Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION F/K/A
THE CONSUMER ELECTRONICS ASSOCIATION

Julie M. Kearney
Vice President, Regulatory Affairs
Alexander B. Reynolds
Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

May 27, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In today's economy, the Internet unquestionably is the engine that drives America and the world. Innovation, in turn, drives the Internet economy and the many benefits that flow from it. Such innovation relies on the beneficial use and sharing of consumer data among ecosystem players, to allow Internet players at all layers in the process to better serve customers' needs both today and tomorrow. CTA member companies understand the critical importance of protecting users' privacy and have strong incentives to do so – consumers will not readily use new technologies that do not protect the privacy of their personal information. CTA members also are leaders in shaping industry-wide, consumer-friendly voluntary efforts on privacy, including by publishing CTA's *Guiding Principles on the Privacy and Security of Personal Wellness Data*.

Although the frameworks in place today are currently working to protect consumers while maintaining the flexibility necessary to innovate, the Commission now seeks to depart from this approach in order to adopt an onerous and prescriptive privacy framework. Whatever action the Commission takes, the agency should bear in mind that it has only limited authority to address privacy and data security. Specifically, the Commission may only adopt and enforce regulations intended to ensure protection of customer proprietary network information, and may do so only with respect to telecommunications carriers in their provision of telecommunications services. Although the *Notice* properly recognizes the bounds of the Commission's authority with respect to edge providers and equipment manufacturers, it impermissibly oversteps Congressional limitations regarding the scope of information covered by the proposal.

The proposal is not just bad law – it is also bad policy. The *Notice*'s proposed approach, if adopted, will inhibit the ability of broadband providers to innovate and meet consumer preferences and needs, and it will cause consumer confusion. For example, the proposed approval framework unwisely would require opt-in consent for most uses and disclosures of *any type* of customer information, which will lead to uncertainty among ISPs and their manufacturer and edge provider partners. The proposed data security standard appears to contemplate a strict liability standard, which would have a chilling effect on investment and innovation by forcing a misallocation of resources. And the overbroad transparency and data breach notification requirements would fatigue, rather than inform, consumers.

This proposed departure from the consistent framework that governs the entire Internet ecosystem will directly harm consumers, undermine their trust in the Internet ecosystem, and stifle innovation, and will do so without a corresponding benefit to consumer privacy. Rather than adopt these confusing and counterproductive privacy and data security rules, the FCC at most should pursue an approach more consistent with the Federal Trade Commission's longstanding and successful framework. This would foster regulatory certainty, in a manner consistent with both consumer expectations and the Commission's consumer privacy goals.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF THE
CONSUMER TECHNOLOGY ASSOCIATION F/K/A
THE CONSUMER ELECTRONICS ASSOCIATION

The Consumer Technology Association ("CTA")[1] respectfully submits these comments in response to the above-captioned *Notice of Proposed Rulemaking* ("*Notice*").[2] The *Notice* proposes sweeping new privacy requirements for broadband Internet access service ("BIAS") providers,[3] chilling investment and innovation and resulting in an inconsistent approach across the Internet ecosystem. Ultimately the proposed framework, which departs from the successful principles-based approach to online privacy regulation by the Federal Trade Commission ("FTC"), will fail to benefit consumers in the manner the Commission intends.

I. INTRODUCTION

In 2016, the Internet unquestionably is the engine that drives America and the world. Innovation, in turn, drives the Internet economy and the many benefits – including jobs,

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $287 billion U.S. consumer technology industry. More than 2,200 companies – 80 percent are small businesses and startups; others are among the world's best known brands – enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development, and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technology. Profits from CES are reinvested into CTA's industry services.

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("*Notice*").

[3] We alternately refer to BIAS providers as Internet Service Providers, or "ISPs."

education, creative works, public safety, and civic engagement – that flow from it. Such innovation relies on the beneficial use and sharing of consumer data among ecosystem players, to allow providers at all layers in the process (not just BIAS providers) to better serve customers' needs both today and tomorrow. As President Barack Obama has described, "[i]n just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information."[4]

CTA has a front-row seat to the Internet economy and its benefits, bearing close witness to its members' rapid development and deployment of new products and services and producing CES, which unfailingly showcases "the next big thing" in technology and innovation. When it comes to privacy, CTA member companies are at the forefront of advanced consumer technologies that increasingly rely on data to provide value to end-users. These companies understand the critical importance of protecting users' privacy and have strong incentives to do so. The reason is simple: *Consumers will not readily use new technologies that do not protect the privacy of their personal information*. Our members are committed to safeguarding their customers' data, and many have comprehensive programs in place to ensure compliance with applicable federal and state laws, as well as with self-regulatory guidelines and best practices governing the protection of personal information.

CTA members also are leaders in shaping industry-wide, consumer-friendly voluntary efforts on privacy. For example, last year CTA published its *Guiding Principles on the Privacy*

[4] Letter from Barack Obama, President, United States (Feb. 23, 2012), *prefaced to* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting innovation in the Global Digital Economy* (Feb. 2012) ("*White House Privacy Blueprint*").

and Security of Personal Wellness Data ("*Principles*"), a first-of-its-kind effort.[5] The *Principles* lay out the essential steps companies can take to address privacy and security risks related to wellness data, particularly the provision of concise notices that accurately communicate a company's data management practices. While sufficiently specific to ensure consumers are educated on the collection and use of their and wellness data, the *Principles* also are flexible enough to allow companies room to innovate in technology and business models. Thus, the *Principles* offer the appropriate formula of protecting consumers' privacy and educating consumers about choices available to them but also allowing innovation and competition to flourish.

CTA's interest in this proceeding stems at the outset from member companies' deep experience in balancing consumer expectations regarding privacy with preserving flexibility to innovate. Indeed, although the Commission lacks authority to regulate equipment manufacturers' and software developers' (including edge providers) privacy practices, and the *Notice* does not contemplate such regulation,[6] this issue is sufficiently important to warrant our participation in this proceeding. We care deeply about preserving a highly functioning ecosystem that provides maximum benefits to consumers. Yet despite the fact that frameworks in place today are currently working to protect consumers, the Commission proposes to muddy the regulatory waters with onerous and prescriptive rules.[7] This proposed approach will inhibit

---

[5] Consumer Technology Association, *Guiding Principles on the Privacy and Security of Personal Wellness Data* (Oct. 20, 2015), http://www.cta.tech/healthprivacy.

[6] *See Notice* ¶ 13 (noting that the *Notice* applies "solely to the existing class of services that Congress included within the scope of Title II, namely the delivery of telecommunications services").

[7] *See, e.g.*, Remarks of Maureen K. Ohlhausen, Commissioner, Federal Trade Commission, *The FTC, The FCC, and BIAS*, at the George Mason University School of Law Public Policy Briefing on Privacy Regulation after Net Neutrality, at 10 (Mar. 20, 2016) ("*Ohlhausen Remarks*"), *available at* https://www.ftc.gov/system/files/documents/public_statements/942823/160331gmuspeech1.pdf ("[I]t shouldn't be surprising that some advocates have already suggested that an FCC-led beachhead of

the ability of broadband providers to innovate and will confuse consumers, all with little to no benefit to consumers.

In contrast, CTA members' experience is that industry self-regulation, combined with the FTC's time-tested and principles-based privacy and data security framework, has worked to benefit consumers, competition, and the U.S. economy.[8] Companies have had the flexibility to innovate and deliver the services that consumers desire in the various, evolving ways consumers demand. By encouraging comprehensive and robust self-regulation and building flexibility into its approach, the Commission can achieve its desired goals of transparency, choice, and security without intrusive, burdensome regulation that would have significant negative consequences for consumers.

II. CONGRESS HAS STRICTLY LIMITED THE COMMISSION'S AUTHORITY TO REGULATE PRIVACY AND DATA SECURITY

Whatever action the Commission takes in response to the record on the *Notice*, the agency should bear in mind that it has only limited authority to address privacy and data security pursuant to Section 222 of the Communications Act of 1934, as amended (the "Act").[9] Under this provision, the Commission may only adopt and enforce regulations intended to ensure

---

restrictive privacy could support similar requirements for edge providers. Thus, all companies that wish to use consumer data for innovative new products and services should pay close attention to the FCC proceeding to set privacy rules for ISPs.") (citing Harold Feld, *Remarks at Preserving Broadband Network Privacy*, Public Knowledge (Feb. 17, 2016) https://www.publicknowledge.org/events/preserving-broadband-network-privacy; Harold Feld (@haroldfeld), Twitter (Mar. 31, 2016, 12:28 PM), https://twitter.com/haroldfeld/status/715576443401469954 ("Totally. Am hoping @FCC action permits @FTC 2 go further despite limits of Sec. 5(n) in areas under its jurisdiction")).

[8] State attorneys general also have emerged as important principles-based privacy and data security enforcers. *See, e.g.*, Danielle Keats Citron, *Privacy Enforcement Pioneers: The Role of State Attorneys General in the Development of Privacy Law*, Notre Dame L. Rev, at 4 (forthcoming Fall 2016) ("State attorneys general have been nimble privacy enforcement pioneers, a role that for practical and political reasons would be difficult for federal agencies to fill.").

[9] 47 U.S.C. § 222.

protection of customer proprietary network information ("CPNI"), and may do so only with respect to telecommunications carriers in their provision of telecommunications services.[10] The Commission's authority to regulate privacy in the communications space is not unbounded.

As an initial matter, CTA appreciates that the Commission properly has recognized the bounds of its authority with respect to edge providers and equipment manufacturers and does not propose to include these entities in any rules it adopts.[11] The agency must continue to adhere to this constraint. While it is bad policy to impose impractical and inconsistent privacy rules on one particular section of the Internet economy (ISPs), it would be bad law as well as bad policy to "correct" for that concern by expanding the scope of the rules beyond carriers. For instance, where data may be shared, the Commission appears to contemplate having mobile BIAS providers effectively regulate mobile device and mobile operating system providers.[12]

In addition, no matter which types of entities would be subject to the rules, the *Notice* is off course with respect to the types of information to which the rules would apply. In contravention of its limited authority, the *Notice* impermissibly seeks to establish rules that

---

[10] *See generally* Petition for Partial Reconsideration by CTIA, WC Docket No. 11-42 et al. (filed Aug. 13, 2015) ("CTIA Petition").

[11] *See Notice* ¶ 14; *see also* Comments of the Consumer Electronics Association, CC Docket No. 96-115 (filed July 13, 2012); Notice of Ex Parte of the Consumer Electronics Association, CC Docket No. 96-115 (filed June 20, 2013); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9619 ¶ 28 ("*Mobile Device CPNI Declaratory Ruling*") (third-party applications outside scope of Section 222 and information stored on mobile device that is not under the carrier's control and not intended to be transmitted to carrier, or otherwise accessible to the carrier, is not CPNI); Statement of Commissioner Jessica Rosenworcel on *Mobile CPNI Declaratory Ruling*, FCC 13-89 (CPNI protections do not apply to the manufacturers of wireless phones and developers of operating systems).

[12] CTA assumes that the discussion of contractual arrangements between mobile BIAS providers and mobile device or mobile operating system ("OS") manufacturers was intended to only address, consistent with the Commission's *Mobile Declaratory Ruling*, covered information collected by the BIAS provider and subject to such provider's control. *See Notice* ¶ 213. It would be entirely inappropriate and unlawful if the Commission intended to use any authority it has over BIAS providers to establish *de facto* privacy requirements for device manufacturers and OS providers.

address customer information that far exceeds the scope of CPNI, creating a wholly new category of information (which appears nowhere in the Act) that it calls "Customer Proprietary Information" or "customer PI," which would encompass both CPNI and "personally identifiable information (PII)."[13] This interpretation of Section 222(a), which expands the scope of customer data protected beyond CPNI, conflicts with the language, structure, and purpose of Section 222 and contravenes Congress's intent in enacting Section 222.[14] Congress chose in Section 222 to cover "proprietary information," not "personal information" or PII, information that identifies an individual and is the kind of information that privacy laws govern.[15] It used the term "proprietary information" in Section 222, not "personal information" or "personally identifiable information," because it intended Section 222 to serve a different purpose.[16] If Congress had wanted Section 222 to cover "personally identifiable information" and not just CPNI, it knew how to do so and would have said so. Thus, the Commission cannot use Section 222 to capture

[13] *See Notice* ¶ 74.

[14] The Commission should not rely here on the Notice of Apparent Liability ("NAL") and Consent Order in *TerraCom/YourTel* for support that Section 222(a) captures a new category of information that neither appears, nor is defined in the statute and that the Commission calls "customer proprietary information." *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) ("*TerraCom/YourTel*"). In that NAL, the Commission ignored its previous longstanding position – that Section 222 covered only three categories of customer information: (1) individually identifiable CPNI; (2) aggregate customer information; and (3) subscriber list information – and instead mischaracterized two sentences from other Commission orders to assert that Section 222(a) imposes a broader obligation. *Id*. at 13330-13333. The Commission should not affirm the mistake of *TerraCom/YourTel* by using it as a foundation here.

[15] Congress chose to use the term "PII" elsewhere in the Act, both before and after Congress drafted Section 222 in 1996. *See* Cable Communications Policy Act of 1984, Pub. L. 98-549 (modifying 47 U.S.C. § 551 to address PII of cable subscribers); Consolidated Appropriations Act of 2005, Pub. L.108-447, § 206 (2004) (modifying 47 U.S.C. § 338 to address PII of satellite subscribers)

[16] Specifically, because CPNI was available only to carriers and their customers, Congress was concerned that "[i]ncumbent carriers already in possession of CPNI could leverage their control of CPNI in one market to perpetuate their dominance as they enter other service markets." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8064 ¶ 2 (1998) ("*1998 CPNI Order*").

ISP customers' information that is not CPNI. Nor can the Commission use other provisions of the Act to overwrite the balance Congress sought to achieve in adopting Section 222.[17]

III. PRESCRIPTIVE PRIVACY RULES WILL CHILL INNOVATION AND INVESTMENT IN THE INTERNET ECOSYSTEM AND FAIL THE CONSUMERS SUCH RULES PURPORT TO SERVE

Beneficial use of customer information in ways not harmful or surprising to consumers generally is a positive thing – the connected world relies on the trusted use of consumer information, and has established the United States online tech economy as the envy of every other country in the world.[18] The *Notice*, however, proposes a particularly prescriptive and onerous consent regime for ISPs that will undoubtedly inhibit the ability of ISPs to make beneficial uses of customer information and to innovate. As a result, the proposal fails to afford the flexibility that providers need to meet consumer preferences and needs.

Indeed, this need for flexibility is well-recognized. The White House, for example, has indicated that flexibility "affording companies discretion in how they implement" general

---

[17] For example, Section 201(b), which provides that "[a]ll charges, practices, classifications, and regulations for *and in connection with* [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification or regulation that is unjust or unreasonable is declared to be unlawful" does not offer a separate basis for regulating consumer privacy. Data privacy and security practices related to non-CPNI customer PII certainly are not practices "in connection with" broadband service, and before the *TerraCom/YourTel* NAL, the Commission had never before asserted that 201(b) gave it authority to regulate data security. The other legal authorities the Commission claims to support its proposed rules are similarly unpersuasive. The Commission claims, for example, that Section 706 would independently support the rules. *See Notice* ¶ 308. However, Section 706 is not an unlimited grant of power. *See, e.g.*, Reply Comments of the Consumer Electronics Association, GN Docket No. 14-28, at 4 (Mar. 21, 2014). Moreover, the proposal may actually have the effect of "retard[ing]" rather than "advanc[ing] the important goal of universal broadband deployment and adoption." Doug Brake, Daniel Castro, Alan McQuinn, *Broadband Privacy: The Folly of Sector-Specific Regulation*, Info. Tech. & Innovation Found at 13 (Mar. 2016).

[18] *See, e.g.*, Avi Goldfarb and Catherine E. Tucker, *Privacy Regulation and Online Advertising*, 57.1 Mgmt. Sci. 57 (2010) (comparing and contrasting EU privacy regulation with the U.S. regime, and finding that European prescriptiveness may have deterred online innovation in part through a decrease in advertising effectiveness). *See* Gary Shapiro, *Innovation: Leading the Great American Comeback*, HuffPost Business, http://www.huffingtonpost.com/gary-shapiro/leading-the-great-america_b_769454.html (2010) ("With ingenuity, creativity and entrepreneurial spirit, Americans lead the post-industrial knowledge economy.").

privacy principles "help[s] promote innovation" and "encourage[s] effective privacy protections by allowing companies, informed by input from consumers and other stakeholders, to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single rigid set of requirements."[19] In contrast, frozen prescriptive broadband privacy rules, as proposed by the Commission, will restrict ISPs' ability to innovate and adjust to consumer demands and expectations of both today and tomorrow. Many of the proposals run the real risk of restricting consumers without a corresponding benefit.

Approval Framework. For example, under the proposal, most uses and disclosures of *any type* of customer information will require opt-in consent.[20] This will lead to absurd results: Broadband providers could be prohibited from marketing without consent a smartphone to their own customers, as they would need to use some customer information (*e.g.*, name and email address) to market the phone, but marketing the phone might not meet the definition of "communications-related services."[21] Yet carving out additional exceptions beyond "communications-related services" or otherwise broadening the definition also is not the answer, as whatever arbitrary line the Commission draws still will leave problems on the other side.

The proposal would also create a great deal of uncertainty among ISPs – and any manufacturer and edge provider partners – regarding what types of activities would not require opt-in consent.[22] For example, would a BIAS provider that uses a customer's information to

---

[19] *White House Privacy Blueprint* at 9 (noting that the FTC's "privacy framework is designed to be flexible to permit and encourage innovation").

[20] *See Notice* ¶ 127 (proposing to require opt-in approval before BIAS providers (1) use customer PI for purposes other than marketing communications-related service; (2) share customer PI with affiliates providing communications-related services for purposes other than marketing those communications-related services; and (3) sharing customer PI with all other affiliates and third parties).

[21] *See id.* ¶ 71 (asking whether to limit "communications-related services" to telecommunications, cable, and satellite services regulated by the Commission).

[22] *See id.* ¶¶ 111-123 (proposing implied approval and opt-out approval requirements).

market a bundle that includes a non-communications-related service (*e.g.*, smart home services) require opt-in consent? If a broadband service offered unlimited video or music from an edge provider, would including that edge provider's logo in the marketing of the broadband service – or even a customer's bill – be using the customer's information to market a non-communications-related service? Or is such a promotion part of marketing the broadband service, and thus subject to implied consent? The proposed rules leave these hypothetical examples – which do not even involve sharing of data with a third party or the use of sensitive data and thus raise few privacy concerns[23] – in a regulatory gray area.[24] Not only will this uncertainty hurt ISPs' ability to market new services and offerings, it will impede potential partnerships between ISPs and other Internet ecosystem players to bundle and market products and services that could offer value to consumers. The results may become even more absurd with respect to "use" of customer PI outside of the marketing context – including customer PI that is obtained through different mechanisms but still used only internally or with affiliates.

These hypotheticals illustrate one key point: that the complete and utter lack of clarity in and arbitrary nature of the proposed approval rules would undoubtedly have a chilling effect on BIAS providers' marketing and development of their own, and any partners' services, even if they are arguably allowed to do so in certain cases without obtaining opt-in consent. By setting such stringent restrictions, consumers likely will miss out on what could otherwise be welcomed opportunities, such as receiving discounts, offerings, and information about new services, or

[23] *See, e.g.*, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 15-16 (Mar. 2012) ("FTC Privacy Report") ("The Commission agrees that the first-party collection and use of non-sensitive data (*e.g.*, data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties.").

[24] These are but a few examples – there may be hundreds, if not thousands, of other scenarios. The FCC should not try to address them by creating carve-outs. Such an approach would just further muddy the landscape and create even more unintentional consequences.

even enjoying customized user experiences based on data collected.[25] Because ISPs would first have to launch a campaign of click-through agreements to get the needed consents, which would have the exact opposite desired result – leaving their customers annoyed, frustrated, and disengaged – it is unlikely that ISPs would even get such offerings out of the gate. The Commission's proposal thus eviscerates an ISP's ability to effectively market to its own customers, cutting its advertising legs right out from under it – all to the detriment of the consumer.

Data Security Obligations. The data security standard set forth in the *Notice* would have an equally chilling effect on investment and innovation. While the Commission touts the proposal as being consistent with the FTC's flexible approach to security,[26] the proposed language for Section 64.7005(a) tells a different story, essentially creating a strict liability standard. Specifically, the proposed language states that a "BIAS provider *must* ensure the security, confidentiality, and integrity of *all* customer PI the BIAS provide receives…."[27] Such an unforgiving and unrefined standard could force an ISP to spend scarce resources on efforts to encrypt large swaths of non-sensitive data to avoid the risk of being subject to enforcement action by the Commission's Enforcement Bureau. This could be a death knell for smaller ISPs. At a minimum, it would deprive ISPs the right to make reasoned business decisions about their security choices and instead force them to divert precious time and money that could otherwise be spent on innovation and investment. The *Notice* fails to adequately justify the purported benefits of such a prescriptive regulatory approach against these inevitable costs.

---

[25] *See* Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center (2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing (noting that "many" consumers are willing to share personal information in exchange for certain deals and benefits).

[26] FTC Privacy Report at 24 (companies must provide reasonable security for consumer data).

[27] Proposed Section 64.7005(a) (emphasis added).

Notice Obligations. In addition, the Commission's approach will undoubtedly result in "notice fatigue." Consumers are undoubtedly already feeling overwhelmed receiving an endless stream of emails most of which likely go straight from the mailbox to the recycle bin.[28] Adding another heap to the mountain of notices will not really serve to help consumers, but instead will leave them desensitized, tuned out, and unable to differentiate between consent requests that involve fairly innocuous data versus those that ask to use highly sensitive data. Yet, the *Notice* proposes to do just that, including by proposing very specific "advance notice" requirements for any "material changes" in the providers' privacy policies[29] and by an overbroad data breach notification standard.[30]

IV. AT MOST, THE COMMISSION SHOULD ADOPT AN APPROACH CONSISTENT WITH THAT OF THE FTC

The FCC's proposal is the equivalent to the regulatory bull in the china shop – it is overbearing, clumsy, and highly disruptive. The *Notice*'s proposed departure from a consistent framework for all Internet ecosystem players will directly harm consumers, undermine their trust in the Internet ecosystem, and stifle innovation.[31] The Commission should instead take a page

---

[28] *See* Florian Schaub et al., *A Design Space for Effective Privacy Notices*, Usenix, at 3 (2015), https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf (noting that "[f]requent exposure to seemingly irrelevant privacy notices results in habituation, i.e., notices are dismissed without even registering their content") (*citing* B. Anderson et al., *Users Aren't (Necessarily) Lazy: Using Neurois To Explain Habituation To Security Warnings*, Proc. ICIS '14 (2014), and N. S. Good et al., *Noticing Notice, A Large-Scale Experiment On The Timing Of Software License Agreements*, Proc. CHI '07 ACM (2007)).

[29] *Notice* ¶ 96.

[30] *See id.* ¶¶ 236-238.

[31] Letter from Matthew M. Polka, President & CEO, American Cable Association et al., to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106, at 2 (filed Feb. 11, 2016), *available at* https://www.ncta.com/sites/prod/files/Privacy_Letter_021116.pdf ("Coalition Letter") ("[A] consistent privacy framework for the Internet … will protect consumers and avoid entity-based regulation that would create consumer confusion and stifle innovation.").

from the FTC's playbook, which has been successful in assuring strong consumer privacy and other protections without inhibiting industry's flexibility to innovate.

The FTC's approaches to privacy and security reflect marketplace realities. With respect to security, it requires that companies put into place "reasonable data security safeguards," which take into account the types of data being collected, the context in which it is being used, and the resources that are available. This approach makes eminently good sense, because "perfect" security simply does not exist, and there is a limit to how practical or feasible it is to use the same level of security in all instances, especially given a company's limited resources. For example, while it generally will make sense to encrypt sensitive data, such as health or financial information, it may not make economic or practical sense to encrypt non-sensitive information, such as information about consumers that may already be publicly available. Providers need and should have flexibility to allocate resources in the way best calculated to protect the consumer data they hold.

The FTC also strives to take a practical approach to ensuring customer privacy. The FTC's approach aims to balance the privacy interests of consumers with the innovation that relies on information to develop beneficial new products and services, indicating that it designed its privacy framework to be flexible specifically "to permit and encourage innovation."[32] As members of industry have noted, the FTC's framework "provides consumers with meaningful privacy protection and helps to enable a dynamic marketplace that supports the emergence of innovative new business models."[33]

In addition, industry players across Internet ecosystem have worked for years devising privacy best practices, understanding that good privacy practices are essential to maintaining a

[32] FTC Privacy Report.at 9.

[33] Coalition Letter at 1.

customer's trust and loyalty. As described above, just last year CTA published its *Principles* for wellness data, and continues to explore areas ripe for the establishment of best practices and guidelines. Likewise, CTIA has established its *Best Practices and Guidelines for Location Based Services* to address privacy concerns stemming from the availability of user location information.[34] And the Digital Marketing Association,[35] Digital Advertising Alliance,[36] and the Network Advertising Initiative[37] have all established codes of conduct or guidelines regarding the collection and use of consumer data. As the industry continues to fine tune these efforts, CTA urges the FCC to practice regulatory restraint and let the results of these efforts bear fruit, instead of seeking a solution in search of a problem.

V. CONCLUSION

As the Administration has recognized, and CTA member companies are well aware, consumer trust is critical to American citizens' confidence in the Internet economy. But promoting trust with respect to the privacy of customer information does not require the heavy-handed, imbalanced rules proposed in the Notice. Rather than impose these confusing and counterproductive privacy and data security rules, at most, the FCC should instead adopt a principles-based approach that is more consistent with the FTC's longstanding and successful framework. This path will foster regulatory certainty, consistent with both consumer

[34] CTIA, *Best Practices and Guidelines for Location-Based Services* (Mar. 23, 2010), http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf?sfvrsn=0

[35] The Direct Marketing Association, *Collection, Use and Maintenance of Marketing Data*, http://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/collection-use-and-maintenance-of-marketing-data/ (last visited May 18, 2016).

[36] Digital Advertising Alliance, *Self-Regulatory Program*, http://www.aboutads.info/ (last visited May 18, 2016).

[37] Network Advertising Initiative, *2015 Update to the NAI Code of Conduct*, http://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf (last visited May 18, 2016).

expectations and the Commission's goals of ensuring ISP customer privacy and increasing broadband adoption.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION F/K/A CONSUMER ELECTRONICS ASSOCIATION

By: */s/ Julie M. Kearney*

Julie M. Kearney
Vice President, Regulatory Affairs
Alexander B. Reynolds
Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7644

May 27, 2016