Kicking off the NIST Privacy Framework: Summary of Workshop #1

October 16, 2018
Austin , Texas

In the first of a series of public workshops, the National Institute of Standards and Technology (NIST) hosted *Kicking off the NIST Privacy Framework: Workshop #1* on October 16, 2018, in Austin, Texas. Approximately 130 stakeholders attended in person to learn about and collaborate on the development of the NIST Privacy Framework: An Enterprise Risk Management Tool. An additional 108 participated via live stream. A video of the event is available at the workshop event page. In advance of the workshop, NIST provided supplemental material for discussion and feedback.

Background

In an increasingly connected and complex environment, it is a challenge to design and implement technologies and larger ecosystems that are mindful of diverse privacy needs. Although good cybersecurity practices incorporate protection of personally identifiable information (PII), they are insufficient on their own to meet individuals' privacy interests and the growing innovation of technology beyond the traditional computing paradigm to larger ecosystems like the Internet of Things. Organizations need access to additional tools to better address the full scope of privacy risk. Privacy risks can arise even within the authorized processing of PII when addressing other organizational needs including mission or business objectives.

With this challenge in mind, NIST is collaborating with the private and public sectors to develop a voluntary, enterprise-oriented, risk management framework to help organizations to protect individuals' privacy. NIST envisions that the framework will serve as a tool that organizations can use to better manage privacy risks within diverse environments – and result in increased trust in products and services.

Summary of Panel Discussion Themes

The workshop was structured around three panel discussions: Introduction to the Privacy Framework, Attributes of the Privacy Framework, and Core Privacy Practices. During the first panel, NIST officials provided an overview of the objectives of the Privacy Framework and the development process. The other two panel discussions were comprised of private and public sector representatives who offered a range of perspectives. NIST used these panel discussions to stimulate an interactive dialogue among panelists and other workshop participants. During the workshop, NIST sought feedback on how to structure the framework and the privacy practices to cover so that organizations can use the framework to improve upon, and easily integrate with, existing privacy risk management processes in order to achieve more effective and consistent privacy outcomes for individuals.

Panel Discussion #1: Introduction to the Privacy Framework

Panelists:

- Naomi Lefkovitz, Senior Privacy Policy Advisor, NIST
- Donna Dodson, Chief Cybersecurity Advisor, NIST
- Kevin Stine, Chief, Applied Cybersecurity Division, NIST

NIST representatives discussed objectives and the process for developing the Privacy Framework. Key points included:

- NIST is committed to providing an open, transparent, and collaborative process to develop the framework with stakeholders, building on the model used to develop the Framework for Improving Critical Infrastructure Cybersecurity (CSF).
- Privacy risk extends beyond data security to risks arising from the byproduct of authorized processing of data.
- NIST's working assumption is that organizations would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections.
- NIST seeks to develop a tool that is interoperable with established privacy guidance and standards, is outcome-based, and supports organizations' ability to operate under various legal or regulatory regimes.

Panel Discussion #2: Attributes of the Privacy Framework

Panelists:

- Marc Groman, Principal, Groman Consulting Group LLC (Moderator)
- Ron Whitworth, Senior Vice President and Chief Privacy Officer, SunTrust
- Kent Landfield, Chief Standards and Technology Policy Strategist, McAfee
- Sarah Morrow, Chief Privacy Officer, Texas Health and Human Services
- Michelle Dennedy, Vice President and Chief Privacy Officer, Cisco

Panelists shared cross-sector perspectives on what needs the framework should address, as well as key attributes and structure of an effective privacy framework. Key points included:

- Modeling this process after the CSF development process is desirable, as that approach enabled a wide variety of sectors to engage, forced tough and productive conversations among stakeholders, and provided a communication tool across organizational levels, including the C-suite.
- There are risks both with not defining, or too narrowly defining, terms associated with the framework, including the fundamental term of "privacy."
- The framework should be repeatable and interoperable with the privacy management tools and models that are already in use; be flexible so that it can be applied in various sectors; be perceived as a benefit to organizations from a business perspective that also supports positive outcomes for individuals; and be an "object of desire" for organizations interested in improving their management of privacy risks.
- There is strong interest in taking a risk-based, more strategic approach to privacy. While addressing legal compliance is important, organizations increasingly are shifting away from strictly compliance-oriented approaches.

Panel Discussion #3: Core Privacy Practices

Panelists:

- Rebecca Herold, CEO, The Privacy Professor; Founder, SIMBUS, LLC (Moderator)
- Sagi Leizerov, Chief Data Solutions Officer, Prifender

- Charlie Cabot, Research Lead, Privitar
- Maritza Johnson, UX Principal, Good Research; Researcher, ICSI
- Michelle Richardson, Director, Privacy and Data Project, Center for Democracy and Technology (CDT)

This panel discussion focused on specific privacy practices for potential inclusion in the framework, including data management, human-centered research techniques, privacy-enhancing technologies, and de-identification. Key points included:

- The framework would be particularly useful if it bridged the fundamental gap between policies and the reality of managing data involved in organizational operations.
- The framework should take into account human-centered design to help organizations make reasonable decisions regarding the processing of data instead of the easiest decision.
- There is value in addressing privacy-enhancing technologies in the framework. It will be important to consider the appropriate level of granularity as the use of these technologies is often context-dependent and may not yet be widely or easily implemented.
- The framework should address a problem that we have today; organizations need to do a better job of understanding where they are storing and processing data and who is being provided with that data.
- The framework should explain what data flows are and introduce foundational terms for governance so that everyone from privacy officers, legal counsel, operations staff, engineers, and customers can all speak the same language.
- The framework should be comprehensive and flexible like the CSF, in that it offers many options without prescribing the implementation or use of all of them.
- As some privacy management tools are cost-prohibitive, it will be important to address small and medium-sized organizations' use of the framework.

Workshop Takeaways

NIST heard a range of high-level takeaways about the development of the framework. Kevin Stine summed up some of those key points, stressing that there were many others that were shared during the workshop and that would be considered by NIST in developing the Privacy Framework:

- The framework should be based on a recognition that data is a resource – an asset – and taken in the aggregate, it is the basis for multiple business models today, and likely in the future.
- There is support for an outcome- and risk-based approach to help organizations deliver better products and services where privacy is not just a compliance discussion. This includes a recognition that privacy risks should be managed strategically alongside other types of risk.
- Stakeholders are interested in a comprehensive framework of privacy outcomes and capabilities that is not prescriptive.
- There is a need for a common language or communication tool to be used across various levels of an organization and with external entities to discuss privacy management from the same reference point.
- The framework could help to bridge foundational gaps in the discipline, including data governance and usability.

- Stakeholders strongly support the use of the collaborative process for stakeholder engagement used for the CSF model for the development of the NIST Privacy Framework.
- The framework should make that case that the goal is not to mitigate all risks; it's to be purpose-driven regarding the management of data throughout the lifecycle.
- The audience for the framework is not just large organizations and board rooms, but small businesses as well.
- Definitions matter, including privacy, harm, etc. NIST should continue to seek input on how terms are defined in the framework.
- The framework should be seamless and interoperable with other approaches; it should facilitate harmonization with other approaches and rulesets.
- NIST wants to engage, share, learn, and collaborate as it develops the framework.

Next Steps

NIST officials reinforced that the agency plans to use the comments, discussions, and feedback from this workshop to inform an annotated outline of the Privacy Framework. They stressed that the agency will continue to engage the broader community of stakeholders to facilitate this work. Subsequent to the workshop, NIST will issue a Request for Information soliciting ideas about the Framework. Additional workshops will be held; details will be shared on the Privacy Framework events page. NIST will announce additional opportunities to participate in the open dialogue to build this Privacy Framework.

Officials reminded workshop participants that if they would like to receive updates when materials are posted online for review and feedback, and when events are announced, they should sign up for the NIST Privacy Framework mailing list – and that feedback can be shared at any time by sending an email privacyframework@nist.gov.