Published on *The National Law Review* https://natlawreview.com

NIST Begins Developing a Voluntary Online Privacy Framework

Article By:

Inside Privacy Blog at Covington and Burling

The Department of Commerce's National Institute of Standards and Technology ("NIST") announced in early September intention to create a Privacy Framework. This Privacy Framework would provide voluntary guidelines that assist organizations in managing privacy risks. The NIST announcement recognized that the Privacy Framework is timely because disruptive technologies, such as artificial intelligence and the internet of things, not only enhance convenience, growth, and productivity, but also require more complex networking environments and massive amounts of data.

Building on the success of the NIST Cybersecurity Framework, the Privacy Framework is meant to be a transparent, enterprise-level tool that helps organizations prioritize resources and strategies in order to create flexible, risk-based privacy solutions. Deliberations between industry, civil society groups, academic institutions, federal, state, and local government entities, standard-setting organizations, and others kicked off with a workshop in Austin, Texas on October 16th, which set the stage by examining how organizations currently manage privacy risks, identifying where the challenges lie, and determining how the Privacy Framework can help organizations meet such challenges.

Shortly thereafter, on October 29, 2018, NIST Senior Privacy Policy Advisor Naomi Lefkovitz discussed the future of the Privacy Framework with a group convened by the American Bar Association's Section of Science & Technology Law's E-Privacy Committee. During the discussion, Ms. Lefkovitz emphasized why a Privacy Framework is needed in addition to NIST's existing, cyber-related frameworks. Although good cybersecurity practices can help manage privacy risks by protecting people's information, privacy risks also can arise from organizations' authorized collection, storage, use, and sharing of information to meet their mission or business objectives. If not effectively managed and communicated, privacy risks can have both individual and industry-wide consequences (such as failure to achieve societal acceptance of an otherwise useful technology due to lack of trust in the marketplace).

Ms. Lefkovitz stressed the benefits of the NIST Privacy Framework as it is currently imagined, including:

- **Risk-Based, Outcome-Based Approach:** The NIST Privacy Framework incorporates a risk-

based model that encourages self-evaluation by organizations. Specifically, the Framework is meant to enable organizations to determine what programs and protocols are appropriate for the organization based on the type, nature, and quantity of data collected. In addition, because the model is framed around outcomes, rather than as a set of prescriptive requirements or a “check-the-box” exercise, the Privacy Framework will be more effective because it will be more tailored to the organization’s extent and scope of data collection, storage, use, and sharing

- **Avoids the Pitfalls of the GDPR:** Ms. Lefkovitz noted that the Privacy Framework sidesteps some of what she believes to be major pitfalls of the GDPR. For example, Ms. Lefkovitz believes that the GDPR inappropriately buckets activities and roles into separate categories (specifically, “processors” and “controllers”). Ms. Lefkovitz explained that such distinctions are not pragmatic in the age of disruptive technologies, which often blurs the roles played by various data stakeholders. Unlike the GDPR, the Privacy Framework does not bucket activities or roles, but instead asks organizations to think through the type of data they collect and use, the risks involved with the data, and how to mitigate those risks through organizational controls.
- **May Reduce Compliance Burdens:** The Privacy Framework emphasizes predictability, manageability, and disassociability in a way that allows businesses of all sizes and scales to adopt relevant and appropriate controls for their data practices. Although this reduces some of the burden of scaling a risk management program for a smaller organization, Ms. Lefkovitz acknowledged that the model still requires a baseline level of risk management expertise in an organization to build and manage a program.

As an initial step, NIST is considering how it should structure the Framework in order to achieve its proposed minimum attributes, which include being consensus-driven, adaptable, non-prescriptive, and compatible with other privacy approaches. Ms. Lefkovitz explained that the Framework may be structured around the information life cycle, objectives (such as compliance with applicable laws, or with the NIST privacy engineering objectives of predictability, manageability, and disassociability), principles such as the fair information practices principles (FIPPs), or a combination of sources. In addition, NIST has asked stakeholders to consider whether certain, broadly applicable privacy practices should be included (such as de-identification, enabling user preferences, and providing users with a reliable understanding of how their information is being collected, stored, used, and shared).

NIST plans to use the input provided at the October 16th workshop to draft an annotated outline of the Privacy Framework, and is scheduled to host a Q&A-based webinar on the Framework on November 29th. At the same time, the Department of Commerce’s National Telecommunications and Information Administration has put out a request for comment regarding its proposed federal consumer privacy framework that is meant to protect innovation. Comments are due November 9, 2018.

National Law Review, Volume VIII, Number 306