Drafting the NIST Privacy Framework: Summary of Workshop #2

May 13-14, 2019
Atlanta, Georgia

On May 13-14, 2019, the National Institute of Standards and Technology (NIST) held its second in a series of public workshops on the development of the Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework) at the Georgia Institute of Technology (Georgia Tech) Scheller College of Business in Atlanta, Georgia.[1] The workshop provided an opportunity for attendees to actively engage in facilitated discussions to advance the development of the Privacy Framework.[2]

A total of 177 participants attended the workshop in-person, representing a broad diversity of sectors including information technology, financial, government, consulting, healthcare, education, civil society, and law, as well as interested individuals. Participants also represented a mixture of roles, sometimes overlapping, but including privacy, security, risk management, and compliance, and a range of positions from the executive level to the technical level. An additional 213 viewers attended via live webcast of the plenary sessions on the morning of May 13.[3]

Workshop Format

Prior to the workshop, NIST released a discussion draft of the Privacy Framework as well as two related resources: the *Core Comparison of the Privacy Framework Discussion Draft and the Cybersecurity Framework* and *NIST Informative References*.[4] NIST organized the workshop around discussion of these three documents in order to obtain participant feedback to improve the next draft of the Privacy Framework.

Participants were welcomed by co-Georgia Tech host, Professor Annie Antón, and Donna Dodson, Chief Cybersecurity Advisor at NIST. Following opening remarks, there were three panels, "Discussion Draft of the Privacy Framework with NIST," "Voices from the Field," and "Global Policy Landscape"—and a presentation on "Expanding the OSI Stack to Describe Categories of Privacy Tasks" by co-Georgia Tech host, Professor Peter Swire.[5] The panels and presentation enabled participants to hear a progress update and overview of the discussion draft from NIST leadership, as well as various viewpoints on the discussion draft from privacy practitioners to stimulate discussion in the working sessions. General themes from the morning discussion panels are incorporated in the "General Workshop Themes" section below.

---

[1] See https://www.nist.gov/news-events/events/2019/05/drafting-nist-privacy-framework-workshop-2.
[2] For more information about the development of the Privacy Framework, see https://www.nist.gov/privacy-framework.
[3] To view a recording of the webcast, see https://www.nist.gov/news-events/events/2019/05/drafting-nist-privacy-framework-workshop-2.
[4] See https://www.nist.gov/sites/default/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf, 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, and https://www.nist.gov/sites/default/files/documents/2019/04/30/nist-informative-references-privacy-framework-discussion-draft.pdf.
[5] For more information about the panels and presentations, see https://www.nist.gov/news-events/events/2019/05/drafting-nist-privacy-framework-workshop-2.

Following the plenary session, participants were assigned to one of six groups for three sequential facilitated working sessions to discuss specific feedback on the core functions, categories, and subcategories; profiles; and implementation tiers as presented in the discussion draft. In the final two facilitated working sessions, participants could select from among six topics and engage in a more in-depth discussion on: 1) informative references and roadmap, 2) communications, 3) privacy risk management, 4) small and medium sized businesses, 5) workforce, and 6) a simulated use case. The sixth topic was initially slated as a "to be announced" session; NIST determined that stress testing the Privacy Framework through a simulated use case would offer opportunities to identify additional areas for improvement, after the plenary and working sessions on the first day of the workshop.[6]

General Workshop Themes

Feedback from workshop participants represented a diversity of views and exemplified the challenges associated with developing a framework that is accessible and scalable to meet organizations' diverse privacy needs. Overall though, participants validated the need and desire for the Privacy Framework to enhance communication about privacy risks across and between organizations.

Privacy Risk Management

Generally, participants agreed with NIST's approach to provide a more in-depth treatment of privacy risk management, in contrast to the approach in the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), although certain aspects generated constructive discussion.[7] For example:

- Although participants generally agreed that individuals should be the focus of privacy risk, a number of participants thought there needed to be more clarification on the relationship between privacy risk and organizational risk.
- There were conflicting viewpoints on the discussion draft's presentation of the relationship between privacy risk and cybersecurity risk (e.g., the Venn diagram presented in discussion draft Figure 1); some agreed with the presentation and representation, while others did not think it accurately portrayed the full scope of privacy risk. Some participants suggested that more specific examples be given on what constitutes a privacy risk.
- Some participants asked for specific examples of problematic data actions including the specific problems or harms to individuals.
- The relationship between privacy risk and compliance risk also generated significant discussion:
    - A number of participants wanted to see a more prominent role for legal requirements throughout the core - often citing that the legal environment is the primary driver of privacy programs and resource allocations.
    - Several participants raised the concept of trust, noting that mere compliance with law does not always achieve trust; therefore, the Privacy Framework offers a mechanism to go beyond just compliance.

Communication

Discussions around use of the Privacy Framework and organizational challenges validated the need for a communication vehicle when it comes to privacy. Many expressed the need for a common language to

[6] See the simulated exercise at https://www.nist.gov/news-events/events/2019/05/drafting-nist-privacy-framework-workshop-2.

[7] See *Framework for Improving Critical Infrastructure Cybersecurity* at https://doi.org/10.6028/NIST.CSWP.04162018.

communicate about privacy and privacy risk with all levels of the organization. Other examples of feedback included:

- Some participants familiar with the Cybersecurity Framework liked the ability to use the five functions to talk to the "C-Suite" about cybersecurity risk and recognized the potential value for it in the Privacy Framework.
- Some participants expressed that the discussion draft seems more accessible to engineering personnel and that more work would need to be done to make the document more accessible to legal and policy personnel who may be partly responsible for implementing organizational privacy programs.
- Some participants raised concerns that the document may not be accessible to small and medium businesses (SMBs) and that additional resources may be necessary to guide them. Then again, other participants thought that there was helpful guidance for SMBs, for example, Appendix D of the discussion draft.

Roles

Much of the discussion about using the Privacy Framework as a communication tool led to questions about which parties within an organization would or should be responsible for implementing the Privacy Framework. For example:

- Participants provided a variety of examples of how their organizational privacy programs are implemented. Some participants, as noted in the *Communication* and *Privacy Framework Alignment with the Cybersecurity Framework* general themes in this report, identified the need to make the document accessible to a variety of roles that might be responsible for implementation.
- Some participants asked for clarification about the relationship between organizations, as the users of the Privacy Framework, and individuals that are impacted by the organizations' products, systems, or services.
- Some participants also asked for clarification about the role of the individual as it relates to the outcome statements presented in core functions like Control and Inform and whether these statements were aimed at conveying rights to individuals or for organizations to build capabilities to enable individual rights (e.g., access, correction, deletion).
- Some participants in the workforce session noted that more work will be needed to identify a workforce with the knowledge, skills, and abilities to execute on the outcomes and informative references. Currently there are few privacy certifications available in the marketplace and these tend to be focused on legal compliance.

Privacy Framework Alignment with the Cybersecurity Framework

For the most part, attendees agreed with aligning the structure of the Privacy Framework with the structure of the Cybersecurity Framework. There were differing viewpoints on specific aspects of the alignment, such as:

- Although there was general agreement that data security has privacy impacts, there were a variety of views on the extent to which the Privacy Framework should reuse functions, categories, and subcategories from the Cybersecurity Framework.
    - Some participants expressed that Cybersecurity Framework functions, categories, and subcategories that address data security should be maintained so the Privacy Framework could be used independently from the Cybersecurity Framework.

    - Other participants expressed concern that security teams rather than privacy teams typically implement data protection measures, and consequently these Cybersecurity Framework outcomes did not belong in a Privacy Framework.
- Some participants felt that NIST should more clearly articulate which categories and subcategories came from the Cybersecurity Framework—either copied exactly or modified slightly.

Improving Core Functions, Categories, and Subcategories

Throughout the workshop NIST heard various suggestions for clarifying and improving upon the functions, categories, and subcategories, including word changes, re-ordering, adding, deleting, or clarifying language. For example:

- Some participants raised concerns about whether the core functions (especially the uniquely privacy ones, Control and Inform) adequately encompassed privacy principles such as data minimization.
- Some participants thought the Control and Inform functions should be renamed, whereas other participants disagreed.
- Some participants commented that the Control function was unclear as to its intended scope and may be confused with controls (e.g., technical or policy measures) that an organization applies to its information systems to meet requirements.
- Some participants suggested re-ordering categories and subcategories in the Identify function to identify the laws and regulations earlier on in the process.
- Some participants thought the Detect and Recover functions from the Cybersecurity Framework should be added to the Privacy Framework.

Utility of Profiles and Tiers

Reactions to the profiles and tiers constructs generally varied by experience with the Cybersecurity Framework. For example:

- Some participants stated that profiles and tiers could be useful and offered perspectives from their experiences with using them in the Cybersecurity Framework.
- Some participants expressed that it was unclear how to use profiles and/or how they could be used by their respective organizations. Such feedback led NIST to offer a hypothetical use case exercise during working sessions 5 and 6 that allowed participants to envision how profiles might be used.
- Some participants expressed concern that despite the discussion draft explicitly stating that tiers are not maturity models, that the discussion draft, as written, still suggests they are maturity models and may be used by auditors and regulators as such.

Terms and Definitions

Participants commented on the clarity of terms and definitions, including:

- Data – many participants questioned whether the definition of data was intended to include only digital data and expressed that the definition should be inclusive of all forms of media (e.g., paper).
- Data Processing – some participants disagreed with the use of the term “data processing” or were unclear whether it was inclusive of the full data life cycle.
- Privacy Breaches and Privacy Events – some participants expressed that privacy breaches and privacy events did not encompass all potential privacy problems and were too cybersecurity focused.

- Individual – some participants commented that use of the term individual may be too broad or that it was not always clear the category of individuals intended (e.g., employees, patients, customers).
- Supply chain – some participants expressed that "supply chain" implied a vertical organizational relationship that was too limited for the privacy context and suggested using "third party" instead.

Informative References

Reactions to informative references generally varied by participants' understanding of how such references could be used by organizations to achieve the outcomes in the core. For example:

- During the morning plenary sessions as well as the working sessions on the core, many participants noted that it was not clear how to achieve the outcomes in the categories and subcategories in part because NIST removed the informative references from the core.
- Some participants had questions generally about the proposed approach to maintain informative references in a separate repository given that it currently varies from the approach taken with the Cybersecurity Framework.
- Some participants suggested that privacy laws and regulations should be considered for informative references given their role in how organizations implement their privacy programs. However, as the workshop progressed participants seemed to be more comfortable with the idea of a Privacy Framework that is agnostic to laws and regulations and suggested that rather than include laws and regulations as an informative reference, industry could attempt to map laws and regulations to the Privacy Framework.

Next Steps

NIST will consider the feedback it received throughout the two-day workshop and use this information to develop the next iteration of the Privacy Framework. NIST announced two upcoming events: a webinar on the discussion draft on May 28, 2019, and a third public workshop, *Getting to V1.0 of the NIST Privacy Framework: Workshop #3*, scheduled for July 8-9, 2019, hosted by the School of Public Service at Boise State University in Boise, Idaho.[8,9] In advance of the third workshop, NIST will release supplemental materials for discussion at the workshop. NIST continues to encourage additional feedback on the discussion draft. Feedback may be sent to privacyframework@nist.gov.

[8] See https://www.nist.gov/news-events/events/2019/05/webinar-nist-privacy-framework-discussion-draft.
[9] See https://www.nist.gov/news-events/events/2019/07/getting-v10-nist-privacy-framework-workshop-3.