Before the
U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Developing the Administration's Approach to Consumer Privacy	)	Docket No. 180821780-8780-01
	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association ("CTA")[1] is pleased to respond to the National Telecommunications and Information Administration's ("NTIA's") Request for Comments ("RFC") on developing the Administration's approach to consumer privacy.[2] CTA supports the Administration's continuing efforts to promote growth and innovation for the internet and the internet-enabled economy. In particular, in light of recent changes in privacy laws in Europe and California, and continued discussions in Washington, D.C. and around the country about the use and protection of personal information, CTA agrees with NTIA that "[t]he time is ripe" for the federal government "to provide the leadership needed to ensure that the United States remains at

[1] The Consumer Technology Association ("CTA")™ is the trade association representing the $377 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. 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 technologies. Profits from CES are reinvested into CTA's industry services.

[2] Department of Commerce, National Telecommunications and Information Administration, *Developing the Administration's Approach to Consumer Privacy*, Notice and Request for Public Comments, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC").

the forefront of enabling innovation with strong privacy protections."[3] Appropriate federal privacy legislation that preempts state law is the most effective way to achieve the Administration's goals of harmonizing the regulatory landscape and establishing a consistent risk- and outcome-based approach to privacy.

I. INTRODUCTION AND SUMMARY

CTA members recognize that the responsible use of data is critical to innovation in the 21st century economy and to achieving the consumer, economic, and societal benefits anticipated from new technologies, including artificial intelligence ("AI") and the Internet of Things. So too is consumer trust.

CTA commends NTIA, as well as the Departments of Commerce and the Administration at large, for continuing to prioritize collaborative work with the private sector and coordination across the government, including here to address the future of the U.S. privacy framework and ensure consumer trust in the digital marketplace. With fast-paced changes in technology and business models, government alone cannot effectively protect consumers or preserve room for innovation. CTA and many of its members are actively working with NTIA, the National Institute of Standards and Technology ("NIST"), and other government agencies, as well as within industry groups, to identify and develop the best path forward on privacy, security, and other challenges while also preserving an environment that promotes innovation. Together, the public and private sectors can find the necessary balance to maintain U.S. leadership in the technology industry.

As detailed below, CTA also supports the high-level goals identified in the RFC and looks forward to continued partnership with NTIA to achieve them.

[3] RFC at 48,600.

II. THE HIGH-LEVEL GOALS IDENTIFIED IN THE RFC ARE CRITICAL TO BALANCING PROTECTION OF CONSUMER INFORMATION WITH PRESERVATION OF CONSUMER-FOCUSED INNOVATION

The RFC seeks comment on high-level goals that would "be understood as setting the broad outline for the direction that Federal action should take" with respect to consumer privacy.[4] CTA strongly supports most of these goals.[5] A consumer privacy framework that achieves these goals would help maintain consumers' trust while also preserving and facilitating innovation that relies on the use of data collected from consumers. Therefore, the goals are appropriately defined to guide the Administration view of privacy, and they should provide a roadmap for Congress as it develops federal privacy legislation that would prevent—and preempt—a patchwork of state and local privacy and data security laws.

Harmonize the regulatory landscape. Privacy and security protections that are consistent across technologies, companies, agencies, and state borders are the bedrock prerequisite to ensure consumer trust, continue data-driven innovation, and realize its benefits. These benefits flow to consumers and businesses alike, generating tremendous gains for the economy and consumer welfare. NTIA correctly identifies the critical and emerging "need to avoid duplicative and contradictory privacy-related obligations placed on organizations."[6] The Administration should continue to promote—both domestically and abroad—consistent,

---

[4] RFC at 48,602.

[5] CTA does not take a formal position with respect to the RFC's proposed goal of incentivizing privacy research. *See* RFC at 48,602. CTA notes, however, that there has been a longstanding and productive exchange between policymakers and private, nonprofit, and academic privacy research initiatives. By way of example, each year the Future of Privacy Forum issues a formal call for privacy research and prepares a digest of winning papers for policymakers. *See* Future of Privacy Forum, *Privacy Papers for Policymakers*, https://fpf.org/privacy-papers-for-policy-makers/.

[6] RFC at 48,602.

interoperable, and robust data protections that also offer flexibility to companies that must operate under different legal regimes. The most effective way to achieve regulatory consistency and harmonization would be to adopt a federal privacy law that guarantees uniform national standards that maintain flexibility for companies to innovate.

Legal clarity while maintaining the flexibility to innovate. Relatedly, CTA agrees that, for a privacy framework, "[t]he ideal end-state would ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies…."[7] Legal clarity does not and should not mean detailed rules—indeed, prescriptive rules can actually undermine legal clarity while also inhibiting innovation. As CTA has explained elsewhere, government intervention can skew or suppress innovation, create market uncertainty, and ultimately harm consumers.[8] Legislation and regulation often fail to keep up with technology, and often rely—to the detriment of the marketplace and consumers—on regulators' static assumptions and predictions about where the market is going and what consumers want. At the same time, the absence of a federal baseline privacy law leaves a space that state-level legislation—the leading example of which is in California—and foreign rules may fill. Yet, internet services and technologies are inherently global; they generally are not offered on a state-specific, let alone country-specific, basis.

Any discussion of federal privacy legislation should be guided by the principles that have been crucial to the success of the data-driven economy, including maintaining the flexibility that allows companies to innovate and ensuring that, to supplement more flexible requirements

[7] RFC at 48,602.

[8] *See, e.g.*, Comments of the Consumer Technology Association Before the Federal Trade Commission, Project Number P181201, Docket Nos. FTC-2018-0049, FTC-2018-0051, FTC-2018-0055, FTC-2018-0056, at 19-20 (filed Aug. 20, 2018) ("CTA FTC Comments").

enshrined in law, industry can use self-regulation to address privacy concerns as they arise. Self-regulation can better address any new and emerging privacy concerns than static and specific laws and regulation and should be a key component of a high-level, flexible privacy framework. CTA and its members have a demonstrated history of proactively addressing emerging privacy and security concerns. For instance, in 2015, CTA's Health and Fitness Technology Division—which includes a diverse membership from across the digital health ecosystem—developed and released the *Guiding Principles on the Privacy and Security of Personal Wellness Data* to address privacy and security risks associated with wellness-related wearable devices.[9]

Comprehensive application. Government policies should avoid favoring specific technologies, industries, or business models. The internet ecosystem is too dynamic and interdependent to accommodate such distinctions. Any approach should focus instead on the type of data at issue, recognizing that sensitive data may warrant heightened protections. But similar data practices involving similar types of data must be treated the same. Accordingly, CTA agrees with NTIA that any new consumer privacy action should consistently apply to all companies not otherwise covered by sectoral laws, and that differences in business models should be not be addressed through business model-specific—or technology-specific—privacy frameworks.[10] Although new technologies can raise questions about new concerns and risks, policy should follow technology-neutral principles, allowing consumers and competition to address such concerns, instead of technology-specific regulations that can stifle innovation and

[9] *See* CTA, *Guiding Principles on the Privacy and Security of Personal Wellness Data*, http://www.cta.tech/healthprivacy; CTA, *Association Unveils First-of-Its-Kind, Industry Supported Principles on Wellness Data Privacy* (Oct. 26, 2015), https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/Association-Unveils-First-of-Its-Kind,-Industry-Su.aspx.

[10] RFC at 48,602.

distort the marketplace. This approach also will be adaptable to new technologies, helping to ensure that consumers remain protected as the digital economy evolves.

Risk- and outcome-based approach. CTA supports NTIA's proposed goal of following a risk- and outcome-based approach to privacy.[11] In general, legal requirements and enforcement should be focused on addressing specific, concrete privacy harms. This focus, in turn, helps to ensure that companies (and enforcement agencies and regulators) use their resources efficiently.

In addition, and relatedly, a critical aspect of a risk- and outcome-based approach is the sensitivity of data and how it is used. Consumer expectations change based on which information is provided and whether the uses of data are compatible with the consumers' relationship with the companies that hold their data—factors sometimes referred to as "context." Indeed, consumers expect particular outcomes—for instance, consumers that use location-based services and apps expect that their location information will be used to deliver such services, reducing privacy risk if used only to deliver those services. In contrast, the collection and use of sensitive data in ways that may not be obvious to consumers can create privacy risk, and therefore may appropriately need additional notice and clear consent.

While privacy laws and enforcement should be specifically focused on concrete consumer harm, Administration efforts to develop voluntary tools can appropriately address privacy risk management more broadly. In this regard, CTA has applauded NIST's effort to develop a Privacy Framework as a voluntary tool that could help organizations better identify, assess, manage, and communicate about privacy risks to individuals.[12] So long as NIST's effort focuses on

[11] RFC at 48,602.

[12] *See* Comments of the Consumer Technology Association Before the Department of Commerce, National Institute of Standards and Technology, on NISTIR 8228 (Draft): Considerations for Managing Internet of Things (IOT) Cybersecurity and Privacy Risks, at 9-10 (filed Oct. 24, 2018).

a framework that companies may use to guide their own privacy risk mitigation efforts and data collection and use decisions, it provides an appropriate complement to NTIA's development of a policy approach.

Interoperability. Interoperability and seamless cross-border data flows are critical for today's global digital economy and the continued strength and growth of America's digital economy. As new, disparate privacy regimes arise in different jurisdictions, the U.S. government should ensure that data protection laws do not become trade barriers. Arrangements such as the EU-U.S. Privacy Shield and APEC Cross-Border Privacy Rules enable cross-border data flows by ensuring consistent, robust data protections, while also offering flexibility to companies that must operate under different legal regimes. CTA therefore encourages NTIA to work with the rest of the Commerce Department and the Administration in support of these data transfer mechanisms.[13]

FTC enforcement. The FTC is the appropriate federal agency to enforce consumer privacy.[14] Over the last twenty years, the FTC has generally—though not without exception—used its privacy authority to take action against companies whose practices cause significant harm to consumers. The FTC has brought over 500 data privacy and security enforcement actions, and it has a deep bench of experienced and tech-savvy staff who are uniquely suited to address these issues. The FTC's enforcement approach to privacy permits innovative uses of data but ensures that consumers are protected against conduct that harms them. Accordingly, the Administration's approach should support and reinforce the FTC's focus on stopping concrete

[13] *See also* Comments of the Consumer Technology Association Before the Department of Commerce, National Telecommunications and Information Administration, Docket No. 180124068-8068-01, at 3-6 (filed July 17, 2018) (discussing the importance of the free flow of data across borders).

[14] *See* RFC at 48,602.

harms and the agency should use its resources to bring actions against and stop practices in the marketplace that cause such harms to consumers.

Scalability. CTA commends NTIA for including the size of a business and its role in handling personal information as considerations in its privacy approach. Privacy frameworks around the world do not sufficiently account for differences in resources and capabilities among companies of different types and sizes, and as a result may harm small businesses' ability to innovate and compete with more established companies. CTA agrees with NTIA that small businesses that collect little personal information and do not maintain sensitive information about their customers should not be the primary targets of privacy-enforcement activity.[15] But even some small businesses that collect a fair amount of personal information should not face burdensome privacy compliance costs and liability risks—as long as they do not collect sensitive personal information, and do not use or share the personal information they collect in ways likely to harm consumers.

Indeed, burdensome, unjustified privacy compliance costs—such as those imposed by regimes abroad—could prevent innovative startups from even proving their technologies and services in the marketplace. By way of example, several of the most promising startups last year at the Eureka Park Marketplace, the flagship startup area at CES, intend to use sensors and data to make consumers, or even their pets, safer.[16] Red tape imposed ostensibly in the name or privacy—including but not limited to a patchwork of varied privacy and data security requirements—could keep these companies from launching, growing, and succeeding, causing great cost to consumers and society at large.

---

[15] *See* RFC at 48,603.

[16] *See* Consumer Technology Association, *The Best of Eureka Park* (Apr. 5, 2018), https://www.cta.tech/News/i3/Articles/2018/March-April/The-Companies-of-Eureka-Park.aspx.

III. NTIA SHOULD CONTINUE TO COLLABORATE WITH INDUSTRY TO IDENTIFY PRIVACY OUTCOMES THAT PROMOTE INNOVATION AND PROTECT CONSUMERS

A wide range of stakeholders, including companies and industry organizations, are developing and publishing proposed privacy principles in light of recent legal and marketplace developments.[17] As part of the development of the Administration's approach, CTA encourages NTIA to review these various proposals and continue to engage with these companies and organizations regarding the proper principles to underlie the U.S. privacy framework—*i.e.*, the "set of user-centric privacy outcomes … that should be produced by any Federal actions on consumer-privacy policy."[18] Ultimately, CTA encourages NTIA to articulate privacy principles that represent a broad consensus and support the foundation of its own proposed list of privacy outcomes. For instance, the time-tested technology-neutral privacy framework based on transparency, consumer choice, security, and heightened protections for sensitive data should serve as the foundation for any privacy framework.[19] To propose additional privacy principles and outcomes, NTIA should ensure that such proposed outcomes have widespread support.

---

[17] *See, e.g.*, U.S. Chamber of Commerce, U.S. Chamber Privacy Principles (Sept. 6, 2018), https://www.uschamber.com/issue-brief/us-chamber-privacy-principles; Google, Framework for Responsible Data Protection Regulation (Sept. 2018), https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf; ITI, Framework to Advance Interoperable Rules (FAIR) on Privacy (Oct. 22, 2018), https://www.itic.org/dotAsset/feb6ab98-7c3b-421b-9f92-27528fa4c4f2.pdf; Kathy Grillo, Verizon, Privacy: It's time for Congress to do right by consumers (Oct. 9, 2018), https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers; BSA, BSA Personal Data Protection Principles, (Sept. 2018), https://www.bsa.org/~/media/Files/Policy/BSA_2018PersonalDataProtectionPrinciples.pdf; Internet Association, IA Privacy Principles For A Modern National Framework (Sept. 12, 2018), https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/; *see also* Intel, Intel's Approach to Privacy, https://usprivacybill.intel.com/ (proposing draft privacy legislation).

[18] RFC at 48,601.

[19] *See, e.g.*, CTA FTC Comments at 8 (stating key principles that should continue to underlie the FTC's approach to privacy and data security).

Once NTIA has identified consensus-based principles, it should endorse the incorporation of such principles in preemptive and forward-looking federal privacy legislation.

IV. CONCLUSION

CTA appreciates NTIA and the Department of Commerce's thoughtful and measured approach to considering a federal approach to privacy that would promote growth and innovation for the internet and the internet-enabled economy. Particularly in light of recent changes in privacy laws in Europe and California, CTA agrees with NTIA that it is an appropriate time for the U.S. federal government to provide leadership ensuring the United States remains at the forefront of enabling innovation with strong privacy protections. To best do so, CTA believes NTIA and the Administration should endorse federal privacy legislation that harmonizes the regulatory landscape and establishes a flexible and consistent risk- and outcome-based approach to privacy.

Respectfully submitted,

CONSUMER TECHNOLOGY
ASSOCIATION

By: */s/ Rachel S. Nemeth*

Rachel S. Nemeth
Director, Regulatory Affairs

Michael Petricone
Sr. VP, Government and Regulatory Affairs

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

November 9, 2018