dictating specific methods quickly become out of date and out of step with constantly changing technology, hampering innovation and harming consumers.

ACA's framework also would enhance the ability of smaller providers that are not exempt to comply without incurring undue cost or burdens. First, the framework is consistent with the requirements of the cable privacy and CPNI statutes, which many smaller providers are required to comply with if they also offer cable or telephone service.[36] Second, ACA's framework aligns with consumer expectations by respecting the context of customer-provider interactions, while

---

35 By contrast, the *Privacy Order* adopted a rule under which a carrier must notify affected customers of any data breach "unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." *Privacy* Order at 14085. While harm-based triggers may be reasonable, the FCC's definition of harm was so broad as to be essentially unbounded, encompassing "financial, physical, and emotional harm." *Id.* at 14022. By including emotional harm as sufficient to trigger a breach notification, the FCC required providers to engage in needless subjective analysis. Providers would have consequently deferred toward notification rather than risking enforcement for failure to notify. As a result, providers and customers would have been left in the same position as if there were no harm-based trigger at all—subjected to an unduly burdensome notification regime unmoored from necessity, precedent, or common sense.

36 *See* 47 U.S.C. §§ 222, 551.

providing smaller providers with flexibility to offer new and innovative services to their customers, increasing consumer choice and competition. Third, the proposed data security rule maintains a robust general security standard, requiring 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 into medium or large providers, the rules naturally will require more sophisticated processes commensurate with their larger operations. Finally, the proposed data breach notification rule provides flexible deadlines that will not overburden smaller 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.

In sum, by continuing to base national privacy policy on an "unfair and deceptive acts or practices" approach for all Internet Providers, customers' privacy needs would be met, and Internet Providers would increase access to innovative products and services. In addition, should NTIA decide that enhanced requirements are necessary, any approach needs to account for the unique attributes of smaller providers—and the fact that they pose a far less threat to their subscribers' privacy interests. ACA believes this is a sound approach that would be consistent with FTC historical oversight. Finally, we should strive to make this approach the sole privacy and data security framework for all Internet Providers and their customers in the US, just as the FCC has done in its *Restoring Internet Freedom Order*.[37] As discussed above, making providers that operate across state lines subject to individual state, or even local, mandates will add enormous amounts of friction, especially for smaller ISPs, with no demonstrable benefit.

---

[37] *Restoring Internet Freedom Order* at 427 (the Order "preempt[s] any state or local measures that would effectively impose rules or requirements that [the FCC has] repealed or decided to refrain from imposing in order or that would impose more stringent requirements for any aspect of broadband service" addressed in the Order).

IV. Conclusion

ACA supports the development of a national privacy policy for Internet Providers that accounts for the unique characteristics of smaller providers and their customers. Any such policy should establish rules that are competitively and technology-neutral. In addition, the rules should apply uniformly in all jurisdictions in the US so that consumers can understand and act on their rights regardless of the entity accessing their personal information and so that businesses have greater certainty and lower compliance burdens. This framework also should be based on the existing risk-based approach, which will protect the reasonable privacy expectations of consumers and recognize that collection, use, and sharing practices will constantly evolve as innovative and beneficial services are deployed.

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
Kelley Drye & Warren LLP
3050 K Street, NW
Washington, DC 20007
(202) 342-8518
Counsel to American Cable Association

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

November 9, 2018