From: Rachel Nemeth <RNemeth@cta.tech>
Sent: Thursday, October 24, 2019 4:15 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Mike Bergman <MBergman@cta.tech>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Good afternoon,

Please see attached for comments from CTA.

Thank you,

Rachel

Rachel Sanford Nemeth

Director, Regulatory Affairs

Consumer Technology Association, producer of CES®

d: 703-907-7631

m: 703-283-1663

CTA.tech | CES.tech

Before the
Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899

In the Matter of	)
	)
NIST Privacy Framework:	)
A Tool for Improving Privacy	)
Through Enterprise	)
Risk Management	)

Comments of the
Consumer Technology Association

I. Introduction

The Consumer Technology Association (CTA)[1] appreciates the opportunity to provide these comments on the preliminary draft of the National Institute of Standards & Technology's (NIST's) "*Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management"* (Privacy Framework or Draft Privacy Framework). CTA supports the role NIST has played as a convener of private and public organizations to address cybersecurity challenges, and believes NIST can play a similar role for privacy concerns. CTA respectfully submits these comments for NIST's consideration in response to its request for public comment on the Draft Privacy Framework.

CTA is providing the feedback below to help facilitate a successful rollout of the finalized Privacy Framework. To that end, CTA believes that the Privacy Framework can more explicitly state what it should, and should not be, used for. CTA recommends that additional clarifying language regarding its proper uses be included throughout the document itself,

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES® – the largest, most influential tech event on the planet.

including in the Executive Summary, so that NIST's intentions are clear – both to stakeholders that have participated in the process, but also to those that review the Privacy Framework for the first time after its completion. As NIST has stated, the Privacy Framework is not a checklist. As such, it should not to be relied upon by regulators or courts to determine whether an organization took the proper steps to protect an individual's privacy.

II. CTA Supports NIST's Role as a Convener for Privacy

As we have previously stated in prior comments in other proceedings, CTA is supportive of the role NIST plays as a convener of the public and private sectors. Public-private partnerships and flexible, non-prescriptive standards have been a critical component of the government's response to cybersecurity challenges. We believe a similar approach can be of value in the privacy space as well.

CTA produces CES®, which serves as the global stage for innovation; it has been a proving ground for innovators and breakthrough technologies for more than 50 years. Each year, CES showcases the dynamic nature of technology and the consumer benefits that are possible when companies innovate freely. And in recent years, CES has demonstrated the proliferation of smart, connected devices available today. The ongoing advances in emerging data-driven technologies, including artificial intelligence, are sure to continue to make their mark at CES and beyond.

Though CTA is the principal trade association representing the interests of the consumer technology industry, CTA also has a long history as a technical standards body going back to the 1920s. Our Technology and Standards program is accredited by ANSI, the American National Standards Institute, and includes more than 70 committees and over 1000 participants. CTA and many of our individual members are actively working with NIST, other government agencies, and

with other sectors of the industry, to develop forward-looking solutions to privacy, security, and other emerging technological challenges.

During recent testimony in a hearing on "Strengthening the Cybersecurity of the Internet of Things" before the Senate Committee on Commerce, Science, and Transportation, CTA commended the productive role NIST has played in convening cybersecurity activities among different ecosystem stakeholders.[2] We advocated for the Committee to continue supporting NIST's efforts.

CTA believes NIST can continue to play a similar, productive role in assisting the federal government with developing an approach to privacy that protects innovation while also protecting consumers.

III. The Privacy Framework Could Be Useful to Facilitate Communication, Especially within an Organization, but Potential for Misuse Remains

CTA agrees that the NIST Privacy Framework could be helpful for encouraging "cross-organization collaboration." As the document states, "The Core enables a dialogue – from the executive level to the implementation/operations level—about important privacy protection activities and desired outcomes." CTA agrees with and supports this premise. The Draft Privacy Framework could be a useful tool to facilitate communication regarding privacy risk across an organization.

CTA does not believe, however, that the document should necessarily be used to facilitate "communication about privacy practices with…regulators" in the same manner. CTA recommends that NIST provide additional detail and specifity on the type of communication the Draft Privacy Framework is intended to facilitate between organizations and regulators. The

[2] Subcommittee on Security for the U.S. Senate Committee on Commerce, Science, and Transportation, *"Strengthening the Cybersecurity of the Internet of Things,"* (Apr. 30, 2019).

Framework is, intentionally, much broader than what is required under privacy laws. For instance, it is intended to address both public and private sector privacy considerations – which vary – as well as considerations that go far beyond requirements enshrined in privacy laws. Proper use of the NIST Privacy Framework was designed to help organizations consider a collection of possible outcomes, rather than apply it as checklist of actions to perform for regulators.

The Subcategories in the "Privacy Framework Core" are very specific. Such specificity can be of use for an organization's internal deliberations and communications over privacy. However, as outlined below, CTA recommends that NIST take additional steps to ensure such specificity is not misinterpreted by regulators as something akin to regulatory requirements for appropriate privacy practices. Additionally, while the "Implementation Tiers" are supposed to "help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile," these tools should not be misused by regulators to determine whether an organization has adopted appropriate privacy practices.

Given that NIST has stated the Draft Privacy Framework should be used to facilitate communication with regulators, it should more explicitly state what that communication would, and would not, entail. Certainly organizations should feel free to share documentation regarding their implementation of the Privacy Framework with a regulator to demonstrate that they have established a thoughtful, risk-based privacy program; regulators, however, should not look to the Privacy Framework and its delineated Categories and Subcategories to suggest an organization has fallen short of regulatory expectations. Given that NIST does not view the Privacy Framework as a "checklist," CTA recommends that NIST explain in further detail what kinds of communications it can facilitate between organizations and regulators.

IV. The Privacy Framework Should More Explicitly State Its Intended Uses

a. CTA Believes NIST Should Include Additional Language Regarding the Intended Use of the Privacy Framework Core

CTA appreciates that NIST has responded to feedback about the need to include language regarding the purpose of the Privacy Framework. CTA also appreciates comments made by NIST officials about the intended use of the Privacy Framework, including that it should not be understood by regulators, legislators, and others as a minimum baseline of privacy requirements and expectations. CTA believes NIST has been clear in its intentions throughout the process, during workshops and roundtables. However, CTA encourages NIST to provide further specificity in the document itself regarding the Privacy Framework's intended uses. CTA believes it is critical that a regulator, legislator, or policymaker who reviews the NIST Privacy Framework for the first time following its completion has the same understanding of its intended purposes.

Understandably, NIST's goal is that organizations voluntarily adopt the Privacy Framework. To maximize the likelihood of adoption, CTA is recommending that additional language and protections be put in place to ensure organizations implementing the Framework can be confident that their actions, either adopting or choosing not to adopt various aspects, will not be misinterpreted by third-parties.[3]

While Section 3.0 (How to Use the Privacy Framework) notes, "The variety of ways in which the Privacy Framework can be used by organizations should discourage the notion of

[3] In this regard, implementing the Privacy Framework creates some concerns and challenges that are distinct from the Cybersecurity Framework. Under current law and regulator expectations, cybersecurity inherently is a risk management process – no regulator expects perfect cybersecurity, and instead regulators understand that cybersecurity is a dynamic process that requires prioritization in the allocation of resources. Privacy, by contrast, is subject to several existing laws and frameworks, as well as an active and evolving policy debate about what privacy rights and protections should be afforded to consumers. To date, privacy has not been considered primarily a risk management exercise and some stakeholders seek to achieve "perfect" privacy, at least as they consider it.

'compliance with the Privacy Framework' as a uniform or externally referenceable concept," CTA believes it would beneficial for the Framework to be even more explicit about its purpose. Specifically, CTA recommends that NIST further clarify the notion that "compliance with the Privacy Framework" is not an "externally referenceable concept," as it may not be a uniformly understood notion. Instead, CTA recommends additional specificity on what constitutes an "externally referenceable concept," and clarity that NIST does not believe the Framework should be used to make enforcement and liability determinations related to an organization's privacy practices. NIST should also consider expounding upon this notion by stating that entities, like courts and regulators, should not be using the Privacy Framework as a "referenceable concept."

Additionally, CTA appreciates that on page 18 in Appendix A, NIST states that "The Subcategories should not be read as a checklist in isolation from their Categories…." CTA recommends that this notion be stated explicitly at the beginning of the document, in the Executive Summary, as well as further explained in Appendix A. The notion that the Subcategories should not be read as a checklist could be highlighted explicitly at the beginning of the document to underscore the threshold significance of this concept.[4] CTA believes that NIST also should include something akin to a "Note to Regulators" at the outset, which states explicitly and expounds on the following:

> The NIST Privacy Framework's Framework Core should not be used as a checklist by third-parties to determine whether an organization has adopted appropriate privacy practices. Rather, it is meant as a guide for organizations evaluating their own risks related to privacy practices.

[4] Concerns that regulators may inappropriately look to the Privacy Framework, if implemented by an organization, for deficiencies in privacy practices, poses a real risk to companies adopting and implementing the Framework.

b. The Implementation Tiers Could Be Misused by Regulators and Courts as Currently Drafted

Under its current formulation, organizations could be taking on legal risk by adopting the "Implementation Tier" system. An organization that creates documentation which self-identifies as "Tier 1" or "Tier 2" could be opening themselves up to scrutiny by a regulator or a court reviewing the organization's privacy practices. Specifically, a regulator or a plaintiff could claim that an organization that self-identifies in these tiers has acknowledged its deficiencies in privacy protections for consumers. As a result, NIST should explicitly state that the "Implementation Tier" system does not equate with deficiencies in privacy practices and therefore should not be the basis for liability for any regulatory or legal regime. NIST also should explicitly state that a "Tier 1" rating has nothing to do with an organization's compliance with privacy laws, and therefore does not mean, nor should serve as a basis for an argument that, the organization is violating any law or regulation related to privacy regime.

The Privacy Framework's current discussion of progression to higher tiers also creates some risks for organizations that choose to adopt the Framework. Specifically, Section 2.3 Implementation Tiers (page 11) states that "Progression to higher Tiers is appropriate when an organization's processes or resources at its current Tier are insufficient to help it manage its privacy risks." We respectfully request revising this statement as follows: "Progression to higher Tiers is appropriate when an organization's processes or resources at its current Tier ***may be*** insufficient to help it manage its privacy risks."

V. NIST Should Clarify or Delete Language that Could be Misinterpreted and/or Misused

In addition to making the changes described above, NIST can reduce barriers to private sector organizations adopting and implementing the Privacy Framework by scrubbing the

document for any and all language that, taken out of context, could be used contrary to NIST's intent. Importantly, given the ongoing, high-profile, domestic and international discussions about the privacy protections individuals should have, as well as the impact that such protections have on marketplaces, innovation, and new technologies, there is currently potential for such unintended uses.[5]

CTA recommends changes to the following subcategories in the Privacy Framework Core:

i. ***ID.IM-P3***

As part of the "Inventory and Mapping" Category of the "Identify-P" function, the Framework refers to "individuals" as customers and "employees or prospective employees." Given that organizations may need to treat information about employees and consumers/customers in different manners – and further, that employees and consumers/customers may be subject to very different legal regimes – it is confusing to treat them as interchangeable within the Framework.

ii. ***ID.RA-P2***

This Subcategory states that, "Data analytic inputs and outputs are identified and evaluated for bias." We believe this Subcategory should either be deleted or additional specificity should be included. "Bias" is a broad term and should be further defined, as it could be entirely appropriate for an organization to categorize certain data analytic outputs.

[5] It is critical that both those that have participated in the process to develop the Framework (and have familiarity with the Cybersecurity Framework) and those who are viewing it for the first time have the same understanding of how it should and should not be used.

iii. ***"Disassociated Processing (CT.DP-P)"***

Through its six subcategories, this category appears to advocate policy positions related to the larger privacy and artificial intelligence debates, rather than processes for organizations to consider to mitigate organizational risk related to privacy risk. For example, one subcategory (CT.DP-P3) is "Data are processed to restrict the formulation of inferences about individuals' behavior or activities." The inclusion of that subcategory suggests that formulating inferences is somehow inherently a "problematic privacy practice." And yet, any company that holds data could appropriately rely upon data to determine, for example, if a customer is interested in receiving information about a sale or a new product – a longtime, expected, and accepted practice in the private sector. Additionally, CT.DP-P6 states, "Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives." "Relevant and necessary…to meet mission/business objectives" could be interpreted as too restrictive and, again, suggests a position on policy. The subcategory should be reworked 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 needlessly restrictive, particularly for private sector organizations.

iv. ***CM.AW-P8***

This Subcategory states that, "Impacted individuals and organizations are notified about a privacy breach or event." Breach notification is regulated on a state-by-state basis and state legislatures have taken time to consider what data necessitates a notification to a consumer and what data does not. This subcategory assumes that any privacy breach would lead to notification. To resolve this confusion, we suggest editing the subcategory to state, "The

organization considers whether impacted individuals and organizations are notified about a privacy breach or event."

Additionally, under state law, notification can be achieved via various methods, including by publishing the notification in media outlets and the organization's website. Even state law recognizes that individual notification is not always the best approach for an organization suffering a breach of data covered by a notification statute. While we acknowledge that an organization should consider whether to notify individuals any time a breach occurs, we do not believe every breach or event would necessitate notification to individuals – and in fact, can lead to notification fatigue.

VI. Conclusion

CTA supports the role NIST has played as a convener of private and public organizations to address cybersecurity challenges, and believes NIST can play a similar role for privacy concerns. CTA is providing this feedback to help facilitate a successful rollout of the finalized Privacy Framework. CTA will continue to coordinate with NIST as it develops a risk-based approach to privacy.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/ Rachel Nemeth*

Rachel Nemeth
Director, Regulatory Affairs

Mike Bergman
VP, Technology & Standards

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