From: Annette Rojas <ARojas@NCTA.com>
Sent: Thursday, October 24, 2019 4:57 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Loretta Polk <LPolk@NCTA.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Thank you.

Annette L. Rojas

Department Coordinator – Legal & Regulatory Affairs

NCTA – The Internet & Television Association

o (202) 222-2361 • e arojas@ncta.com

The Internet & Television Association
25 Massachusetts Avenue, NW | Suite 100
Washington, DC 20001
(202) 222-2300

Legal Department
(202) 222-2445

October 24, 2019

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

Subject: Privacy Framework Preliminary Draft

Dear Ms. MacFarland:

NCTA — The Internet & Television Association (NCTA) hereby submits this letter in response to the request for comments from the National Institute of Standards and Technology (NIST) regarding the Preliminary Draft of the NIST Privacy Framework.[1/]

In its comments on the Request for Information (RFI) preceding the development of the Preliminary Draft, NCTA emphasized the need for NIST to adhere to the foundational principles that made the Cybersecurity Framework successful and useful: collaboration, voluntariness, and flexibility.[2/] NCTA also highlighted the value of identifying organizational processes that can help an enterprise pinpoint and prevent potentially harmful privacy outcomes, rather than setting forth a detailed set of specific procedures, practices, and controls for companies to follow. These guideposts are especially critical because the enterprises that would seek to utilize the Privacy Framework are diverse in their size, scope, business model, relationship to individual consumers, and resources – and are subject to a widely varying range of obligations, and sector-specific legal requirements.

NIST envisions the Privacy Framework as a "risk management tool."[3/] Privacy risk management consists of a "set of processes" that aid organizations in understanding "how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks."[4/] NIST views privacy risk assessments

---

1/ *NIST Privacy Framework: A Tool for Improving Enterprise Privacy Risk Management*, Preliminary Draft, National Institute for Standards and Technology, Sept. 6, 2019 ("Preliminary Draft").

2/ Comments of NCTA – The Internet and Television Association, Developing a Privacy Framework – Docket No. 181101997-8997-01, Jan. 14, 2019, https://www.nist.gov/sites/default/files/documents/2019/02/04/ncta_loretta_polk_rick_chessen_508.pdf.

3/ Preliminary Draft at 12.

4/ *Id.* at 7.

as a "sub-process" of privacy risk management that, where necessary, "assists organizations in connection with identifying, evaluating, prioritizing and responding to specific privacy risks."[5/] The Preliminary Draft correctly notes that organizations can and will "choose to respond to privacy risks in different ways, depending on the potential impact to individuals and resulting impacts to organizations."[6/] Thus, the Privacy Framework is designed to function as a voluntary, flexible aid for helping companies undertake the process of identifying and assessing risks, and applying controls and protocols that reflect their business model, customer preferences, risk profile, data usage practices, and legal obligations. This flexibility – and the intended variety of means by which it is adapted and used – is critical because the Framework must be inter-operable with a broad range of sectors, business models and risk profiles – as well as a wide variety of applicable legal obligations.

The Preliminary Draft shows promise as a tool to help enterprises organize, develop, and prioritize their practices, protocols, and measures for managing their privacy risks. It provides useful guidance and a common language and understanding that can assist organizations assess their internal systems and services for privacy risks, and aid in facilitating communication about privacy risk management issues and practices within an organization.

The comments offered below are aimed at ensuring that the Privacy Framework functions as an organizational blueprint that assists enterprises in connection with the *process* of managing the particular privacy risks most relevant to them. The Privacy Framework should be a process document for activity related to data risk management — it should not become synonymous with a "reasonable privacy program" or treated as a manual of substantive privacy protection measures and tools for companies to adopt. With these changes, the Privacy Framework could become as successful a tool for enterprises around the country as the Cybersecurity Framework.

NIST Should Clarify and Reinforce the Framework's Intended Function as a Voluntary, Risk Management Process Tool, Not a Substantive Compliance Manual. The Preliminary Draft states that the Framework is designed to be "agnostic to any particular technology, sector, law, or jurisdiction." While the Framework might help organizations comply with their privacy obligations — including both applicable laws and contractual and other requirements — that is not its purpose or function. Rather, the Framework should be designed to "assist an organization in its efforts to optimize beneficial uses of data and the development of innovative systems, products, and services while minimizing adverse consequences for individuals."[7]/

The Preliminary Draft includes language that helps reinforce this approach, but such language should be made more prominent. In particular, language contained in the Notes to Appendix A should be moved to the front of the document to help frame its scope and intent.

5/ *Id.*

6/ *Id.*

7/ *Id.* at 12.

For example, Note 1 states that:

> An organization may not need to achieve every outcome or activity reflected in the Core. It is expected that an organization will use Profiles to select and prioritize the Functions, Categories, and Subcategories that best meet its specific needs by considering its organizational or industry sector goals, legal/regulatory requirements and industry best practices, the organization's risk management priorities, and the privacy needs of individuals who are directly or indirectly served or affected by the organization's systems, products, or services. **The Subcategories should not be read as a checklist in isolation from their Categories, which often provide a risk-based modifier on Subcategory selection.**[8/]

Note 2 adds helpfully: "It is not obligatory to achieve an outcome in its entirety. An organization may use its Profiles to express partial achievement of an outcome, as not all aspects of an outcome may be relevant for the organization to manage privacy risk, or the organization may use a Target Profile to express an aspect of an outcome that it does not currently have the capability to achieve."[9/]

Taken together, these statements provide important context with respect to how the Privacy Framework should be used, as well as clarity – for enterprises using the Framework *and* external audiences, such as regulators and policymakers – regarding what the Framework is, and is not, designed to do. In particular these statements underscore that an organization should adapt the substance and elements of the Framework to its own internal organizational structure, business model, and risk profile. The Preliminary Draft appropriately recognizes that an organization's profile and risk tolerance may vary across different business units, and hence the Framework need not – and should not – be adapted in a monolithic fashion. In short, the Privacy Framework is to be adapted to an organization's privacy risk management objectives, and not vice-versa. The language from Appendix A highlighted above should be moved to the Executive Summary or Introduction of the Privacy Framework to reinforce these foundational concepts.

Further re-orientation of the Preliminary Draft along these lines also would allay the tension currently in the document between its stated purpose as a voluntary risk management tool and its susceptibility to being read, particularly with regard to some of the Subcategories, as a compliance checklist. For example:

- Subcategory ID.DE-P.5 envisions that "data processing ecosystem parties" would be "routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations."[10/] There are myriad ways of assessing service provider adherence to data management obligations and the regulatory connotation associated terms such as "audits" and "test results" is counter-

---

8/ *Id.* at 18 (emphasis in original).

9/ *Id.*

10/ *Id.,* Appendix A, Table 2, at 23. The references to "surveys" and "focus groups" in Sub-category CM.AW-P.2 in connection with obtaining feedback on data processing should likewise be deleted as potentially prescriptive. *See id.* at 26.

productive. In addition, the reference to "framework obligations" may inadvertently create confusion regarding the voluntariness of the Framework. The subcategory should be written along the following lines: "Data processing ecosystem parties are routinely assessed to confirm they are meeting their contractual or other applicable obligations."

- Subcategory CT.PO-P.4 directs companies to align information life cycles for managing data with system life cycles for managing systems, but such relatively sophisticated privacy by design processes, while appropriate in some circumstances, are not always technically feasible or consistent with product and system timetables and objectives.[11/]
- Subcategory CT.DM-P envisions that data elements will be accessible for alteration and deletion. While providing access/correction and deletion rights are part of some applicable privacy regimes, the and other language in the Preliminary Draft suggests that they should be part of any privacy program. Further, even privacy frameworks that contain such rights may limit the type of data to which they apply and provide for exceptions in certain circumstances. The guidance in the Framework should be less categorical with respect to these elements.
- Subcategory CM.AW-P.7 assumes that all data breaches require notifications, even though some applicable statutes and rules may not trigger notification absent a harm threshold, use of unencrypted data, or other exempt circumstances. [12/]

NIST Should Review and Modify Its Treatment of De-Identification in the Preliminary Draft. NCTA's comments highlighted the continuum of risks associated with different types of collection, use, and disclosure of consumer data, stressing in particular that information that cannot reasonably be linked to a specific individual carries a very different risk profile than information identifying a known individual. Accordingly, NCTA emphasized that the Privacy Framework should promote companies' use of de-identification as a risk management tool. The Preliminary Draft could do more to advance that objective.

First, there are passages in the Preliminary Draft that may unwittingly discourage companies from taking measures that reduce privacy risks. In Section 1.2.2, the Framework attempts to illustrate the relationship between privacy risk management and risk assessment with an example that posits a false trade-off between de-identifying data and satisfying consumer requests to access data:

> "For instance, if the organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or privacy-enhancing cryptographic techniques that hide data even from the organization. If the organization is also trying to enable individual control, the measures could conflict. For example, if an individual requests access to data, the organization may not be able to produce the data if the data has been distributed or encrypted in ways the organization cannot access. Privacy risk

---

[11/] *Id.* at 24.

[12/] *Id.* at 26.

> assessments can help an organization understand in a given context the values to protect, the methods to employ, and the way to balance implementation of different types of measures."[13/]

This passage implies a false equivalence between the reduction in privacy risks associated with de-identifying information and the potentially offsetting risk of reducing data accessibility – even though de-identification advances the *paramount objective* of reducing privacy risks to the consumer.

Second, the discussion of "disassociated processing" in Appendix A, Table 1 risks bleeding over into policy positions animating the larger privacy debate.[14/] For example, Subcategory, CT.DP-P3 directs users to process data in a manner that would "restrict the formulation of inferences about individuals' behavior or activities,"[15/] implicitly suggesting that formulating inferences is somehow a "problematic data action."[16/] However, any company that holds data could appropriately rely upon that data to make determinations about the interests or preferences of its customers in order to provide a more customized experience or service. Moreover, the subcategories addressing Disassociated Processing could more clearly call out the utility of business rules and technical measures that seek to minimize an organization's collective exposure to identifiable information while preserving beneficial uses of data.

Subcategory CT.DP-P.6 states that: "[d]ata processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives." This implicitly advances a policy position and is potentially too restrictive.[17/] The subcategory should be revised to state, "Data processing is reviewed to ensure it is related to the mission/business objectives of the system/product/service." The "relevant and necessary" language is unnecessarily restrictive.

Lastly, subcategory CT.DP-P.1 encourages the processing of data "in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography)." This formulation lacks a commonly employed "reasonable" qualifier – i.e., "reasonably" unobservable or unlinkable – that is critical to ensuring that the threshold for considering data to be de-identified is not excessive or impracticable. Further, the language of this subcategory suggests that NIST explicitly favors local processing over processing in the cloud or other more centralized locations. Depending on the context and use case, this may actually create more risk than it reduces.

13/ Preliminary Draft at 8.

14/ *Id.*, Appendix A, Table 2, at 25. Given the goal of creating a common language across widely diverse layers of an organization with varying levels of experience or engagement with privacy risk management, NIST should consider substituting more commonly used terms such as "de-identification" or "anonymization" for the term "Disassociated Processing."

15/ *Id.*

16/ *See id.*, Appendix B, at 30.

17/ *Id.*, Appendix A, Table 2, at 25.

NIST Should De-Emphasize the Framework Tiers and Eliminate References to Regulators. In connection with NIST's adoption and iteration of the Cybersecurity Framework, companies raised concerns about the Framework Implementation Tiers being used by regulators and other external audiences as short-hand proxies for gauging the efficacy of an organization's cybersecurity practices.[18/] In response, NIST modified its discussion of the tiers, making clear that they were intended more as an internal gauge of a company's progress than as a quantitative assessment of their cyber readiness.[19/]

In the context of privacy risk management, the concerns about misuse of the tier ranking scheme are even more acute. Unlike the context in which the Cybersecurity Framework was developed, the Privacy Framework will be used in a legal and regulatory environment that is the subject of intense focus, with international, U.S. state, and sector-specific laws, as well as FTC privacy enforcement actions already shaping companies' privacy practices, along with companies' own publicly available privacy policies, representing enforceable public commitments and overhanging their privacy risk management processes. Companies are striving both to be compliant and to manage privacy risks in a manner consonant with their business objectives, customer relationships, and legal obligations. Because companies are legally accountable for complying with applicable privacy laws and policies, NIST should take particular care to ensure the tier ranking scheme cannot be misapplied as a measure of the effectiveness of a company's privacy program or its compliance with any particular legal regime. However, some changes in the Preliminary Draft made from the Discussion Draft undermine that objective:

- On page 5, the denoted change in this sentence could be read to expand the external import of the Framework Implementation Tiers, rather than to confine it: "Implementation Tiers ('Tiers') provide context a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk."[20/] NIST should revert to the original formulation of this sentence in the Discussion Draft.
- A similar concern arises from the deletion of this sentence that was in the Discussion Draft: "Successful implementation of the Privacy Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination."[21/] A similar sentence was an important addition to the Cybersecurity Framework, and should also be included in the Privacy Framework.
- The underlined material below that was added to the Preliminary Draft on p. 11 could encourage regulators and other external audiences to view a company's Tier ranking as a proxy for the level of resources and depth and sophistication of its privacy risk management processes: "Progression to higher Tiers is appropriate when an

---

18/ *See, e.g., Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Draft 1), Comments of NCTA – The Internet and Cable Association, April 10, 2017, at 7-9.

19/ *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Draft 2), Comments of NCTA – The Internet and Cable Association, Jan. 19, 2018, at 2.

20/ Preliminary Draft at 5.

21/ *See NIST Privacy Framework: A Tool for Improving Enterprise Privacy Risk Management*, Discussion Draft at 10.

organization's processes or resources at its current Tier are insufficient to help it manage its privacy risks. An organization can use the Tiers to communicate with stakeholders whether it has sufficient resources and processes in place to achieve its Target Profile."[22/] That language is unnecessary and even potentially counterproductive and should be removed. At a minimum, NIST should change "communicate with stakeholders" to "communicate internally about".

The Preliminary Draft also states that the Privacy Framework "can drive better privacy engineering and help organizations protect individuals' privacy by . . . facilitating communication about privacy practices with customers, assessors, and regulators."[23/] NIST should be mindful of the risks of regulators (or courts) misapplying the subcategories in the "Privacy Framework Core" as requirements for, or evidence of, a legitimate or reasonable privacy program. References to regulators such as in the above quote are misaligned with the Framework's stated purpose as a voluntary, risk management *process* guide which should not function as the basis for dialogue with regulators.

NIST Should Separate "Use" of the Framework from Adoption of the Informative References. NIST should make clear that "use" of the Framework entails internalizing the process of risk management outlined in the main document and should not be equated with use of the controls and practices specified in the separate document containing the informative references. The informative references in the Privacy Framework draw almost entirely from NIST/NISTIR publications, leaning especially heavily on NIST 800-53, Security and Privacy Controls for Information Systems and Organizations. Many of these informative references, however, may have only limited application or relevance to the enterprise context, since they are geared toward government agencies that are not subject to Federal and State sector-based privacy laws. Accordingly, NIST should underscore the illustrative and supplemental nature of the informative references in order to reduce the risk of discouraging private company "use" of the otherwise helpful process blueprint in the Framework document itself.

NCTA appreciates NIST's continued thoughtfulness and diligence in connection with its work on the Privacy Framework. We look forward to continuing to collaborate with NIST on refining and improving this important resource for managing privacy risks.

Sincerely,

/s/ Rick Chessen

Rick Chessen

Loretta Polk

October 24, 2019

22/ Preliminary Draft at 11.

23/ Preliminary Draft at 3.