From: Scott, Kathleen <KScott@wileyrein.com>
Sent: Thursday, October 24, 2019 3:12 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Brown, Megan <MBrown@wileyrein.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments; Comments of CTIA

To Whom It May Concern,

Please find attached the comments of CTIA in response to the NIST Privacy Framework: Preliminary Draft. If you have any questions, please feel free to contact me.

Thank you,

Kat Scott

Kathleen E. Scott | Attorney at Law
Wiley Rein LLP
1776 K Street NW | Washington, DC 20006
T: 202.719.7577 | kscott@wileyrein.com
wileyrein.com | Bio | LinkedIn| Twitter | WileyonMedia Blog

Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

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

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

October 24, 2019

Table of Contents

I. INTRODUCTION AND SUMMARY.

CTIA[1] appreciates the opportunity to work with NIST on the Privacy Framework. As privacy policy is debated across the country and around the world, the United States needs a practical tool that can help establish a common language and identify resources for privacy risk management. The Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management ("Draft Privacy Framework" or "Draft") does just that.[2]

Protecting consumer privacy is a top priority for the wireless industry. Good privacy practices are good business. Strong majorities of consumers say that it is either "important" or "extremely important" for businesses to maintain the privacy of data about them.[3] As NIST explains, good privacy practices help "avoid[] losses of trust that damage organizations' reputations, slow adoption, or cause abandonment of products and services."[4] CTIA's members take privacy seriously and engage in privacy risk management. For example, the carrier signatories to CTIA's *Consumer Code for Wireless Service* have committed to abide by policies that protect consumer privacy.[5] Companies across the wireless ecosystem promote privacy and

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NIST, Preliminary Draft, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Sept. 6, 2019), https://www.nist.gov/sites/default/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf ("Draft Privacy Framework").

[3] IBM, Consumer Attitudes Towards Data Privacy, IBM-Harris Poll Survey 2019: US Data at 6 (2019), https://newsroom.ibm.com/download/IBM+Data+Privacy.pdf.

[4] Draft Privacy Framework at 8.

[5] *See Consumer Code for Wireless Service*, CTIA (last accessed Oct. 14, 2019), https://www.ctia.org/the-wireless-industry/industry-commitments/consumer-code-for-wireless-service ("Each wireless carrier will abide by a policy regarding the privacy of customer information in accordance with applicable federal and state laws, and will make available to the public its privacy policy concerning information collected online. Each wireless carrier will abide by the CTIA Best Practices and Guidelines for Location-Based Services.").

customer choice, in varied ways. For example, AT&T bases its global privacy program on four principles: transparency, security, choice and control, and integrity.[6] Among other things, AT&T "limit[s] access to customer information within the company to those who have a business need"[7] and provides privacy and security training throughout the year for employees.[8]

The wireless industry is engaged with public sector partners on privacy. CTIA fully supports federal, comprehensive, technology-neutral privacy legislation enforced by the Federal Trade Commission ("FTC").[9] CTIA has collaborated with actors across the federal government on this issue, for example, in response to the National Telecommunications and Information Administration's ("NTIA") Request for Comments on Developing the Administration's Approach to Consumer Privacy;[10] NIST's Request for Information ("RFI") about the Privacy Framework;[11] and the FTC's hearings on Competition and Consumer Protection in the 21st Century that focused on privacy and data security.[12] CTIA recently joined a broad coalition calling on Congress to pass a comprehensive federal privacy law.[13]

CTIA suggests only a few targeted edits to the Draft Privacy Framework. *First*, NIST should clarify how to incorporate the Cybersecurity Framework into an organization's privacy risk management approach. This will make the Privacy Framework easier to use. *Second*, the

[6] *Customer Privacy*, AT&T (last accessed Sept. 23, 2019), https://about.att.com/csr/home/reporting/issue-brief/customer-privacy.html.
[7] *Id.* at *Championing Privacy Within Our Business.*
[8] *Id.*
[9] *See Privacy Position*, CTIA (last accessed Sept. 22, 2019), https://www.ctia.org/positions/privacy; *see also* Kelly Cole & Tom Power, *Protecting Consumers with Federal Privacy Legislation*, CTIA (Nov. 9, 2018), https://www.ctia.org/news/protecting-consumers-with-federal-privacy-legislation.
[10] *See* Comments of CTIA, *Developing the Administration's Approach to Consumer Privacy*, NTIA, Request for Comments, Docket No. 180821780-8780-01 (Sept. 25, 2018).
[11] *See* Comments of CTIA, *Developing a Privacy Framework*, NIST, Request for Information, Docket No. 181101997-8997-01, 83 Fed. Reg. 56824 (Nov. 14, 2018) ("CTIA RFI Comments").
[12] *See* Comments of CTIA, *Competition and Consumer Protection in the 21st Century Hearings*, FTC, Docket Nos. FTC-2018-0098, FTC2018-0099 (May 31, 2019), https://www.regulations.gov/document?D=FTC-2018-0098-0078 ("CTIA FTC Comments").
[13] Letter from CTIA et al., to The Honorable Roger Wicker, United States Senate, et al. (July 11, 2019), https://api.ctia.org/wp-content/uploads/2019/07/Privacy-Trade-Coalition-Letter.pdf.

Draft should include a discussion on de-identification, aggregation, and pseudonymization to highlight and promote tools that facilitate beneficial uses of data and provide insights for organizations that choose to use the Privacy Framework. *Third*, NIST should emphasize the voluntary and flexible nature of the Privacy Framework more consistently. *Fourth*, to further the goal of policy neutrality, CTIA urges NIST to avoid wading into policy debates.

II. NIST'S DRAFT PRIVACY FRAMEWORK WILL ENCOURAGE INNOVATIVE AND BENEFICIAL USES OF DATA.

NIST is approaching privacy in much the same way it built the Cybersecurity Framework five years ago, by building consensus around a voluntary, flexible, broadly applicable tool in an area where guidance is needed. The Cybersecurity Framework has been downloaded more than half a million times and deployed "across all sectors of the economy."[14] NIST Director Walter Copan attributes the Cybersecurity Framework's resoundingly successful results to a few key characteristics: "It is voluntary."[15] "It's created collaboratively with expert input from across private and public sectors."[16] "It can be used by any size or any type of organization [to] help manage cybersecurity risks."[17] "It's a guide and not a one-size-fits-all prescription."[18] "It focuses on desired outcomes."[19]

NIST has rightly taken a nearly identical tack here. The Draft Privacy Framework is flexible, outcome-oriented, and voluntary, and will be the result of a highly collaborative

[14] *NIST Marks Fifth Anniversary of Popular Cybersecurity Framework*, NIST (Feb. 12, 2019), https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework (explaining that the Cybersecurity Framework has been downloaded "more than half a million times since its initial publication in 2014" and deployed "across all sectors of the economy").

[15] Transcript of Walter Copan, *Developing the NIST Privacy Framework: How Can a Collaborative Process Help Manage Privacy Risks?* The Brookings Institution (Sept. 24, 2018), https://www.brookings.edu/wp-content/uploads/2018/09/gs_20180924_nist_privacy_transcript.pdf at 10.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

process.[20] CTIA supports these key features.

A. NIST's Draft Balances Beneficial Uses of Data and Risks to Privacy.

The Draft strikes a good balance of discussing both the utility and risks of data processing. CTIA has previously emphasized the importance of recognizing the innovative and beneficial uses of data, while at the same time tackling privacy risks.[21] The Draft Privacy Framework does this. NIST rightly explains that "the Internet and associated information technologies have driven unprecedented innovation, economic value, and improvement in social services."[22] NIST recognizes that the role of privacy risk assessment is "to weigh the benefits of . . . data processing against the risks and to determine the appropriate response . . . ."[23] In describing how to use the Privacy Framework, NIST notes that it "can 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."[24]

B. The Privacy Framework Is Flexible and Risk-and Outcome-Based.

The Privacy Framework is flexible. It correctly notes that "[d]eriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one-size-fits-all solutions."[25] One of its explicit goals is to be "flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current with technology trends, including artificial intelligence and the Internet of Things."[26]

[20] *See, e.g.*, *Past Events (Privacy Framework)*, NIST (Sept. 19, 2019), https://www.nist.gov/privacy-framework/past-events.
[21] CTIA RFI Comments at 3–4.
[22] Draft Privacy Framework at 3–4.
[23] *Id.* at 7.
[24] *Id.* at 12.
[25] *Id.* at 3.
[26] *Id.*

The Draft achieves its goal of flexibility in several ways. It explains that "organizations may not need to achieve every outcome or activity reflected in the Core."[27] Rather, "an organization may select or tailor the Privacy Framework's Functions, Categories, and Subcategories to its specific needs" or "develop its own additional Functions, Categories, and Subcategories to account for unique organizational risks."[28] In explaining the Draft's tier system, NIST notes that "[t]iers do not represent maturity levels," and "[s]ome organizations may never need to achieve Tier 3 or 4 or may only focus on certain areas of these tiers."[29] Indeed, "[p]rogression 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."[30] Ultimately, "there are a wide variety of ways to use the Privacy Framework," and "[t]he decision about how to apply it is left to the implementing organization."[31]

The Draft Privacy Framework is risk- and outcome-based. NIST explains that implementation of the Privacy Framework will depend on organizational risk factors: "Effective privacy risk management requires an organization to understand its business or mission environment; its legal environment; its enterprise risk tolerance; the privacy risks engendered by its systems, products, or services; and its role or relationship to other organizations in the ecosystem."[32] Additionally, the Core Functions rightly are flexible and risk-based, rather than prescriptive. Take "Control-P" for example. The "Control-P" Function counsels that organizations "[d]evelop and implement *appropriate activities* to enable organizations or individuals to manage data with sufficient granularity to *manage privacy risks*."[33] The

[27] *Id.* at 10.
[28] *Id.* at 10–11.
[29] *Id.* at 11.
[30] *Id.*
[31] *Id.* at 12.
[32] *Id.* at 14.
[33] *Id.* at 24 (emphases added).

actionable principles in "Control-P"—*e.g.,* "implement appropriate activities"—are high level and avoid carving prescriptive controls in stone. In turn, organizations are given room to maneuver and develop the protocols that will be best for their particular organization. And as "Categories" and "Sub-Categories" of "Control-P" get more granular—*e.g.,* "Data are transmitted using standardized formats"—NIST has generally stuck to "discrete outcomes"[34] and made clear that "[w]hen developing a Profile, an organization may select or tailor the Privacy Framework's Functions, Categories, and Subcategories to its specific needs."[35]

C. The Privacy Framework Appears Useful Across a Variety of Privacy Regimes and Regulatory Approaches.

NIST has made clear that policy-neutrality is key. This is particularly important as regulatory and legal regimes are varied and in flux. NIST should continue to prioritize regulatory compatibility and interoperability with global standards.[36]

Stakeholders want a Privacy Framework that is policy neutral and applicable across an array of regulatory regimes: "respondents expressed that the Framework should support organizations' ability to comply with a range of legal responsibilities, including U.S. state and federal sector-specific laws and regulations and international regimes such as the APEC Cross-Border Privacy Rules, the European Union's General Data Protection Regulation, and Brazil's General Data Protection Law."[37] This feedback came from diverse stakeholders across industries, including information technology, healthcare, and telecommunications,[38] whose practices are generally governed by different legal regimes. NIST rightly explains that "[t]he

[34] *Id.* at 5.
[35] *Id.* at 10.
[36] *See Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* , NIST (Feb. 27, 2019), https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf at 2.
[37] *Id.* at 4.
[38] *See generally id.*

Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction."[39]

III. NIST SHOULD CONSIDER TARGETED EDITS TO DEVELOP A FLEXIBLE AND POLICY-NEUTRAL TOOL THAT CAN BE WIDELY ADOPTED.

NIST can build on the Draft Privacy Framework to maximize its utility in helping organizations manage privacy risks and facilitate beneficial uses of data.

A. NIST Should Clarify How the Cybersecurity Framework Can Be Used with the Privacy Framework.

NIST illustrates the relationship between cybersecurity and privacy, which are interrelated, but have several critical differences. For example, many cybersecurity standards are mature and well-developed, whereas some privacy practices are nascent and debated. CTIA has long urged NIST to avoid conflating the two[40] and NIST rightly treats them distinctly.

NIST can improve its guidance about how the Cybersecurity Framework can be used with the Privacy Framework to manage privacy breach risks. CTIA fully supports NIST's intent that the Cybersecurity Framework can be flexibly integrated into the Privacy Framework. However, CTIA suggests that NIST clarify this point in order to make the document more usable for organizations. NIST could introduce the diagram (Figure 8) showing how the two frameworks overlap in Section 2 of the body of the document, as opposed to introducing it in Appendix A. Additionally, NIST should add a discussion in Section 2 that exclusively discusses how the two frameworks can be used separately or in conjunction with each other, as opposed to making a brief reference to it in the discussion of Functions more generally. CTIA welcomes the flexibility that NIST has built into the Privacy Framework with respect to Cybersecurity Framework integration, but further clarity on this integration would be useful.

[39] Draft Privacy Framework at 4.

[40] *See, e.g.,* CTIA RFI Comments at 8–9.

B. NIST Should Provide More Examples of Beneficial Uses of Data and Practices That Promote Innovation and Protect Privacy—Such as De-identification, Aggregation, and Pseudonymization.

NIST should emphasize privacy-enhancing practices that industry uses and that can further develop. For example, NIST should specifically discuss de-identification, aggregation, and pseudonymization in CT.DP-P2 (Control-P, Disassociated Processing). These practices have privacy and security benefits, including facilitating information sharing and turning useful data into a less attractive target to bad actors. By enabling the processing of data, these practices and tools yield larger societal benefits, including improving research. NIST already cites to its work on de-identification—NISTIR 8053—in its companion Informative References.[41] Explicitly identifying such privacy-enhancing practices in the Privacy Framework itself would encourage their adoption and promote beneficial uses of data, as well as give organizations that implement the Privacy Framework even more tools to help manage privacy risks while innovating.

C. NIST Should Emphasize the Privacy Framework's Flexible and Non-Prescriptive Approach.

NIST rightly emphasizes that the Draft Privacy Framework is voluntary and flexible, not a set of "one-size-fits-all solutions."[42] NIST should make these points clearly in every facet of the document to preempt any confusion. CTIA suggests three targeted edits.

First, NIST should bolster language about the flexible, voluntary nature of the Privacy Framework in the body of the document. Some of NIST's strongest language on the flexible and voluntary nature is in Appendix A under the Note to Users. In particular, this section says:

An organization may not need to achieve every outcome or activity reflected in the Core.

[41] NIST, NIST Informative References for the Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management Preliminary Draft (Sept. 6, 2019), https://www.nist.gov/sites/default/files/documents/2019/09/06/nist-informative-references-privacy-framework-preliminary-draft.pdf at 9.
[42] *Id.* at 3.

> 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.[43]

NIST should include similar language in the body of the document to provide clarity sooner.

Second, NIST should clarify or replace the term "privacy requirements," which appears throughout the document.[44] NIST should make clear at the outset that "privacy requirements" do not refer to government-imposed requirements or requirements imposed by the Privacy Framework, but rather are "a means of expressing the legal obligations, privacy values, and policies to which the organization intends to adhere."[45] Alternatively, NIST could simply use a different term, such as "privacy targets." Clarifying that any "requirements" are often self-imposed would reduce any potential ambiguity about the voluntary nature of the Draft.

Third, NIST should ensure that in describing Functions, Categories, and Subcategories NIST's language cannot be misconstrued as being prescriptive. NIST should add clarifying language to make clear that its descriptions are not misconstrued as requirements. For example, NIST could edit CT.PO-P4 as follows: "Policies, processes, and procedures for enabling individuals' data processing preferences and requests, where applicable, are established and in place." As another example, NIST could amend CM.AW-P7 to read: "Impacted individuals and organizations are notified, where appropriate, about a privacy breach or event."

D. A Few Edits Will Ensure that the Privacy Framework's Guiding Principle of Policy-Neutrality Is Consistently Achieved.

[43] Draft Privacy Framework at 18.

[44] *See id.* at 12, 13, 15, 17, 30, 33, 34, 35, 37.

[45] *Id.* at 34.

To achieve wide applicability, the Privacy Framework should not promote any policy approach and should remain neutral and value-agnostic. NIST generally follows this approach,[46] but three edits will preserve this approach across the entirety of the Draft.

First, NIST should refrain from defining privacy harms broadly. The Draft says that "problems" that may arise from data processing "rang[e] from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm."[47] CTIA understands that NIST is trying to illustrate a wide range of risks, including problems beyond legally cognizable harms. But NIST should avoid grouping "dignity-type effects" with tangible economic or physical harms. There is significant debate over whether the former should be included in legislative or regulatory definitions of "harm." Indeed, CTIA has urged the FTC to focus on actual, concrete injuries.[48] The question of privacy harm should be addressed by policymakers, so NIST should ensure that its discussion of privacy "problems" does not inadvertently address contested issues.

Second, NIST should reconsider its definition of "privacy breach"[49] to ensure that NIST is not favoring one legal regime. One important issue in breach notification legal and regulatory approaches is how to define "breach,"[50] with a key element being a reasonable expectation of harm; however, NIST's definition does not incorporate this element.[51] Unauthorized access—standing alone and without a reasonable expectation that such action will lead to harm—is not

[46] *Id.* at 4 ("The Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction.").
[47] *Id.* at 6.
[48] CTIA FTC Comments at 9-10.
[49] Draft Privacy Framework at 30 (defining the term as "[t]he loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other than authorized purpose.").
[50] *See Security Breach Notification Laws*, National Conference of State Legislatures (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[51] *See* Draft Privacy Framework at 30.

necessarily a problem. For example, unauthorized access to data by a customer service agent who accidentally and with no ill-intent accesses the wrong information about a customer should not be swept into the definition of "breach." At the very least, NIST should make clear that the reasonable expectation of harm is an important part of what constitutes a "breach" under any given legal regime, and that NIST's use of the term "breach" is distinct from the legal term—which triggers often onerous obligations for companies who have suffered a breach.

Third, NIST should refrain from taking a position on the political question of when notice is required and what constitutes adequate notice. In describing the Communicate-P Function, NIST states that "individuals *need* to know how data are processed in order to manage privacy risk effectively."[52] Whether, when, and how to address notice to consumers is a policy judgment. It might be better to use language from elsewhere in the draft: that an organization "*[d]evelop and implement appropriate*"[53] mechanisms to communicate to individuals how data are processed to manage privacy risk effectively.

IV. CONCLUSION.

CTIA supports the Privacy Framework. It will be a valuable tool for industry moving forward and—like the Cybersecurity Framework—the Draft bears all the hallmarks of a highly effective NIST publication. CTIA encourages NIST to adopt targeted edits to further its goals.

[52] *Id.* at 10 (emphasis added).

[53] *Id.* at 25-26 (Control-P, Communicate-P, and Protect-P) (emphasis added).

Respectfully submitted,

/s/ Melanie Tiano

Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas C. Power
Senior Vice President and General Counsel

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

Comments of CTIA

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	CTIA appreciates the opportunity to work with NIST on the Privacy Framework. As privacy policy is debated across the country and around the world, the United States needs a practical tool that can help establish a common language and identify resources for privacy risk management. The Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management ("Draft Privacy Framework" or "Draft") does just that. CTIA suggests only a few targeted edits to the Draft Privacy Framework.	N/A	General
2	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	NIST has rightly taken a nearly identical tack on the Privacy Framework as it did for the Cybersecurity Framework. The Draft Privacy Framework is flexible, outcome-oriented, and voluntary, and will be the result of a highly collaborative process. CTIA supports these key features.	N/A	General
3	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	The Draft strikes a good balance of discussing both the utility and risks of data processing.	N/A	General
4	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	The Privacy Framework is flexible and risk- and outcome-based.	N/A	General
5	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	NIST has made clear that policy-neutrality is key. This is particularly important as regulatory and legal regimes are varied and in flux. NIST should continue to prioritize regulatory compatibility and interoperability with global standards.	N/A	General
6	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	NIST illustrates the relationship between cybersecurity and privacy, which are interrelated, but have several critical differences. CTIA has long urged NIST to avoid conflating the two and NIST rightly treats them distinctly.	N/A	General
7	CTIA	Melanie Tiano / MTiano@ctia.org	3; 5; 9; 19	104-05; 176-80; 321-25; 660-73	Exec. Summ.; 1.1; 2.1; App. A	NIST can improve its guidance about how the Cybersecurity Framework can be used with the Privacy Framework to manage privacy breach risks. CTIA fully supports NIST's intent that the Cybersecurity Framework can be flexibly integrated into the Privacy Framework. However, CTIA suggests that NIST clarify this point in order to make the document more usable for organizations.	NIST could introduce the diagram (Figure 8) showing how the two frameworks overlap in Section 2 of the body of the document, as opposed to introducing it in Appendix A. Additionally, NIST should add a discussion in Section 2 that exclusively discusses how the two frameworks can be used separately or in conjunction with each other, as opposed to making a brief reference to it in the discussion of Functions more generally. CTIA welcomes the flexibility that NIST has built into the Privacy Framework with respect to Cybersecurity Framework integration, but further clarity on this integration would be useful.	Technical

8	CTIA	Melanie Tiano / MTiano@ctia.org	25	684	App. A	NIST should emphasize privacy-enhancing practices that industry uses and that can further develop. For example, NIST should specifically discuss de-identification, aggregation, and pseudonymization in CT.DP-P2 (Control-P, Disassociated Processing). These practices have privacy and security benefits, including facilitating information sharing and turning useful data into a less attractive target to bad actors. By enabling the processing of data, these practices and tools yield larger societal benefits, including improving research. NIST already cites to its work on de-identification—NISTIR 8053—in its companion Informative References. Explicitly identifying such privacy-enhancing practices in the Privacy Framework itself would encourage their adoption and promote beneficial uses of data, as well as give organizations that implement the Privacy Framework even more tools to help manage privacy risks while innovating.	For example, NIST should specifically discuss de-identification, aggregation, and pseudonymization in CT.DP-P2 (Control-P, Disassociated Processing).	Technical
9	CTIA	Melanie Tiano / MTiano@ctia.org	18	617-24	App. A	NIST rightly emphasizes that the Draft Privacy Framework is voluntary and flexible, not a set of "one-size-fits-all solutions." NIST should make these points clearly in every facet of the document to preempt any confusion. CTIA suggests three targeted edits.	First, NIST should bolster language about the flexible, voluntary nature of the Privacy Framework in the body of the document. Some of NIST's strongest language on the flexible and voluntary nature is in Appendix A under the Note to Users. NIST should include similar language in the body of the document to provide clarity sooner.	Technical
10	CTIA	Melanie Tiano / MTiano@ctia.org	12, 13, 15, 17, 30, 33-35, 37	422; 458; 464; 531; 538; 589-91; 593; 605; 607; 687; 709; 750-51; 754; 787; 794-95; 797; 845; 851-52	3.0; 3.2; 3.4; 3.5; 3.6; App. B; App. D	NIST rightly emphasizes that the Draft Privacy Framework is voluntary and flexible, not a set of "one-size-fits-all solutions." NIST should make these points clearly in every facet of the document to preempt any confusion. CTIA suggests three targeted edits.	Second, NIST should clarify or replace the term "privacy requirements," which appears throughout the document. NIST should make clear at the outset that "privacy requirements" do not refer to government-imposed requirements or requirements imposed by the Privacy Framework, but rather are "a means of expressing the legal obligations, privacy values, and policies to which the organization intends to adhere." Alternatively, NIST could simply use a different term, such as "privacy targets." Clarifying that any "requirements" are often self-imposed would reduce any potential ambiguity about the voluntary nature of the Draft.	Technical
11	CTIA	Melanie Tiano / MTiano@ctia.org	24, 26	684	App. A	NIST rightly emphasizes that the Draft Privacy Framework is voluntary and flexible, not a set of "one-size-fits-all solutions." NIST should make these points clearly in every facet of the document to preempt any confusion. CTIA suggests three targeted edits.	Third, NIST should ensure that in describing Functions, Categories, and Subcategories NIST's language cannot be misconstrued as being prescriptive. NIST should add clarifying language to make clear that its descriptions are not misconstrued as requirements. For example, NIST could edit CT.PO-P4 as follows: "Policies, processes, and procedures for enabling individuals' data processing preferences and requests, where applicable, are established and in place." As another example, NIST could amend CM.AW-P7 to read: "Impacted individuals and organizations are notified, where appropriate, about a privacy breach or event."	Technical

12	CTIA	Melanie Tiano / MTiano@ctia.org	6-7	215-32	1.2.1	To achieve wide applicability, the Privacy Framework should not promote any policy approach and should remain neutral and value-agnostic. NIST generally follows this approach, but three edits will preserve this approach across the entirety of the Draft.	First, NIST should refrain from defining privacy harms broadly. The Draft says that "problems" that may arise from data processing "rang[e] from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm." CTIA understands that NIST is trying to illustrate a wide range of risks, including problems beyond legally cognizable harms. But NIST should avoid grouping "dignity-type effects" with tangible economic or physical harms. There is significant debate over whether the former should be included in legislative or regulatory definitions of "harm." Indeed, CTIA has urged the FTC to focus on actual, concrete injuries. The question of privacy harm should be addressed by policymakers, so NIST should ensure that its discussion of privacy "problems" does not inadvertently address contested issues.	Technical
13	CTIA	Melanie Tiano / MTiano@ctia.org	30	687	App. B	To achieve wide applicability, the Privacy Framework should not promote any policy approach and should remain neutral and value-agnostic. NIST generally follows this approach, but three edits will preserve this approach across the entirety of the Draft.	Second, NIST should reconsider its definition of "privacy breach" to ensure that NIST is not favoring one legal regime. One important issue in breach notification legal and regulatory approaches is how to define "breach," with a key element being a reasonable expectation of harm; however, NIST's definition does not incorporate this element. Unauthorized access—standing alone and without a reasonable expectation that such action will lead to harm—is not necessarily a problem. For example, unauthorized access to data by a customer service agent who accidentally and with no ill-intent accesses the wrong information about a customer should not be swept into the definition of "breach." At the very least, NIST should make clear that the reasonable expectation of harm is an important part of what constitutes a "breach" under any given legal regime, and that NIST's use of term "breach" is distinct from the legal term—which triggers often onerous obligations for companies who have suffered a breach.	Technical

14	CTIA	Melanie Tiano / MTiano@ctia.org	10	364-67	2.1	To achieve wide applicability, the Privacy Framework should not promote any policy approach and should remain neutral and value-agnostic. NIST generally follows this approach, but three edits will preserve this approach across the entirety of the Draft.	Third, NIST should refrain from taking a position on the political question of when notice is required and what constitutes adequate notice. In describing the Communicate-P Function, NIST states that "individuals need to know how data are processed in order to manage privacy risk effectively." Whether, when, and how to address notice to consumers is a policy judgment. It might be better to use language from elsewhere in the draft: that an organization "[d]evelop and implement appropriate" mechanisms to communicate to individuals how data are processed to manage privacy risk effectively.	Technical
15	CTIA	Melanie Tiano / MTiano@ctia.org	N/A	N/A	N/A	CTIA supports the Privacy Framework. It will be a valuable tool for industry moving forward and—like the Cybersecurity Framework—the Draft bears all the hallmarks of a highly effective NIST publication. CTIA encourages NIST to adopt targeted edits to further its goals.	N/A	General