wiley

ALERT

Privacy Activity in the Federal Government Ramps Up Dramatically

September 25, 2018

Federal policymakers have been grappling with many aspects of privacy these days, and this week has already seen two major developments: today's release of privacy principles by the National Telecommunications and Information Administration (NTIA), and yesterday's roll out of a Privacy Framework process by the National Institute of Standards and Technology (NIST). Both long-awaited developments mark a more aggressive foray by the federal government into privacy, and present private industry a critical opportunity to shape the direction of federal law on these important issues. Notably, all of these efforts are coming at the same time the Federal Trade Commission (FTC) is conducting hearings on privacy and related issues.

NTIA releases privacy principles that will shape national policy, regulation, and legislation.

After numerous meetings with stakeholders across the economy, NTIA has released a Request for Comment (RFC) entitled *Developing the Administration's Approach to Consumer Privacy*. It is taking comment on the document until **October 26**. It lays out core principles or "outcomes" that the Trump Administration suggests may be bedrocks for federal policies:

1. Organizations should be **transparent** about how they collect, use, share, and store users' personal information.
2. Users should be able to exercise **control** over the personal information they provide to organizations.
3. The collection, use, storage and sharing of personal data should be **reasonably minimized** in a manner proportional to

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

Telecom, Media & Technology

the scope of privacy risks.

4. Organizations should employ **security** safeguards to protect the data that they collect, store, use, or share.
5. Users should be able to reasonably **access and correct** personal data they have provided.
6. Organizations should take steps to **manage the risk** of disclosure or harmful uses of personal data.
7. Organizations should be **accountable** for the use of personal data that has been collected, maintained or used by its systems.

In addition to the privacy outcomes, the RFC sets forth several high-level goals for federal action, including:

1. Harmonize the regulatory landscape.
2. Legal clarity while maintaining the flexibility to innovate.
3. Comprehensive application.
4. Employ a risk and outcome-based approach.
5. Incentivize privacy research.
6. FTC enforcement.
7. Scalability.

This initiative comes at a time when the private sector confronts burgeoning global privacy demands, and state regulatory efforts, as in California. The Administration is looking to collect input to chart a productive path forward.

NIST has kicked off a Privacy Framework effort that aims to develop best practices and risk management tools for government and the private sector.

Claiming to model its activity on its lauded Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), NIST has officially launched its Privacy Framework project. This project is intended to yield a voluntary framework, informed through collaboration with the public and private sectors, to help all 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."

NIST officially announced this effort on September 4. At yesterday's NIST Privacy Framework event, NIST officials laid out their plans for the development of the new Framework. The first stakeholder workshop in the effort will be held on **October 16** in Austin, Texas, and NIST is planning webinar Q&A on the new Privacy Framework in **November**.

As described at yesterday's event, NTIA and NIST are attempting to harmonize the two privacy efforts. While NTIA's process will focus on *what* the privacy principles and policies should be, the NIST product is meant to be an implementation tool.

NIST has other privacy efforts underway, including those focused on the Internet of Things (IoT).

Just today, NIST also released Draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. This document is meant to aid federal agencies and other organizations to understand and manage the privacy and cybersecurity risks associated with IoT devices. In the draft, NIST proposes a set of 15 baseline capabilities for IoT devices to mitigate cyber and privacy risks. The draft currently maps to NIST's Cybersecurity Framework, as well as its security and privacy controls already established in NIST Special Publication 800-53, which itself is in the process of being updated. Comments on NIST's draft IoT guidance are due **October 24**.

***

The privacy and security team at Wiley Rein has already been actively involved in all of these activities and has worked with NTIA and NIST for years. We are helping clients inform federal policy and comment on these many initiatives. For more information about how these efforts may affect you or how to get involved, please contact our team.