U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

Developing the Administration's Approach to Consumer Privacy	)	Docket No. 180821780–8780–01

COMMENTS OF NCTA – THE INTERNET AND TELEVISION ASSOCIATION

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

November 9, 2018

TABLE OF CONTENTS

Page

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration

Developing the Administration's Approach to Consumer Privacy	)	Docket No. 180821780–8780–01

COMMENTS OF NCTA –
THE INTERNET AND TELEVISION ASSOCIATION

NCTA – The Internet and Television Association[1/] hereby submits its comments in response to the Request for Comments (RFC)[2/] issued by the Commerce Department's National Telecommunications and Information Administration (NTIA) on ways to advance consumer privacy while protecting prosperity and innovation.

INTRODUCTION AND SUMMARY

NCTA commends NTIA for its thoughtful framing of a complex issue, its recognition of the plethora of countervailing factors that need to be considered in crafting a workable federal privacy framework, and its willingness to re-examine the continued utility of established approaches to implementing and operationalizing privacy safeguards.

For over 40 years, cable operators have been taking steps to ensure the privacy of their cable television subscribers in accordance with robust protections enacted by Congress.[3/] Since emerging as leading providers of broadband Internet access service, cable companies likewise

---

1/ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving approximately 85 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is also a leading provider of broadband service after investing more than $250 billion over the last two decades to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to more than 30 million customers.

2/ Department of Commerce, National Telecommunications and Information Administration; Department of Homeland Security, *Developing the Administration's Approach to Consumer Privacy*, Docket No. 180821780–8780–01, 83 FR 46800 (Sept. 26, 2018) ("RFC").

3/ 47 U.S.C. § 551.

have been careful to secure the privacy of their broadband customers' data. Their broadband data practices have been guided by the key principles of transparency, choice, and security that undergird the Federal Trade Commission's (FTC) privacy framework.

The privacy protection measures taken by cable companies have been driven not simply by the requirements of federal law. They also reflect the business imperative to secure and strengthen the trust of the customers with whom they share an ongoing relationship by serving as responsible stewards of their personal data. As both the FTC and the Federal Communications Commission (FCC) have recognized, respecting consumer privacy and properly safeguarding consumer data is key to successfully maintaining that customer relationship.[4/] NCTA's approach to the important issues under review in this RFC is informed by its members' long track record of safeguarding the privacy of their customers, implementing controls to ensure data is used properly and lawfully, and delivering advanced products and services to consumers.

Tens of millions of households served by NCTA member companies enjoy the convenience, customization, promotional offers and discounts, enhanced content, and tailored advertising made possible by data-driven services and features. These capabilities and innovations make consumers' experiences with our members' products and services more engaging and fulfilling. But consumers also expect – and deserve – the assurance that the

---

4/ *Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION, at 38-39 (2012), 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*") (highlighting importance of the "customer's relationship with the business" in determining application of privacy controls under its framework); *Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd. 14860, ¶ 37 (2002) ("Because of commercial constraints required to ensure customer accountability, therefore, the carrier with whom the customer has the existing business relationship has a strong incentive not to misuse its customers' CPNI or it will risk losing its customers' business.").

privacy and security of their personal information is fully safeguarded. A uniform national policy for privacy can and should ensure that consumers continue to receive both robust protection of their personal information and the benefits of data-driven services and innovation.

This is an opportune time to examine this issue. As the RFC recognizes, a growing number of countries, regions, and some U.S. states have articulated their own distinct visions for addressing privacy. This national and global fragmentation in the regulatory landscape regarding the collection, use, and sharing of consumer data is increasing calls for harmonization in the U.S. as businesses face potentially disparate, costly, and burdensome regimes and consumers face a confusing and likely frustrating array of privacy regimes. There is growing interest among a broad cross-section of industry, consumer advocates, and other stakeholders in forging a single national framework on privacy.

NCTA members support NTIA's effort to advance a national framework that utilizes a technology-neutral approach to privacy and data security issues. Such a framework should enable consumers to enjoy transparency, choice, and security with respect to how their data is handled, regardless of where they are or what product or service they are using. Broadly applicable national standards not only would serve the important interest of protecting consumers, they also would promote fair competition by avoiding the market distortions caused by asymmetric regulation. Accordingly, NTIA should ensure that its recommendations for a privacy and data security framework are rooted in a technology-neutral and sector-neutral approach that does not distort competition or cement the dominance of current market leaders.

The RFC laudably seeks to avoid rigid mandates and instead explores the viability of forging a workable user-centric, outcome-based framework for privacy. Data-driven products, services, and capabilities are marked by near-constant technological change, spurring innovation

and growth in the economy and precipitating transformative changes across not only all industry sectors, but also in the ways that consumers and businesses engage and interact with one another. Privacy protection must be sufficiently agile and flexible to both keep pace with, and allow for, continued changes in technology and consumer preferences.

NCTA's members operate in a highly competitive and changing landscape. Regulatory parity is critical in such a vibrant and dynamic segment of the economy, in order to ensure that market forces and consumer preferences dictate marketplace outcomes. Such parity also is critical to ensuring that consumers are afforded the same level of privacy protection as they navigate this market, regardless of the identity or business model of the entity they are interacting with, the service or product they are using, or the nature of the technology employed.

In order to promote competition, consumer welfare, and effective privacy protection, NCTA supports a balanced, globally interoperable privacy framework that treats all businesses consistently, that provides meaningful control to consumers, preempts state and local privacy laws and regulations applied to online and offline businesses, is enforceable by the FTC, and precludes private rights of action. A comprehensive, competitively-neutral privacy framework predicated upon the principles of parity, transparency, consumer control, security, access, risk management, enforcement and accountability, and harmonization can both protect consumers and promote innovation, growth, and new services.

I. THE ISSUES RAISED IN THE RFC ARE ESPECIALLY TIMELY GIVEN ONGOING DEVELOPMENTS IN THE PRIVACY POLICY LANDSCAPE

NTIA's release of the RFC coincides with a considerable amount of activity across the privacy policy landscape. By enacting last year's Congressional Review Act resolution vacating the 2016 FCC privacy rules imposed solely on Internet service providers (ISP), Congress made clear that it was rejecting the imposition of disparate privacy frameworks based solely on the

type of entity holding a consumer's data.[5/] In the wake of that action, and growing recognition of the scale and scope of data collection and use by edge platforms and other entities whose business models rely primarily or completely on monetizing consumer data, policy-makers and legislators are taking a more holistic approach at the federal level aimed at establishing a single framework applied consistently to all entities that collect, receive, or use consumer data.[6/]

This year has witnessed significant movement on privacy issues at the state level, exemplified by the Vermont privacy law that focuses on data brokers and the California Consumer Privacy Act (CCPA) that applies to businesses that collect and process California consumers' personal information.[7/] Meanwhile, the General Data Protection Regulation (GDPR) governing privacy rights in the European Union went into effect in May.[8/] The GDPR has extraterritorial effect, applying to companies – including those located in the U.S. – that process

---

5/ *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* 31 FCC Rcd 13911 (2016). *See also* Joint Resolution of Apr. 3, 2017, Pub. L. No. 155-22, 131 Stat. 88; 163 CONG. REC. S1929 (2017) (statement of Sen. Thune) ("The resolution before us today is the first step toward restoring regulatory balance to the internet ecosystem. The best way for that balance to be achieved is for there to be a single, uniform set of privacy rules for the internet--the entire internet--rules that appropriately weigh the need to protect consumers with the need to foster economic growth and continued online innovation."); 163 CONG. REC. H2492 (2017) (statement of Rep. Walden) ("In addition, the FCC's approach only protects consumer data as far as the internet service provider is involved. An entirely separate set of rules applies to providers of edge services. . . What America needs is one standard, across-the-internet ecosystem, and the Federal Trade Commission is the best place for that standard.").

6/ *See, e.g.*, *Restoring Internet Freedom*, Declaratory Ruling, Order, Report and Order, 33 FCC Rcd 311, ¶ 183 (2018) ("Consumers expect information to be 'treated consistently across the Internet ecosystem and that personal information will be subject to the same framework, in all contexts"); Joint Statement of Acting Chairman Maureen K. Ohlhausen and Chairman Ajit Pai on Protecting America's Online Privacy, at 1 (Mar. 1, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/03/joint-statement-acting-ftc-chairman-maureen-k-ohlhausen-fcc (endorsing a "comprehensive and consistent framework" to protect online privacy and noting that Americans shouldn't have to be lawyers or engineers to figure out if their information is protected differently depending on which part of the Internet holds it"). *See also* BROWSER Act, H.R. 2520, 115th Cong. (2017) (establishing an FTC-administered uniform framework for online privacy); MY DATA Act, S. 964, 115th Cong., (2017) (authorizing FTC to establish online privacy rules applicable to both edge providers and ISPs).

7/ An act relating to data brokers and consumer protection, 2017 Vt. Adv. Legis. Serv. 171; The California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100, et. seq. (2018) ("CCPA"). Businesses that do not meet certain thresholds related to revenue or number of consumers whose data is processed fall outside the scope of the CCPA. *See* § 1798.140(c).

8/ General Data Protection Regulation, Regulation (EU) 2016/679, Article 99, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

personal data of individuals who are in the EU, regardless of whether the company has a physical presence there or where the processing takes place, and irrespective of the regime's compatibility with U.S. law and policy.[9/] In addition, the privacy framework established by the Asian-Pacific Economic Cooperation (APEC) is now being used to facilitate cross-border data flows among Pacific Rim countries.[10/] Compliance with the APEC framework underpins a voluntary, enforceable certification program that provides assurance that certified businesses in participating countries – which include the U.S., Mexico, Canada, Australia, Japan, Singapore, and South Korea, with more expected to join – adhere to baseline privacy standards.[11/]

In a global economy driven by the exchange of digital goods and services, a poorly calibrated national privacy framework heightens the risk of inhibiting economic growth, trade, and innovation.[12/] The potential for a fragmented privacy landscape therefore is fueling calls for

---

9/ *See, e.g.*, Gus Rossi, *Is the GDPR Right for the United States?*, Public Knowledge, Apr. 9, 2018, *available at* https://www.publicknowledge.org/news-blog/blogs/is-the-gdpr-right-for-the-united-states ("We think that it would be impractical and ineffective to copy and paste the GDPR to U.S. law – the institutions and legal systems are just too different"); *Examining Safeguards for Consumer Data Privacy before the S. Comm. on the Judiciary & S. Comm. Commerce, Science, & Transportation*, 115th Cong. (Sept. 26, 2018) (testimony of Andrew DeVore, Amazon.com, Inc.) ("[M]eeting [GDPR's] specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and record-keeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices"); Niam Yaraghi, *A Case Against the General Data Protection Regulation*, Brookings, June 11, 2018, *available at* https://www.brookings.edu/blog/techtank/2018/06/11/a-case-against-the-general-data-protection-regulation/ ("GDPR could increase the cost of the services that consumers are so used to receiving free of charge… The other rarely discussed consequence of GDPR is the lower quality of services and products.").

10/ APEC Privacy Framework, *available at* https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

11/ *See, e.g.*, *Pacific Privacy Rules to Ease Trade Are Set to Take Off*, Bloomberg Law, Mar. 9, 2017, *available at* https://www.bna.com/pacific-privacy-rules-n57982084970/.

12/ *See* Ziyang Fan and Anil Gupta, *The Dangers of Digital Protectionism*, HARVARD BUS. REV., Aug. 30, 2018, *available at* https://hbr.org/2018/08/the-dangers-of-digital-protectionism ("Our view is that too much regulation will create, in effect, data islands, which will in turn prevent citizens and consumers trapped on those islands from enjoying the many benefits of tighter links to the global digital economy. These include access to digital goods and services, being part of global supply chains, accelerating and partaking in the fruits of innovation, and helping citizens access information, entertainment, and connectivity on a worldwide basis."); Joshua P. Meltzer and Peter Lovelock, *Global Data Flows and Connectivity Are Creating New Economic and Trade Opportunities*, Brookings, Mar. 20, 2018, *available at* https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/ ("Restrictions on cross-border data flows harm both the competitiveness of the country implementing the policies and other countries.").

the development of a uniform, national privacy framework, enforced and administered at the federal level by the FTC. A uniform, globally interoperable framework that provides consumers and companies alike with a consistent set of privacy rights and obligations can both strengthen privacy protection and advance competition and innovation in the global economy.

II. CONSENSUS IS EMERGING AROUND CERTAIN KEY PILLARS OF A NATIONAL PRIVACY POLICY

A number of industry groups and companies have highlighted their own position on privacy through the articulation of privacy 'principles' that should animate federal legislative efforts. Among those that have released legislative principles are the U.S. Chamber of Commerce,[13/] BSA | The Software Alliance,[14/] the Internet Association,[15/] and the Information Technology Industry Council,[16/] and other groups and companies may follow suit.[17/]

The diverse range of proposed privacy principles and frameworks that have emerged recently are grounded in a set of common concepts, even while there are differences in approaches to operationalizing some of these concepts. These concepts, discussed below, align closely with the principles highlighted in the RFC.

Parity. Consumers are best served by a single, national framework applied consistently across all businesses. Privacy proposals that impose different rules based upon the type of entity

---

13/ *See* Press Release, U.S. Chamber of Commerce, U.S. Chamber Releases Privacy Principles (Sep. 6, 2018), *available at*, https://www.uschamber.com/press-release/us-chamber-releases-privacy-principles.

14/ BSA Personal Data Protection Principles (2018)("BSA Principles"), *available at*, https://www.bsa.org/~/media/Files/Policy/BSA_2018PersonalDataProtectionPrinciples.pdf.

15/ *See* Press Release, Internet Association, Internet Association Proposes Privacy Principles For A Modern National Regulatory Framework (Sep. 12, 2018), *available at* https://internetassociation.org/internet-association-proposes-privacy-principles-for-a-modern-national-regulatory-framework/.

16/ *See* News Release, Information Technology Industry Council, Framework to Advance Interoperable Rules on Privacy (Oct. 22, 2018) ("ITI Framework"), *available at* https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf.

17/ In addition, in 2017, a group of leading ISPs and their associations released a set of privacy principles based upon the long-standing FTC privacy framework. *See* https://www.ncta.com/positions/isp-privacy-principles.

handling consumer data or the type of service being provided foster consumer confusion and distort competition.

Consumers want uniformity in how their data is protected. A national survey conducted by Public Opinion Strategies and Peter D. Hart found that people overwhelmingly, 94 percent, believe that all companies collecting online consumer data should be subject to the same set of privacy rules.[18/] A privacy framework that ensures consistency of protection, no matter what product or service consumers are using or whether the business model is paid or ad-supported, would give consumers greater confidence that their data is protected by all entities and would promote a level playing field in the use of consumer data to deliver innovative products and services.[19/] The RFC likewise recognizes that action to address consumer privacy should have "comprehensive application" in which any differences between business models and technologies are addressed in a flexible, fact-specific – rather than categorical – manner "which would allow for similar data practices in similar context to be treated the same rather than through a fragmented regulatory approach."[20/] A pro-competitive and technology- and sector-neutral privacy framework would provide the consistent protections consumers want. And it would encourage more companies to use consumer data in ways that benefit consumers – *i.e.*, to deliver services, improve products, innovate, and compete in the marketplace.

18/ *See* Memorandum from Public Opinion Strategies and Peter D. Hart to the Progressive Policy Institute, Key Findings from Recent National Survey of Internet Users (May 26, 2016), https://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf.

19/ *See Competition and Consumer Protection in the 21st Century*, Federal Trade Commission, Project No. P181201, Comments of Charter Communications, Inc., Aug. 20, 2018, at 4 ("Parity across every step of a consumer's online experience is particularly important to maintain consumer confidence. If certain entities are exempt from the online data privacy requirements or held to a lower standard, those entities will be able to collect and use personal information from consumers without their knowledge and will not be constrained by consumers' expectations regarding the privacy and security of personal data—a result that will only sow consumer doubt and confusion. For these reasons, it is essential that consumers have confidence that all entities in the internet ecosystem adhere to the same requirements governing the collection, use, disclosure and security of online personal data.").

20/ RFC at 10.

Transparency. All companies collecting consumer data should provide clear and conspicuous notice that describes the consumer data they collect, how that data is used, why such data may be shared with third parties, and the categories of entities with which such information is shared. Information about a company's privacy policies and data handling practices should be available prior to, or at the time of, collection of any consumer data, written in plain language that is easy-to-understand, and should be readily accessible to consumers at any time. Consumers also should be notified of any material changes to a company's privacy policy.

Consumer Control. The Administration's desired outcome is "a reasonably informed user, empowered to meaningfully express privacy preferences, as well as products and services that are inherently designed with appropriate privacy protections. . . ."[21/] To meet this objective, a national privacy framework should provide consumers with simple ways of controlling the use, transfer, and sale of their information while also preserving opportunities for beneficial uses of consumer data that lead to innovation, new products and capabilities, and customized services that consumers increasingly want.

To that end, consumers should have easy-to-understand privacy choices. The RFC asserts that controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making.[22/] These are sensible and responsible criteria for ensuring that consumers exercise purposeful and meaningful control of their personal information.

The RFC also states that decisions about "which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a

---

21/ *Id.* at 5.

22/ *Id.* at 7.

user's expectations and the sensitivity of the information."[23/] While a company should have the flexibility to use consumer data to engage in legitimate business activities that are consistent with the transaction or business relationship with its customers, consumers should have control over uses or disclosures of their data outside of that context.

Context has been a significant element of consent regimes in both the FTC privacy framework and in privacy principles previously endorsed by the Obama Administration. Under the FTC's long-standing approach, context is employed as an element of the control principle, in tandem with an expressly delineated opt-in/opt-out/implied consent choice architecture.[24/] Likewise, the 2012 privacy report issued by the Obama Administration relied on a "Respect for Context" principle as part of its approach to consumer control.[25/] This approach can offer greater flexibility and adaptability, particularly when applied to new products and services,[26/] but further guidance would advance greater certainty on how this concept is applied.

23/ *Id.* at 7.

24/ *See, e.g.*, *FTC Privacy Report*, *supra* n.4, at 38-39 ("The standard should be sufficiently flexible to allow for innovation and new business models but also should cabin the types of practices that do not require consumer choice. To strike that balance, the Commission refines the standard to focus on the context of the interaction between a business and the consumer. This new 'context of the interaction' standard is similar to the concept suggested by some commenters that the need for choice should depend on reasonable consumer expectations, but is intended to provide businesses with more concrete guidance."). *See id.* at 36-42, 47-50, 57-60.

25/ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 15 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("*2012 White House Privacy Framework*") ("Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data"). The CCPA also employs context as a component of its choice architecture. While specifying that consumers must be permitted to opt out of a covered entity's "sale" of the consumer's personal information to a third party, *see* CCPA, *supra* n. 7, § 1798.120(a), the CCPA exempts from such opt-out requirements uses by the business and transfers to "service providers" of personal information for a "business purpose," which is defined to include "an operational purpose that is compatible with the context in which the personal information was collected." *See id.*, § 1798.140(d), (t),(v).

26/ The FTC's approach to context is predicated on the notion that a business's relationship with its customer can evolve over time and encompass products, services and capabilities that may differ from those involved in the initial transaction with the consumer. *FTC Privacy Report* at 38-39. *See also 2012 White House Privacy Framework* at 16 (while context principle "emphasizes the importance of the relationship between a consumer and a company at the time consumers disclose data, it also recognizes that this relationship may change over time in ways not foreseeable at the time of collection. Such adaptive uses of personal data may be the source of innovations that benefit consumers.").

There is already some helpful guidance on uses of consumer data that have been recognized as consistent with the context of a business relationship,[27/] and NTIA could provide a more concrete vision of how a context-based permissions regime would operate – and be administered – in a manner that protects and benefits consumers. For example, the FTC privacy framework treats most first-party marketing as within consumer expectations and consistent with the context of a consumer's relationship with a company.[28/] Both the 2012 White House privacy framework and the CCPA accord similar treatment to first-party marketing.[29/] The APEC privacy framework also employs an analogous "compatible" use or purpose test in connection with the operation of its permissions regime, which could also be taken into account.[30/] Conversely, context should not be stretched to justify non-consensual uses of consumer data by

---

27/ *FTC Privacy Report* at 39-40 (providing "illustrative guidance regarding the types of practices that would meet the [context] standard and thus would typically not require consumer choice," including product or service provision and fulfillment of customer requests, fraud prevention and security, internal operations, product improvement and analytics, compliance with legal process and law enforcement requests, and most first-party marketing); *2012 White House Privacy Framework* at 17-18.

28/ *FTC Privacy Report* at 40 ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); FTC Staff, Comments on Notice of Proposed Rulemaking, WC Docket No. 16-106, at 15-16 (May 27, 2016) ("FTC Staff Comments") ("As the FTC has stated, consent may be inferred for collection, sharing, and use that is within consumer expectations – *i.e.*, consistent with the context of the transaction or the consumer's existing relationship with the business"). Consumers benefit from learning about discounted offers of broadband service from their video or telephony provider, as well as being apprised of broadband-related offerings (such as home security, music streaming, home energy management and other "Internet of Things" offerings), smart devices and related peripherals, and any content, games, software or other services, promotions, or discounts, offered by an online services provider or its affiliates or partners.

29/ *2012 White House Privacy Framework* at 17 ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it."); CCPA, § 1798.140(d)(5).

30/ APEC Privacy Framework, *supra* n.10, at 14, Part III, Sec. IV(25) (Subject to certain exceptions, consent obligation triggered by uses of personal information that are not undertaken to "fulfill the purposes of the collection and other compatible or related purposes" and stating that the "fundamental criterion for determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes").

third-party entities that are outside the context of the transaction and business relationship and thus unexpected by the customer.

It is essential that whatever role respect for context plays in the consent regime of a national privacy framework, it cannot be viewed or treated as simply a pretext to disadvantage, or create discriminatory regulatory burdens for, certain types of entities, services, or business models. While some large edge platform providers have suggested that consideration of context should be employed to favor their business model and categorize certain entities' uses of consumer data as inherently impermissible or more constrained,[31/] such an approach would be antithetical to innovation and consumer welfare, regulatory parity, competitive- and technological-neutrality, and basic fairness.[32/]

Security. Companies should take reasonable physical, technical, and administrative security measures to protect consumer data they collect or store. Such measures should be risk-based, taking into account factors such as the sensitivity of data, the size and complexity of a company's data operations, the costs of available tools and resources, and the potential for actual consumer harm from misuse.[33/] They should also keep pace with technological development.

31/ *See* Facebook Responses to Senate Commerce Committee Questions for the Record, June 8, 2018, at 14-15, *available at* https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Commerce%20Committee%20QFRs1.pdf.

32/ Indeed, several recent high-profile data breaches and data misuse controversies have arisen due to failures to adequately safeguard consumer data by companies that are totally or almost exclusively reliant on the monetization of consumer data.

33/ *See* "Commission Statement Marking the FTC's 50th Data Security Settlement," January 31, 2014 ("The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities").

There is already a considerable body of precedent that has developed around the FTC's enforcement of its "reasonable measures" standard for securing consumer data.[34/] That guidance not only informs good security practices by companies that handle consumers' data, it also provides insight into how case-by-case adjudication can effectively provide visibility and guidance regarding compliance with an outcome-based standard.[35/] Thus, NTIA can examine the evolution of the FTC's "reasonable measures" standard for security in an effort to help glean whether and how other outcome-based standards might evolve to produce more clarity and certainty for both consumers and regulated entities.

Right to Access, Delete, and Correct. A company that collects consumer data should provide consumers with access to a description of the categories of data the company collects from consumers as part of its transparency obligations, and all consumers should have the right to obtain access to the personally identifiable information they have provided directly to the company, as well as a reasonable opportunity to correct inaccuracies in such information, consistent with previous FTC guidance.[36/]

The RFC recognizes that users should have "qualified access [to] personal data that they have provided," which "should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligation, or the ability of consumers and third parties to exercise other rights."[37/] Additionally, as recognized by the FTC, the benefits of consumer access should be weighed against "the costs of providing

---

34/ *See id.* *See also* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2017 (Jan. 2018), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives.

35/ *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia Law Review 583 (2014).

36/ *See FTC Privacy Report* at 65-71.

37/ RFC at 8.

individualized access and correction rights."[38/] The RFC focuses on access to data that consumers "have provided" to companies that use their data, appropriately cabining the scope of the obligation in a reasonable and balanced manner. Companies should not be required to re-identify or otherwise manipulate de-identified data to fulfill any duties associated with this principle.

Consumers should also have a qualified right to delete personally identifiable information that they provide to a business and that is maintained in individually identifiable form, subject to certain exemptions for circumstances in which deletion of data would be problematic. Such exemptions should include provision of a good or service requested by the consumer, or reasonably anticipated within the context of the business's ongoing relationship with the consumer; completion of a transaction; fulfillment of consumer requests; security and fraud prevention; identification and repair of errors in functionality; preservation of the right to exercise free speech or another right provided for by law; compliance with the law; engagement in research for which the consumer has provided informed consent; fulfillment of solely internal uses, including sharing with service providers that support the business's use, reasonably aligned with the context of the relationship between the consumer and the business; and protection of the covered entity's rights or property and public health or safety.[39/]

Risk Management. NCTA agrees with NTIA that a uniform privacy framework should incentivize organizations to "mitigate the risk of harmful uses or exposure of personal data" while providing "the flexibility to encourage innovation in business models and privacy tools."[40/]

38/ *See FTC Privacy Report* at 65.

39/ This list of exceptions from a deletion requirement comports with the exceptions in other privacy laws, including those included in the CCPA. *See* CCPA, § 1798.105(d).

40/ RFC at 8. *See also* APEC Framework at Part III, Sec. I (20) ("[O]ne of the primary objectives of the Framework is to prevent misuse of information and consequent harm to individuals. Therefore, privacy protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement

Consumers do not benefit from rigid approaches that foster a checklist mentality and create cumbersome procedural burdens "without necessarily achieving measurable privacy protections."[41/] A framework that focuses on preventing harmful outcomes, rather than on prescribing a detailed set of specific rules and practices for companies to follow, has the potential to yield a better balance between the business considerations, consumer expectations, legal obligations, and potential privacy risks at stake in connection with data usage decisions.

As the RFC notes, a risk management model has been successful in improving the nation's cyber defense posture while ensuring flexibility for individual companies to take measures best suited to addressing and mitigating the cybersecurity risks associated with their business model and network environment. In the privacy context, de-identification can be a significant tool for companies to employ to manage privacy risks and reduce the potential for harm to consumers, while preserving beneficial uses of data.[42/]

To accurately assess risks while preserving the utility of data, precise and practical definitions of identifiable, pseudonymized, and de-identified data are critical. "Consumer data" that is deemed identifiable should not include attributes or information that can merely be associated with individuals but do not identify them, such as device identifiers, as long as these

---

mechanisms should designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, organizational controls should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection, use or transfer of personal information.").

41/ RFC at 10.

42/ Ann Cavoukian & Daniel Castro, Information and Privacy Commissioner Ontario, Canada, Big Data and Innovation, *Setting the Record Straight: De-Identification Does Work* (June 16, 2014), http://www2.itif.org/2014-big-data-deidentification.pdf. *See also FTC Internet of Things Report* at 37 (Noting that "maintaining data in de-identified form . . . helps minimize the individualized data companies have about consumers, and thus any potential consumer harm"); Stuart S. Shapiro, Homeland Security Systems Engineering and Development Institute, *Situating Anonymization Within a Privacy Risk Model*, at 3 (2012), https://www.mitre.org/sites/default/files/pdf/12_0353.pdf ("[A]nonymization is more accurately viewed as reducing the ability to associate information with specific individuals. To the extent the implicated characteristics of risks involve identity information and sensitive attributes, anonymization can serve to reduce privacy risk.").

attributes and identifiers are separated from consumers' identities using reasonable administrative, contractual, and technical controls.[43/] Companies should be encouraged to invest in tools, resources, and protocols to de-identify the data they employ for purposes of enhancing the customer experience, marketing products and services, delivering interest-based ads that help subsidize content and services, or other beneficial purposes.

The use of de-identified data, or even pseudonymous data, significantly reduces privacy risks.[44/] Even the GDPR recognizes the important benefits that come from de-identification and pseudonymization.[45/] Equating the risks and harms associated with the use of identifiable data with the use of de-identified data puts consumers' privacy at greater risk, by effectively deterring companies from committing resources to de-identifying data to protect their customers' privacy.[46/]

The RFC process could be useful in raising awareness of effective de-identification techniques and promoting incentives for more widespread use and adoption.[47/] In conjunction

---

[43/] Indeed, many of the significant concerns and criticisms of the CCPA stem from the Act's overly broad definition of personal information and its unclear definition of de-identified data.

[44/] Simson L. Garfinkel, *De-Identification of Personal Information*, NISTIR 8053, National Institute of Standards and Technology, at iii, 5 (2015) ("De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing, or publishing information. . . .all data exist on an identifiability spectrum. At one end (the left) are data that are not related to individuals . . . and therefore pose no privacy risk. At the other end (the right) are data that are linked directly to specific individuals. Between these two endpoints are data that can be linked with effort, that can only be linked to groups of people, and that are based on individuals but cannot be linked back"). *See also*, Future of Privacy Forum, *A Visual Guide to Practical De-Identification*, April 25, 2016, *available at* https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/.

[45/] *See, e.g.*, GDPR, Recital 28 ("The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.").

[46/] *FTC Privacy Report* at 22. *See also FTC Internet of Things Report*, at 43 ("[R]obust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way. Companies can use such de-identified data without having to offer consumers choices").

[47/] *See supra* at nn.42, 44. *See also De-identification Guidelines for Structured Data*, Information and Privacy Commissioner of Ontario, June 2016, *available at*, https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf; K El Eman, *A de-identification*

with NTIA, NIST has embarked on a process designed to develop a voluntary, enterprise-level framework to assist companies in managing their privacy risks – a project modeled after work in the cybersecurity context to assist industry in the management of cyber risks. Indeed, NIST has done important work already in the area of de-identification.[48/] In its *Guide to Protecting the Confidentiality of Personally Identifiable Information,* it defined "de-identified information" as data that has "had enough [personally identifiable information] removed or obscured . . . such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual," and it provided guidance regarding actual techniques companies could use to de-identify data.[49/] NTIA should look to incorporate this helpful, balanced, and practical NIST guidance into its national privacy framework.

Enforcement and Accountability. Privacy violations resulting in concrete harm to consumers should be subject to enforcement pursuant to the FTC's authority under Section 5 of the FTC Act to prevent unfair and deceptive acts and practices. The RFC likewise acknowledges that the FTC "is the appropriate federal agency to enforce consumer privacy with certain exceptions made for sectoral laws outside the FTC's jurisdiction, such as HIPAA."[50/]

The FTC has long been the nation's foremost consumer protection agency and enforcer of privacy and data security protections, and its longstanding privacy and data security

---

protocol for open data, International Association of Privacy Professionals, May 16, 2016, *available at*, https://iapp.org/news/a/a-de-identification-protocol-for-open-data/.

48/ *See supra* at n.44.

49/ Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* 4-4 (NIST, Special Publication 800-122 April 2010), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=904990.

50/ RFC at 11. It is critical to ensure that a company's privacy and security practices not be subject to dual or conflicting jurisdiction.

frameworks have successfully protected consumers and provided consistent standards. It should continue to be the lead enforcer in this arena. Where necessary, the FTC has not hesitated to pursue enforcement action, with over 500 privacy and data security cases to date under its Section 5 unfair and deceptive acts and practices authority.[51/] This "body of cases covers both offline and online information and includes enforcement actions against companies large and small," including actions addressing failures to dispose of sensitive consumer data properly, failures to secure consumers' personal information, deceptive online tracking of consumers, spamming consumers, installation of spyware on consumers' computers, violations of Do Not Call obligations, and various other forms of misconduct.[52/]

The FTC has been particularly active in ensuring privacy and data protection for consumers of technology and Internet-based products and services. In 2014, the FTC initiated administrative proceedings against social media company Snapchat, Inc., regarding the company's various deceptive claims about user privacy and the company's data collection, as well as the company's failure to secure data.[53/] In 2017, it initiated similar proceedings against laptop manufacturer Lenovo for pre-loading software on laptops that compromised security protections in order to deliver ads to consumers.[54/] This year, the FTC authorized a suit against electronic toy manufacturer VTech Electronics for collecting children's personal data without providing direct notice and obtaining parental consent.[55/] Just recently, the FTC reached a

---

[51/] FTC Privacy & Data Security Update, *supra* n.34, at 2.

[52/] FTC Staff Comments, *supra* n.28, at 4-5.

[53/] Complaint, *In re Snapchat, Inc.*, Docket No. C-4501 (Fed. Trade Comm'n May 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.

[54/] Complaint, *In re Lenovo, Inc.* Docket No. C-4636 (Fed. Trade Comm'n Sept. 5, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc.

[55/] Complaint, *United States v. VTech Electronics Ltd.,* Case No. 1:18-cv-0014 (N.D. Ill. Jan. 8, 2018), *available at* https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited.

settlement with ride-share company Uber Technologies, Inc, addressing deceptive conduct about the company's privacy and data security practices.[56/] And over the years, the FTC has established that it is up to the task of disciplining even the largest entities in this space, bringing enforcement actions against companies such as Google, Facebook, and Twitter.[57/]

In short, the FTC has proven itself as an effective and trusted steward of consumer privacy and data security, even as technology, markets, and consumer preferences have evolved. And its balanced approach to safeguarding privacy while promoting innovation and new services has protected consumers and generated clear and familiar rules of the road for industry. Notwithstanding its effective track record to date, the FTC must have the "necessary resources, clear statutory authority, and direction to enforce consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate."[58/] NCTA is prepared to work with NTIA, the FTC, and Congress to determine whether and, if so, which additional tools are necessary for an optimally effective FTC privacy enforcement framework.

Harmonization. A patchwork of conflicting state and local laws imposing varying obligations on how companies collect, use, and share consumer data will hurt the economy,

---

56/ Revised Complaint, *In re Uber Technologies, Inc.*, Docket No, C-4662 (Fed. Trade Comm'n Oct. 26, 2018), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf; Press Release, Federal Trade Commission Gives Final Approval to Settlement with Uber (Oct. 26, 2018), *available at* https://www.ftc.gov/news-events/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber.

57/ *E.g.*, Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; Press Release, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; Press Release, Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (June 24, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal.

58/ RFC at 11-12.

disrupt consumers' online experience, and thwart innovation. The RFC correctly identifies harmonizing the regulatory landscape as a key high-level goal for federal action.

A new national framework should promote greater consistency in consumer protection and avoid the fragmentation that "disincentivizes innovation by increasing the regulatory costs for products that require scale."[59/] Consumers will benefit from the predictability and consistency of a uniform national framework, in lieu of a confusing and conflicting set of inconsistent state-by-state regimes. Privacy protection should not vary simply because a consumer lives in Connecticut and works in New York, or takes a business trip from one state to another. As the RFC notes, we "are actively witnessing the production of a patchwork of competing and contradictory baseline laws," and this "emerging patchwork harms the American economy and fails to improve privacy outcomes for individuals."[60/] Preemption of state and local privacy laws and a bar on private rights of action will be key components of the effort to provide a uniform national privacy framework that protects consumers while promoting competition, innovation, and new services.

59/ RFC at 3.

60/ *Id.* at 9.

CONCLUSION

For the reasons set forth herein, NTIA should lead efforts to develop and enact a single national privacy framework for consumers, consistent with the principles discussed in these comments.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431
(202) 222-2445

November 9, 2018