Before the
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of Developing a Privacy Framework	))))	Docket No. 181101998-8997-01

COMMENTS OF CONSUMER TECHNOLOGY ASSOCIATION

Michael Petricone
Sr. VP, Government and Regulatory Affairs

Rachel S. Nemeth
Director, Regulatory Affairs

Consumer Technology Association

January 14, 2019

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of Developing a Privacy Framework	))))	Docket No. 181101998-8997-01

COMMENTS OF
CONSUMER TECHNOLOGY ASSOCIATION

Consumer Technology Association ("CTA")[1] welcomes the opportunity to provide input to the National Institute of Standards and Technology ("NIST") as the agency works with stakeholders to develop a framework to improve organizations' management of privacy risk arising from the collection, storage, use, and sharing of personal information (the "Privacy Framework").[2] CTA supports NIST's development of a Privacy Framework and encourages NIST to rely on existing standards and guidelines, establish guidance on considering the benefits of data use in risk management decisions, and incorporate reference to existing privacy standards, guidelines, and organizational practices.

[1] Consumer Technology Association (CTA)™ is the trade association representing the $398 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 Institute for Standards and Technology, *Developing a Privacy Framework*, Request for Information, 83 Fed. Reg. 56,924 (Nov. 14, 2018) ("RFI").

I. INTRODUCTION

CTA members develop and build products and services based on Artificial Intelligence, the Internet of Things, and other technologies that deliver significant benefits to consumers, the economy, and society as a whole. Fully realizing the benefits of these data-dependent products and services requires companies to use data responsibly and to build and maintain consumer trust. Accordingly, CTA members have strong incentives to ensure that their uses of personal information meet their obligations under applicable laws as well as consumers' privacy expectations. As consumer technologies have become more data-intensive, CTA members' data governance policies, practices, and processes address an increasingly broad range of consumer-facing and internal considerations.

CTA believes, as noted in comments filed with the National Telecommunications and Information Administration ("NTIA") late last year, that "in light of recent changes in privacy laws in Europe and California . . . 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."[3] The optimal way to achieve these goals is through federal privacy legislation that harmonizes the regulatory landscape and establishes a flexible and consistent risk- and outcome-based approach to privacy. Voluntary frameworks, however, also can and should be a source of guidance to companies as they design, implement, and maintain consumer privacy protections.[4]

[3] Comments of Consumer Technology Association, *Developing the Administration's Approach to Consumer Privacy*, Before the National Telecommunications and Information Administration, Docket No. 180821780-8780-01, at 10 (filed Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/cta_comments_in_response_to_ntia_privacy_rfc-c1.pdf.

[4] *Id.*

CTA therefore applauds NIST's effort to create a flexible, risk-based, outcome-based, and cost-effective tool to help increase consumer trust.[5] A framework that companies and other organizations can use to guide their own privacy risk mitigation efforts and data collection and use decisions provides a helpful complement to discussions at NTIA,[6] the Federal Trade Commission ("FTC"),[7] and elsewhere about the legal and policy framework for consumer privacy in the United States.

II. NIST SHOULD BUILD ON THE SUCCESS OF THE CYBERSECURITY FRAMEWORK, AS WELL AS OTHER EXISTING GUIDANCE AND STANDARDS

NIST's initiative to develop the Framework for Improving Critical Infrastructure Cybersecurity (the "Cybersecurity Framework")[8] through a partnership with multiple critical infrastructure sectors is widely regarded as a resounding success. A key to this success is that the Cybersecurity Framework does not provide a "one-size-fits-all" solution and instead outlines a voluntary, flexible approach that organizations can adapt to their current practices, business models, assets, and other variables.

---

[5] *See* RFI at 56,824.

[6] As noted in the RFI, NTIA is undertaking a parallel effort to develop the Administration's approach to privacy. *See* RFI at 56,824 n.2. *See also* 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).

[7] As part of its series of hearings on competition and consumer protection, the FTC plans to host a hearing on consumer privacy issues on February 12-13, 2019. *See* FTC, FTC Hearings on Competition and Consumer Protection in the 21st Century, An FTC Event on February 12-13, 2019, *available at* https://www.regulations.gov/contentStreamer?documentId=FTC-2018-0098-0003&contentType=pdf.

[8] *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, https://www.nist.gov/cyberframework/framework (2018).

NIST should use the process to develop the Cybersecurity Framework and certain of its attributes as a model for the Privacy Framework.[9] Ensuring that a framework is voluntary, flexible, and scalable is just as important in the privacy context as in cybersecurity; enterprises of all shapes and sizes must consider widely varying business models, industries, technologies, and other factors to assess and manage their privacy risks.[10] In addition, the Privacy Framework should focus on outcomes rather than prescribe specific practices or approaches.[11] Otherwise, the Privacy Framework could favor certain technologies and business models, curbing innovation and distorting competition. Moreover, a flexible framework – as opposed to an overly prescriptive one – is more likely to remain relevant as technologies, services, and the marketplace change over time, allowing the Privacy Framework to retain its utility.

The Privacy Framework, like the Cybersecurity Framework, should also rely on widely adopted standards, guidelines, and other sources of privacy risk management practices. As the RFI notes, using such sources as the foundation of the Privacy Framework will advance NIST's goal of "identif[ying] common practices across contexts and environments" to help organizations "achieve positive privacy outcomes."[12] Nevertheless, to ensure the adaptability and scalability of the Privacy Framework, it is critical for NIST to ensure that privacy guidance incorporated into the Privacy Framework is appropriate for commercial and government entities. The private and public sectors face markedly different privacy issues, including different consumer expectations and legal obligations. In particular, consumers expect and understand that many companies use

[9] RFI at 56,826 (asking whether any aspects of the Cybersecurity Framework could be a model for the Privacy Framework, and about the relationship between the two).

[10] *Id.* at 56,825 (proposing minimum attribute of adaptability to many different organizations, technologies, lifecycle phases, sectors, and uses).

[11] *Id.* (proposing that the Privacy Framework be risk-based, outcome-based, voluntary, and non-prescriptive).

[12] *Id.* at 56,826.

data to provide and improve their services, and that companies often provide these services at no cost because they earn revenue through advertising. By contrast, government entities do not rely on advertising-supported models. As a result, privacy standards developed for the private sector may address practices that government agencies do not use, and conversely, government-focused standards might not address common private sector practices. These differences are less stark in cybersecurity; government or commercial entities share the fundamentally similar goal of identifying and mitigating cybersecurity risks and threats and preventing attacks in ways that are practical and effective based on the circumstances. Distinguishing between commercial and government settings was not necessary in the Cybersecurity Framework, but it is of central importance to the Privacy Framework.

III. THE PRIVACY FRAMEWORK SHOULD EXPLICITLY INCORPORATE THE CONSIDERATION OF DATA USE BENEFITS ALONG WITH PRIVACY RISKS

The Privacy Framework should explicitly account for and support the benefits to consumers, competition, and society of responsible data use and collection, and should not focus exclusively on privacy risk. Consideration of the benefits of responsible data use is integral to many companies' risk management processes. A framework that does not take benefits into account would offer an incomplete picture of the considerations needed to identify, consider, and mitigate privacy risk associated with the next generation of data-driven technologies. This omission could lead users of the Privacy Framework to undervalue the benefits of data-driven innovations for consumers' convenience, health, and safety. Including in the Privacy Framework guidance to help organizations consider the benefits of responsible data collection and use while also taking steps to mitigate privacy risk would avoid this potential pitfall.

IV. THE PRIVACY FRAMEWORK SHOULD INCORPORATE ESTABLISHED PRINCIPLES, ATTRIBUTES, AND PRACTICES, INCLUDING THOSE CURRENTLY PRACTICED BY CTA MEMBERS

CTA supports including in the final Privacy Framework the attributes NIST identified in the RFI, namely that the Privacy Framework is (i) consensus-driven; (ii) in accessible language; (iii) adaptable to different organizations and technologies; (iv) risk-based, outcome-based, voluntary, and non-prescriptive; (v) readily usable as part of an enterprise's broader risk management strategy; (vi) compatible with other privacy approaches; and (vii) a living document.[13]

As NIST considers specific practices to include in the Privacy Framework, CTA encourages NIST to consult with stakeholders about the practices they use in their management of personal information. CTA members use myriad practices in their privacy programs, and the mix of practices used by a particular company reflects a wide variety of factors, including its size, legal and regulatory obligations, and the scale, complexity, and sensitivity of its personal information operations. For instance, companies might collect data about a particular individual, data that is not linked to a particular individual, or both; each of these scenarios raises different potential privacy risks and concerns. CTA members' practices also may include developing internal and customer-facing privacy notices and policies; adopting privacy-by-design practices; instituting robust oversight and compliance programs, including by naming a chief privacy officer; establishing controls and policies governing the sharing of personal data with third parties; and fostering comprehensive data security programs, which are often informed by the Cybersecurity Framework. Such practices are compatible with existing legal and regulatory regimes, and thus their inclusion in the Privacy Framework would enable widespread adoption.

[13] *Id.* at 56,825.

V. CONCLUSION

The Privacy Framework promises to provide a valuable resource for companies to use in connection with their management of privacy risks. CTA appreciates NIST's collaborative approach and looks forward to working with other stakeholders and providing further input as the Privacy Framework development process moves forward.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

Michael Petricone
Sr. VP, Government and Regulatory Affairs

Rachel S. Nemeth
Director, Regulatory Affairs

January 14, 2019