Supplemental Material for Kicking off the NIST Privacy Framework: Workshop #1

In this first of a series of public workshops that NIST is hosting on the development of the Privacy Framework: An Enterprise Risk Management Tool, participants will begin to consider how to organize the NIST Privacy Framework and what it should cover. NIST plans to use the input from this workshop to produce an annotated outline of the Privacy Framework for the next round of discussion with stakeholders.

Why is a privacy framework needed?

It is a challenge to design, operate, or use technologies in ways that are mindful of diverse privacy needs in an increasingly connected and complex environment. Cutting-edge technologies such as the Internet of Things and artificial intelligence are raising further concerns about their impacts on individuals' privacy. Inside and outside the U.S., there are multiplying visions for how to address these challenges. Accordingly, NIST is developing a voluntary privacy framework, in collaboration with private and public sector stakeholders, to help organizations: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.

While good cybersecurity practices help manage privacy risk by protecting people's information, privacy risks also can arise from how organizations collect, store, use, and share this information to meet their mission or business objective, as well as how individuals interact with products and services. NIST believes that organizations that design, operate, or use these products and services would be better able to address the full scope of privacy risk with more tools to support better implementation of privacy protections.

What will the NIST Privacy Framework look like?

The purpose of this workshop is to begin the discussion of how to organize the framework and what it should cover. To determine the optimal structure of the framework, it's important to understand where organizations are challenged with achieving better privacy outcomes for their products and services. To facilitate this discussion and for the purposes of this document, NIST is proposing as a working assumption that organizations are challenged with bridging between policies or principles and implementation of effective privacy practices. Through the perspectives of the panelists and participant interaction, NIST would like to explore this working assumption, as well as the attributes of an effective framework to address this challenge, models for structuring the framework, and core privacy practices that the framework should cover.

Potential Attributes of the NIST Privacy Framework

Based on experience with developing *the Framework for Improving Critical Infrastructure Cybersecurity* ("Cybersecurity Framework"),[1] NIST is considering the following set of minimum attributes for the Privacy Framework:

1. **It is consensus-driven and developed and updated through an open, transparent process.** All stakeholders should have the opportunity to contribute to the framework's development. NIST has a long track record of successfully and collaboratively working with the private and public sectors to develop guidelines and standards. NIST will model the approach for this framework based on the successful, open, transparent, and collaborative approach used to develop the Cybersecurity Framework.
2. **It uses common and accessible language.** The framework should be understandable by a broad audience, including senior executives and those who are not privacy professionals. The framework can then facilitate communications among various stakeholders by promoting use of this common language.
3. **It is adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses.** The framework should be scalable to organizations of all sizes, public or private, in any sector, and operating within or across domestic borders. It should be platform- and technology- agnostic and customizable.
4. **It is risk-based, outcome-based, voluntary, and non-prescriptive.** The framework should provide a catalog of privacy outcomes and approaches to be used voluntarily, rather than a set of one-size-fits-all requirements, to foster innovation in products and services and to promote research for and adoption of effective privacy solutions. The framework should assist organizations to better manage privacy risks within their diverse environments without prescribing the methods for managing privacy risk.
5. **It is readily usable as part of any enterprise's broader risk management strategy and processes.** The framework should be consistent with, or reinforce, other risk management efforts within the enterprise, recognizing that privacy is one of several major areas of risk that an organization needs to manage.
6. **It is compatible with or may be paired with other privacy approaches.** The framework should take advantage of existing privacy standards, methodologies, and guidance. It should be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes.
7. **It is a living document.** The framework should be updated as technology and approaches to privacy change and as stakeholders learn from implementation.

[1] https://www.nist.gov/cyberframework/framework

Structuring the Privacy Framework

NIST is interested in understanding how to structure the Privacy Framework to achieve the desired set of attributes and improve integration of privacy risk management processes with the organizational processes for developing products and services for better privacy outcomes.

NIST is particularly interested in how organizations currently structure their privacy programs to manage privacy risk—for example, whether programs are structured around:

- The information life cycle;
- Principles such as the fair information practices principles;
- Objectives, such as the NIST privacy engineering objectives of predictability, manageability, and disassociability;
- Use cases or design patterns; or
- Other constructs.

Core Privacy Practices

NIST is considering including in the Privacy Framework core privacy practices that are broadly applicable across sectors and organizations. To determine whether there are broad-reaching practices that make sense to include in the framework, NIST is interested in information on the degree of adoption of the following practices:

- De-identification;
- Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;
- Enabling user preferences;
- Setting default privacy configurations;
- Use of cryptographic technology to achieve a privacy engineering objective such as disassociability;
- Data management, including:
    - Tracking permissions or other types of data tracking tools,
    - Metadata,
    - Machine readability, and
    - Data correction and deletion;
- Usable design or requirements; or
- Other practices.

STAY ENGAGED

All organizations have an opportunity to be part of the process and contribute to the development of the Privacy Framework. Please send feedback, notes, continued observations, further suggestions, and other applicable information to: privacyframework@nist.gov

For more information about the NIST Privacy Framework, visit: https://www.nist.gov/privacyframework

Sign up for the mailing list receive regular updates on this effort: https://groups.google.com/a/list.nist.gov/forum/#!forum/privacyframework