ITL BULLETIN

ITL BULLETIN JUNE 2020

NIST Privacy Framework: An Overview

Naomi Lefkovitz and Katie Boeckl
Applied Cybersecurity Division
Information Technology Laboratory (ITL)
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce

Introduction

As the Internet and associated information technologies drive unprecedented innovation, economic value, and access to social services, the amount of data about individuals that is changing hands is nearly incalculable. Many of these technological advancements are powered by individuals' data flowing through a complex ecosystem. Finding ways to continue to derive benefits from data while also protecting individuals' privacy is challenging and not well-suited to one-size-fits-all solutions.

To enable better privacy engineering practices and help organizations protect individuals' privacy, NIST developed the Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) following a transparent, consensus-based process including both private and public stakeholders. The voluntary Privacy Framework is a flexible tool intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction.

The Privacy Framework supports:

- Building customer trust through ethical decision-making while minimizing adverse consequences for individuals' privacy
- Fulfilling current and future compliance obligations
- Facilitating communication about privacy practices with organizations, customers, and other interested parties.

Relationship Between Cybersecurity and Privacy Risks

While managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to the loss of confidentiality, integrity, and availability. The Privacy Framework approach to privacy risk is to consider privacy events as potential problems individuals could experience arising from data processing, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. The problems individuals may experience include embarrassment or stigmas, discrimination, economic loss, or physical harm.

Privacy Risk and Organizational Risk

While individuals experience the impact of problems directly, an organization may experience impacts such as noncompliance costs, revenue loss arising from customer abandonment of products and services, or harm to its external brand reputation or internal culture. Organizations commonly manage these types of impacts at the enterprise risk management level. By connecting problems that individuals experience to well-understood organizational impacts, organizations can bring privacy risk into parity with other risks they are managing in their broader portfolio and build better privacy foundations.

Framework Structure

The Privacy Framework follows the structure of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), so that both frameworks can be used together, with three parts:

- The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk.
    - The Privacy Framework's Core Functions are:
        - Identify-P: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
        - Govern-P: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
        - Control-P: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
        - Communicate-P: Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.
        - Protect-P: Develop and implement appropriate data processing safeguards.
- **Profiles** are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.
- **Implementation Tiers** help an organization communicate about whether it has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile.

Laying the Groundwork for the Future

The companion Roadmap for Advancing the NIST Privacy Framework supports continued collaboration between NIST and stakeholders on priority areas that pose challenges to organizations in achieving their privacy objectives. These evolving areas, which require continued focus to advance privacy risk management and the evolution of the Privacy Framework, include:

- Privacy Risk Assessment
- Mechanisms to Provide Confidence
- Emerging Technologies
- De-Identification Techniques and Re-identification Risks
- Inventory and Mapping

- Technical Standards
- Privacy Workforce
- International and Regulatory Aspects, Impacts and Alignment

Additional Resources

- NIST Privacy Framework
- NIST Cybersecurity Framework
- NIST Privacy Engineering Program

ITL Bulletin Publisher: Katherine Green
Information Technology Laboratory
National Institute of Standards and Technology
katherine.green@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.