From: Kate Goodloe <Kateg@bsa.org>
Sent: Thursday, October 24, 2019 3:57 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Aaron Cooper <aaronc@bsa.org>
Subject: NIST Privacy Framework: Preliminary Draft Comments

BSA | The Software Alliance appreciates the opportunity to comment on the preliminary draft NIST Privacy Framework. Our comments are attached. If the NIST team has any questions or comments, please let us know. We would welcome the opportunity to further engage on these important issues.

Best,

Kate Goodloe

BSA
Kate Goodloe
Director, Policy
BSA | The Software Alliance
P 202-530-5122
W bsa.org

October 24, 2019

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

RE: Preliminary Draft of NIST Privacy Framework

Dear Ms. MacFarland:

BSA | The Software Alliance appreciates the opportunity to comment on the preliminary draft Privacy Framework developed by the National Institute of Standards and Technology ("NIST"). BSA is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.[1]

BSA supports NIST's development of a voluntary risk management framework for enterprises, which can be an important operational tool for businesses seeking to identify and address privacy risks. Moreover, BSA supports NIST's open and collaborative process in developing the Privacy Framework.

BSA submits these comments to suggest improving the Privacy Framework in two ways:

- *First, we encourage NIST to clarify how different types of companies can use the Privacy Framework differently*. This can be done by: (1) encouraging companies to identify their role in the data processing ecosystem before using the Privacy Framework, (2) emphasizing that companies should apply the Privacy Framework in light of that role, and (3) providing new examples of how different types of companies may use the Privacy Framework. In particular, we encourage NIST to show which aspects of the Privacy Framework should be applied by companies that decide how data about individuals is collected, used, and shared (and thus act as data controllers), and which aspects should be applied by companies that store, analyze, or process data at the direction of another company (and thus act as data processors).

- *Second, we encourage NIST to support interoperability with international standards*. In particular, we encourage NIST to ensure the process for accepting informative references to existing guidance prioritizes the publication of mappings to key global standards.

[1] BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

These suggestions will help ensure that a wide range of companies—across business types, industries, and geographies—can more readily adopt the Privacy Framework.

I. NIST Should Clarify How Different Types of Companies—Including Controllers and Processors—Can Use the Privacy Framework Differently.

When companies focus on their role in handling data about individuals, they can more effectively identify and implement controls to help protect the privacy of those individuals. For that reason, we encourage NIST to clarify how different types of companies should use the Framework differently, based on their role in the data processing ecosystem.

To help companies identify their role in the data processing ecosystem—and the privacy protections best suited to that role—we recommend that NIST incorporate the concepts of data controllers and data processors into the Privacy Framework. This distinction pervades the ecosystem, and distinguishes companies that decide how data about individuals is collected, used, and shared—and thus act as controllers of that data—from companies that process data at the direction of another company—and thus act as processors of that data.

The roles of controllers and processors are important from a privacy perspective because when companies adopt role-dependent responsibilities it improves privacy protection. Both controllers and processors have important obligations to ensure consumers' privacy. However, a company that adopts privacy controls not suited to its role as either a controller or processor may inadvertently adopt practices that increase privacy risks rather than reduce them. For example, a processor often does not know the content of data being processed, a restriction that supports personal privacy by limiting the number of individuals who view personal information. However, in order to provide some important consumer rights—such as the right to access or correct personal data, or to object to processing—a company must know the content of data at issue. For that reason, the controller is generally the entity that should respond to those requests. If processors adopted procedures to provide such consumer rights, it might require them to access data they otherwise would not. That result would inadvertently undermine, not increase, privacy protection. It would also be inefficient for companies that process data on behalf of another business to undertake the same obligations as the business that decides how data is collected, used, and shared; even if processors could comply with these obligations—which is not always the case—doing so would lead to duplicative and unnecessary efforts and expenses.

Incorporating the concepts of controllers and processors into the Privacy Framework will also help maximize adoption of the Privacy Framework in two ways:

- *Maximizing Use of The Framework by a Range of Different Companies and Industries.* The Privacy Framework already recognizes the broad range of companies in the data processing ecosystem, including service providers, customers, partners, product manufacturers, and application developers. These companies may act as controllers if they decide how data about individuals is collected and used, and as processors if they handle data at the direction of another company. By recognizing these different roles, the Framework can help companies more readily identify and adopt controls that are appropriate to their role.

- *Maximizing Use of the Framework Globally.* Although the terms controller and processor are drawn from the European Union's General Data Protection Regulation ("GDPR"), the distinction is also recognized in widely-adopted voluntary frameworks that promote data privacy and cross-border transfers. For example, the APEC Cross Border Privacy Rules, which the U.S. Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data

demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors.

In addition, privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.[2] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others.[3] In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology.[4] In the United States, the California Consumer Privacy Act ("CCPA") also makes this distinction, assigning a set of legal obligations to "businesses" that "collect[] consumers' personal information . . . and that alone, or jointly with others, determine[] the purposes and means of the processing of consumers personal information" while assigning other legal obligations to "service providers" that "process information on behalf of a business."[5]

Companies worldwide can more readily adopt the Privacy Framework if it reflects this fundamental distinction between controllers and processors, which is vital to the data processing ecosystem. Moreover, adopting the concepts of controllers and processors will make the Privacy Framework more interoperable, because it will allow companies to more readily understand how its controls map onto other legal and regulatory obligations they may have across jurisdictions.

We suggest three changes to the Privacy Framework to incorporate the concepts of controllers and processors:

(1) encourage companies to identify their role in the data processing ecosystem before using the Framework;

(2) emphasize that the Framework should be applied in light of that role; and

(3) provide new examples of how different companies may use the Framework, including controllers and processors.

We have included an Appendix to these comments that identifies specific language NIST may use to implement each suggestion.

---

[2] The GDPR defines controllers as "the natural or legal person, public authority, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." Article 4(7). In contrast, processors are defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." Article 4(8).

[3] Hong Kong Personal Data (Privacy) Ordinance Section 2(1) (defining data user); Malaysia Personal Data Protection Act 2010, Section 4 (defining both data users and data processors); Argentina Personal Data Protection Law Article 2 (defining data user) and Article 25 (defining third party processors).

[4] Mexico Federal Law on the Protection of Personal Data Held by Private Parties, Article 3, XIV (defining controller) and Article 3 IX (defining controller); Philippines Republic Act 10173 – Data Privacy Act of 2012, Section 3(h) (defining personal information controller) and Section 3(i) (defining personal information processor); Switzerland Federal Act on Data Protection, Article 3(j) (defining controller) and Article 10 (regulating processing by third parties).

[5] California Consumer Privacy Act, Cal. Civil Code § 1798.140(c) (defining business) and § 1798.140(v) (defining service provider).

II. NIST Should Incorporate International Standards Into the Privacy Framework.

BSA also encourages NIST to ensure the Privacy Framework is interoperable with international standards. The Privacy Framework already recognizes the importance of aligning to existing international standards, guidelines, and practices, which can evolve with technology and related business needs. We agree with the Privacy Framework's recognition that using existing and emerging standards will "enable economies of scale and drive the development of systems, products, and services that meet identified market needs while being mindful of the privacy needs of individuals."

We understand that NIST will not conduct mappings itself, beyond mapping the Subcategories to relevant NIST guidance. Rather, it will accept mappings from organizations and industry sectors, which will be maintained as informative references on NIST's website. We encourage NIST to ensure this process of accepting informative references prioritizes the publication of mappings to key existing global standards. In particular, we encourage NIST to ensure there is an authoritative mapping to the International Standards Organization 27701. That standard, released in August 2019, identifies requirements and provides guidance for establishing, implementing, maintaining and improving a privacy information management system, and thus complements the goals of the Privacy Framework. In addition, NIST should consider prioritizing mappings to standards that may be relevant to data security and breach incidents, such as the CIS20.

* * *

Finally, we also we encourage NIST to further explain how companies using the Privacy Framework should consider the Cybersecurity Framework in developing a privacy risk management system. When a company voluntarily implements both the Privacy Framework and Cybersecurity Framework, it can create a consistent and unified approach to privacy and security. We suggest specific language in the Appendix to implement this suggestion.

NIST's Privacy Framework comes at a critical time, when a range of organizations are assessing how to best protect consumer privacy. BSA appreciates NIST's contribution to this broader dialogue and is pleased to serve as a resource on these issues.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance

APPENDIX

This Appendix identifies specific language for incorporating the concepts of controllers and processors into the Privacy Framework As set out above, we recommend three sets of revisions to: (1) encourage companies to identify their role in the data processing ecosystem before using the Framework, (2) emphasize that the Framework should be applied in light of that role, and (3) provide new examples of how different companies may use the Framework.

- **First Suggestion: Emphasize that a company should consider its role in the data processing ecosystem before using the Privacy Framework.**

  This suggestion can be implemented by revising the following sections of the Privacy Framework:

  - Section 3.0: This section explains how companies can use the Privacy Framework. We suggest adding new text in the introduction, explaining that a company should identify its own role in the data processing ecosystem before using the Privacy Framework and to recognize that one company may have different roles in different contexts. For example, a service provider may act as a processor with respect to certain data, but as a controller for its own internal HR data. To help companies identify their roles, NIST could add a new paragraph that states the Privacy Framework is intended for use by a wide variety of companies across the data processing ecosystem, including both companies that decide to collect, use, or share data about individuals (and thus act as data controllers) and companies that store, analyze, or otherwise process data at the direction of other companies (and thus act as data processors). Before utilizing the Privacy Framework, a company should identify its role in the data processing ecosystem, including whether it acts as a controller or a processor of the relevant data, so that it can use the Privacy Framework to identify controls appropriate to that role.

  - Section 3.3: This section introduces "ready, set, go" phases to establish or improve a privacy program. We suggest adding new language to the "ready" phase, to emphasize that an organization should identify its role in the data processing ecosystem to be ready to implement a privacy program. For example, the current language can be modified to state that "Effective privacy risk management requires an organization to understand its business or mission environment, *including its role in the data processing ecosystem. For example, a company seeking to use the Privacy Framework should determine if it collects, uses, or shares an individual's data, or only stores, analyzes or otherwise processes that data at the direction of another company, so that it can establish or improve a program that is appropriate to its role."*

    In the "Go" phase, we similarly suggest new language clarifying that an organization "should determine which standards, guidelines, and practices, including those that are sector specific, work best for its needs, *given the role of the organization in handling data about individuals*."

- **Second Suggestion: Explain that a company should apply the Privacy Framework in light of its role in the data processing ecosystem.**

  This suggestion can be implemented by revising the following sections of the Privacy Framework:

- Section 1.0: This introductory section explains that the Privacy Framework is "usable by any organization or entity regardless of its role in the data processing ecosystem." We suggest emphasizing this point, by moving the text to the first bullet point in this subsection. (The remaining points would then follow.)

- Section 1.1: In describing the three parts of the Privacy Framework, NIST should be clear that each of these parts (core, profile, and implementation tiers) will apply differently to different organizations, based on their role in collecting, using, and sharing data about individuals. In particular, at the end of the bullet point explaining the Core, we suggest adding a new sentence stating that "*Organizations may apply the Core differently depending on their role in the data processing ecosystem, including whether they decide to collect and use data about individuals or only process that data on behalf of other companies*."

- Section 2.1: This section discusses the Core and emphasizes that the five Core Functions are "not intended to form a serial path or lead to a static desired end state." We suggest adding new language at the end of this section, to state that the Functions "should be performed concurrently and continuously to form or enhance operational culture that addresses the dynamic nature of privacy risk, *depending on the organization's role in handling data about individuals."*

- Section 2.2: This section discusses how organizations may use profiles. We suggest clarifying that "When developing a Profile, an organization may select or tailor the Privacy Framework's Functions, Categories, and Subcategories to its specific needs, *and in light of the organization's role in handling data about individuals*."

- Section 3.0: In addition to recognizing that there are a "wide variety of ways to use the Privacy Framework," we suggest adding "*depending on the organization's role in handling data about individuals*."

- Section 3.5: We recommend re-ordering this section, to make the first and primary point that "An organization should use the Privacy Framework from its standpoint in the data processing ecosystem." By moving this existing text to the top of the section, NIST can emphasize the broad range of companies that can use the Privacy Framework, before explaining the secondary point that all of those companies can communicate through the common language created in the Privacy Framework. We also support retaining the existing text explaining that "In practice, an organization's role(s) may be legally codified – for example, some laws classify organizations as data controllers or data processors – or classifications may be derived from sector-specific classifications."

- Appendix A: This appendix contains the Core of the Privacy Framework and an introductory note on how to use it. We suggest three changes to that note:

    - *First*, we recommend elevating the bullet point on "ecosystem" to the beginning of the note. This would make clear that the Core can be used by a wide range of organizations, and that organizations using the Privacy Framework should do so from their "standpoint in the ecosystem."

    - *Second*, in discussing the "Privacy Framework's risk-based approach" we recommend revising the first bullet point to more clearly state how the Core will apply differently to different types of organizations. For

example, the text could be modified to state "[a]n organization may not need to achieve every outcome or activity reflected in the core, *and the application of the core will depend in the organization's role in collecting and using data about individuals, including whether it decides how such data will be collected and used or instead processes the data on behalf of another company*."

- *Third*, in the paragraph on implementation, we recommend being clear that implementation will depend on an organization's role in the data processing ecosystem. For example, the text could be revised to state that: "Implementation may be nonsequential, simultaneous, or iterative, depending on the SDLC stage, status of the privacy program, scale of the workforce, *or role of the organization in collecting and using data about individuals*."

- Appendix D: This appendix considers key practices relating to privacy risk management. In the section on "organizational-level privacy requirements," we suggest adding an additional bullet point to the list from which privacy requirements may be defined: "*The organization's role in collecting and using information about individuals, (e.g., whether it acts as a controller or a processor of the data)."*

- **Third Suggestion: Provide new examples of how different companies may use the Privacy Framework.**

  This suggestion can be implemented by revising the following sections of the Privacy Framework:

  - Section 3.5: This section on the data processing ecosystem explains that a range of companies can use the Privacy Framework. We suggest revising the text to incorporate examples of those companies, and to explain how different companies may use the Privacy Framework differently, depending on their role.

    Specifically, we suggest modifying the four bullet points in this section that provide examples of how an organization can use Profiles to select Functions, Categories, and Subcategories, to highlight how different companies may use the Profiles based on their role in the data processing ecosystem. These changes can include:

    - Modifying the first example to state that "An organization *that makes decisions about how to collect and use data about individuals* may use a Target Profile to express privacy risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data)."

    - Adding an example about service providers or processors, which could state that: "An organization that processes data on behalf of other companies may use a Target Profile to demonstrate the privacy controls it has adopted to process data in line with contractual obligations."

  - Other Sections: More broadly, we encourage NIST to incorporate additional examples throughout the Framework, including either in Section 3.5 or elsewhere, to illustrate how the core functions may apply differently to controllers and processors. Specifically, we recommend incorporating examples that

discuss how each of the Core functions can apply to controllers and processors. For example:

- In explaining the "Identify" function, NIST could recognize that many of its categories are appropriately implemented by companies that decide how data about individuals will be collected and used (e.g., controllers). Companies that process data about individuals at the direction of another company are unlikely to have insight into information needed to use several of the subcategories. Processors that do not actually look at the content of data they process on behalf of other companies, for example, may not know the categories of individuals whose data is being processed, and thus could not distinguish between customer data and employee data in the ordinary course.

- Similarly, the control and communicate functions contain subcategories better suited to controllers, since they generally have a direct relationship with individuals whose data they collect. In contrast, the "Govern" function may be used by both processors and controllers to develop governance policies tailored to their role in the data processing ecosystem. For example, processors may have a "privacy value" of processing data in line with instructions from a controller. In addition, the "Protect-P" function contains data security controls that may be appropriately utilized by both controllers and processors.

* * *

We also suggest three changes to explain how companies using the Privacy Framework should consider the Cybersecurity Framework in developing a privacy risk management system:

- In Appendix A, we recommend modifying the explanatory note to emphasize how users of the Privacy Framework can use the Cybersecurity Framework's functions in developing their privacy risk management system. For example, the language could be modified to state that "Organizations should consider functions under the Cybersecurity Framework, particularly the Respond function, as they create current and target profiles. Privacy risks are appropriately managed with cybersecurity risk management, and the ability to respond to privacy events and breaches is an important component of a privacy risk management framework."

- In Appendix A, we recommend modifying the explanatory note to reference not only the Cybersecurity Framework but also the NIST Risk Management Framework. In particular, we encourage NIST to show that all three frameworks can be used together to effectively manage privacy risk.

- Finally, we recommend including within the Framework itself or as an informative reference a detailed mapping of the Privacy Framework's functions, categories, and subcategories to those in the Cybersecurity Framework. This mapping could build on NIST's prior efforts to map the two frameworks.[6]

[6] *See, e.g.*, Comparison of the Privacy Framework Discussion Draft and the Cybersecurity Framework Cores, *available at* https://www.nist.gov/sites/default/files/documents/2019/05/09/comparison_of_the_privacy_framework_core_to_the_cybersecurity_framework_core_05.09.2019.pdf.