ncta
The Internet & Television Association

Rick Chessen
Chief Legal Officer
Senior Vice President, Legal & Regulatory Affairs

January 14, 2019

Ms. Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: Developing a Privacy Framework – Docket No. 181101997-8997-01

Dear Ms. MacFarland:

NCTA – The Internet & Television Association (NCTA)[1] hereby submits these comments in response to the request for information (RFI) from the National Institute of Standards and Technology (NIST) in the above-captioned proceeding. NIST seeks input in connection with the development of a voluntary framework "that can be used to improve organizations' management of privacy risk for individuals arising from the collection, storage, use, and sharing of their information." [2/]

NIST envisions the Privacy Framework to function as a tool to assist with enterprise risk management. NCTA represents an industry that has many years of experience with prioritizing consumer privacy, successfully managing privacy risks, and using information in a privacy-protective manner to innovate and deliver high-quality video, Internet, and other communications products and services. NCTA applauds NIST's efforts to help companies manage privacy risks associated with the handling of personal information and offers the following suggestions for NIST's consideration as it develops its framework.

1/ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving 80 percent of the nation's cable television households and more than 200 cable program networks. The cable industry is the nation's largest 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/ *Developing a Privacy Framework*, National Institute for Standards and Technology, 83 Fed. Reg. 56824 (Nov. 14, 2018).

Consumer-Facing Companies Have Strong Incentives to Protect Users' Privacy. As a threshold matter, NIST should recognize that, for consumer-facing entities like NCTA member companies, assessing and addressing privacy risks is driven not simply by the requirements of applicable law. These companies have a 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 Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have recognized, respecting consumer privacy and properly safeguarding consumer data is a key component to successfully maintaining that customer relationship.[3/] NCTA's views on privacy risk management reflects its members' long track record of safeguarding the privacy of their customers; implementing controls to ensure data is used properly, lawfully, and in line with consumers' expectations; and delivering advanced products and services to consumers.

NIST Should Be Mindful of the Already Complex Legal Landscape. As the RFI acknowledges, new digital products and services made possible by the Internet of Things, artificial intelligence, and ubiquitous mobile and social media platforms not only offer enhanced customization, increased mobility, and advanced features and capabilities, they also present new privacy challenges as well. These challenges include complex technological, operational, user interface, and data management and storage issues, and their complexity is amplified by an array of overlapping – and very often conflicting – legal and regulatory privacy regimes at the federal, state, and international level. NCTA continues to urge NTIA and others to eliminate such conflicts and complexity by encouraging Congress to adopt national privacy requirements that are applicable to all businesses in a uniform and non-discriminatory manner. [4] We also commend NIST for focusing on developing a voluntary, risk-based framework to assist businesses with their

---

3/ *Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION, at 38-41 (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, and calling for more flexibility and reliance on implied consent when the user has such a relationship with the business and when the context of the data collection and use is consistent with that relationship; for example, it is within the context of the relationship between a customer and a business for the business to use the customer's personal data to market the customer other services offered by the business, so privacy restrictions should be reduced); *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.").

4/ Department of Commerce, National Telecommunications and Information Administration, *Developing the Administration's Approach to Consumer Privacy*, Docket No. 180821780–8780–01, 83 FR 48600, (Sept. 26, 2018) Comments of NCTA, Nov. 9, 2018 at 3, 7, and 19. ("*NTIA Privacy RFC*").

privacy compliance, and for its stated commitment to avoid prescribing specific measures and approaches that would inadvertently add to such complexity.

NIST should continue to make clear that the framework is not intended to have any binding legal or regulatory effect, nor is it intended to endorse any particular legal regime. Rather, it is meant to complement existing privacy protocols and practices. Indeed, it will be critical for NIST to ensure that its privacy framework interacts seamlessly with the wide variety of privacy legal regimes in effect today, and any privacy regime that may be adopted in the future. To that end, NIST should focus on the *process* of managing privacy risks, rather than prescribing additional substantive privacy obligations and compliance measures for safeguarding privacy rights. In addition, it will be important for NIST to recognize that measures and risk management processes that may be important for Federal agencies may not be appropriate in a privacy framework intended for private entities. Federal agencies are subject to different legal and regulatory requirements than are organizations in the private sector, and the data they collect and the purposes for which they collect the data are necessarily going to be different. As a result, processes that might be suitable for Federal agencies could merely increase compliance costs for the private sector – including by serving as a drag on innovation – without providing any material privacy improvements to consumers.

NIST Should Follow the Flexible Approach It Took Developing the Cybersecurity Framework. Just as the NIST Cybersecurity Framework was instrumental in identifying best practices and voluntary measures that can help companies operationalize security risk management and security-by-design, a NIST Privacy Framework has the potential to assist companies' efforts to institutionalize privacy-by-design and privacy risk management.

The NIST Cybersecurity Framework is in many respects the seminal document on cybersecurity risk management. However, it was developed in the context of a relatively sparse legal and regulatory landscape governing cybersecurity. In contrast, any privacy framework developed by NIST will be forged against the backdrop of myriad laws and regulations governing the manner in which companies across a wide variety of sectors address privacy issues.

Notably, risk management is an integral component of existing privacy regimes. The FTC, the primary enforcer of privacy rights in the United States for over four decades, has stated that "a risk-based approach is in the FTC's institutional DNA," embodied within the core prohibition against unfair or deceptive acts or practices.[5/] Under Section 5 of the FTC Act, "an act or practice is unfair only if it causes or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves."[6/] Thus, the FTC's key enabling statute requires the Commission to "perform a cost-benefit analysis before

---

5/ *NTIA Privacy RFC*, Comments of FTC Staff, Nov. 9, 2018, at 11.

6/ Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, May 27, 2016, at 3. *See also* 15 U.S.C. § 45(n).

finding a practice is unfair."[7/] NCTA also strongly supports NIST's goal of coordinating its work in this proceeding with NTIA, which is seeking to advance a risk management approach to privacy as well.[8/]

As with the NIST Cybersecurity Framework, it is critical to keep in mind that there are no one-size-fits-all approaches to privacy risk management. Different companies face different types of privacy risks and issues, due to their size, the type and scope of their data uses, and the nature of their relationship with the consumers and entities whose data they collect and use. The NIST Cybersecurity Framework succeeded precisely because NIST recognized the importance of having a flexible, voluntary framework that individual organizations could adapt to their particular business model and circumstances. This same approach should be followed in the NIST Privacy Framework.

NIST Can Best Achieve an Outcome-Based Approach by Focusing on Processes, Not Prescriptive Standards. In examining the business processes for managing privacy risks, NIST should focus on identifying organizational measures, practices, tools, and resources that can help an enterprise pinpoint and prevent potentially harmful privacy outcomes, rather than on setting forth a detailed set of specific procedures and practices for companies to follow. There is a continuum of risks associated with different types of collection, use, and disclosure of consumer data. For example, information that poses little or no risk of being linked to a specific individual carries a different risk profile than information that identifies a known individual.[9/] A risk management framework should materially distinguish between the risk profile attached to uses of individually identifiable data and the profile of data that is not associated with a specific person, and take account of the various points along the spectrum of identifiability.[10/] Equating the risks and harms associated with the use of identifiable data

---

7/ *NTIA Privacy RFC*, Comments of FTC Staff, Nov. 9, 2018, at 12.

8/ *NTIA Privacy RFC* at 48602 ("Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools").

9/ *See, e.g., Internet of Things, Privacy & Security in a Connected World*, FTC Staff Report, January, 2015, at 37 ("*FTC Internet of Things Report"*) (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.").

10/ 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. . . . [A]ll 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/.

with the use of de-identified data puts consumers' privacy at greater risk, by effectively deterring companies from committing resources to de-identifying personal data to protect their customers' privacy.[11/] NIST has done important work already in the area of de-identification, and can build upon that work in this proceeding.[12/]

NIST Should Help Companies Balance Risk Mitigation with Innovation. By its nature, risk *management* does not seek to eliminate all potential risk or prevent all possible harms, since such an objective is unattainable and heightens the likelihood of unnecessarily increasing costs, thwarting innovation, and harming consumer welfare.[13/] It is instead focused on identifying and prioritizing risks so that the organization can address them in a way that is proportionate with the potential harms to consumers.[14/] NIST's risk management model should assist organizations with appropriately calibrating the competing concerns at stake in connection with any particular data collection, use, or disclosure. Risk management is fundamentally a balancing test that involves identifying benefits, fostering awareness of potential harms and their severity, prioritizing actions,

---

11/ *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").

12/ In its *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, NIST 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.

13/ *Cf.* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 45 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("The increasing quantities of personal data that [networked] technologies subject to collection, use, and disclosure have fueled innovation and significant social benefits"); *Report to the President, Big Data and Privacy: A Technological Perspective*, President's Council of Advisors on Science and Technology, 11-14 (May 2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (Highlighting "the enormous benefits that big data can provide and also the privacy challenges that may accompany these benefits"); *Big Data: Preserving Opportunities, Preserving Values*, Executive Office of the President, 39-41 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("*White House Big Data Report*") (Noting the "enormous benefits associated with the rise of profiling and targeted advertising and the ways consumers can be tracked and offered services as they move through the online and physical world").

14/ APEC Privacy Framework, *available at* https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015), Part III, Sec. I(20) ("[A]cknowledging the risk that harm may result from [] misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information"); *id.* Part III, Sec. VII(28) ("Personal information controllers should protect personal information that they hold with appropriate safeguards against risks. . . . Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment").

incorporating applicable legal and regulatory obligations, mitigating known risks, and assessing and refining an organization's privacy risk management practices.

FTC Commissioner Noah Phillips recently noted that one of the key benefits of what he termed the "American risk-based approach to privacy" is that "it has both targeted the areas of greatest privacy need and still permitted a tremendous amount of innovation."[15/] Amid growing concerns regarding the security and privacy of consumer data, the development of a voluntary privacy risk management framework that can help enterprises organize and operationalize their practices, protocols, and tools for protecting data could be a highly valuable resource that maximizes consumer welfare, competition, and innovation far better than costly, burdensome, and overly-prescriptive data privacy regimes.[16/] Ultimately, however, the utility of such a framework will be determined not just by its substance and adaptability, but also by the flexibility - and amenability to risk-management principles - of the privacy regime to which it is being applied. Accordingly, NIST should work in close concert with the effort by NTIA to promote adoption of a national policy predicated upon an outcome-based, risk management approach to privacy protection.

NCTA appreciates NIST's thoughtful approach to developing a voluntary framework for management of privacy risks and we look forward to collaborating with NIST on this important resource.

Sincerely,

Loretta Polk
Vice President &
Deputy General Counsel

Rick Chessen
Senior Vice President
Law & Regulatory Policy

15/ *Keep It: Maintaining Competition in the Privacy Debate*, Prepared Remarks of FTC Commissioner Noah Phillips, Internet Governance Forum USA, at 11 (July 27, 2018).

16/ *See* "Beware the Big Tech Backlash," *Wall St. Journal*, Dec. 19, 2018 ("Ghostery speculates that Google and Facebook had more resources to devote to compliance, and that website owners dropped smaller advertisers that may have struggled to prove compliance. Either way, the early effect of the [GDPR] has been to entrench the advertising duopoly of Google and Facebook); "Google and Facebook Likely to Benefit from Europe's Privacy Crackdown," *Wall Street Journal*, April 23, 2018; "GDPR Will Make Big Tech Even Bigger," *Forbes*, June 26, 2018.