NIST releases version 1.0 of Privacy Framework

Tool will help optimize beneficial uses of data while protecting individual privacy.

January 16, 2020

Our data-driven society has a tricky balancing act to perform: building innovative products and services that use personal data while still protecting people's privacy. To help organizations keep this balance, the National Institute of Standards and Technology (NIST) is offering a new tool for managing privacy risk.

The agency has just released Version 1.0 of the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.* Developed from a draft version in collaboration with a range of stakeholders, the framework provides a useful set of privacy protection strategies for organizations that wish to improve their approach to using and protecting personal data. The publication also provides clarification about privacy risk management concepts and the relationship between the Privacy Framework and NIST's Cybersecurity Framework.

"Privacy is more important than ever in today's digital age," said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan. "The strong support the Privacy Framework's development has already received demonstrates the critical need for tools to help organizations build products and services providing real value, while protecting people's privacy."

Personal data includes information about specific individuals, such as their addresses or Social Security numbers, that a company might gather and use in the normal course of business. Because this data can be used to identify the people who provide it, an organization must frequently take action to ensure it is not misused in a way that could embarrass, endanger or compromise the customers.

The NIST Privacy Framework is not a law or regulation, but rather a voluntary tool that can help organizations manage privacy risk arising from their products and services, as well as demonstrate compliance with laws that may affect them, such as the California Consumer Privacy Act and the European Union's General Data Protection Regulation. It helps organizations identify the privacy outcomes they want to achieve and then prioritize the actions needed to do so.

"What you'll find in the framework are building blocks that can help you achieve your privacy goals, which may include laws your organization needs to follow," said Naomi Lefkovitz, a senior privacy policy adviser at NIST and leader of the framework effort. "If you want to consider how to increase customer trust through more privacy-protective products or services, the framework can help you do

that. But we designed it to be agnostic to any law, so it can assist you no matter what your goals are."

Privacy as a basic right in the USA has roots in the U.S. Constitution, but its application in the digital age is still evolving, in part because technology itself is changing at a rapidly accelerating pace. New uses for data pop up regularly, especially in the context of the internet of things and artificial intelligence, which together promise to gather and analyze patterns in the real world that previously have gone unrecognized. With these opportunities come new risks.

"A class of personal data that we consider to be of low value today may have a whole new use in a couple of years," Lefkovitz said, "or you might have two classes of data that are not sensitive on their own, but if you put them together they suddenly may become sensitive as a unit. That's why you need a framework for privacy risk management, not just a checklist of tasks: You need an approach that allows you to continually reevaluate and adjust to new risks."

The Privacy Framework 1.0 has an overarching structure modeled on that of the widely used NIST Cybersecurity Framework, and the two frameworks are designed to be complementary and also updated over time. Privacy and security are related but distinct concepts, Lefkovitz said, and merely adopting a good security posture does not necessarily mean that an organization is addressing all its privacy needs.

As with its draft version, the Privacy Framework centers on three sections: the *Core,* which offers a set of privacy protection activities; the *Profiles,* which help determine which of the activities in the Core an organization should pursue to reach its goals most effectively, and the *Implementation Tiers,* which help optimize the resources dedicated to managing privacy risk.

The NIST authors plan to continue building on their work to benefit the framework's users. Digital privacy risk management is a comparatively new concept, and Lefkovitz said they received many requests for clarification about the nature of privacy risk, as well as for additional supporting resources.

"People continue to yearn for more guidance on how to do privacy risk management," she said. "We have released a companion roadmap for the framework to point the way toward more research to address current privacy challenges, and we are building a repository of guidance resources to support implementation of the framework. We hope the community of users will contribute to it to advance privacy for the good of all."

Information technology and **Privacy**

MEDIA CONTACT

- **Chad Boutin**

  charles.boutin@nist.gov

  (301) 975-4261

ORGANIZATIONS

Information Technology Laboratory

Applied Cybersecurity Division

Cybersecurity and Privacy Applications Group

RELATED LINKS

NIST Privacy Framework

SIGN UP FOR UPDATES FROM NIST

Released January 16, 2020