wiley

NEWSLETTER

February Was a Big Month in Privacy: Here's What You Need to Know

March 2019

Privacy in Focus®

February was a busy month in privacy – from the federal government to the states, from legislatures to agencies, various governmental authorities have been hard at work on a diverse array of potential privacy approaches. Here is a quick overview of the action and some key takeaways:

U.S. Congress

House of Representatives

On February 26, the House Subcommittee on Consumer Protection and Commerce of the Committee on Energy and Commerce held its first hearing of the 116th Congress to discuss the merits of federal data privacy legislation.

On the surface, there were two broad bipartisan themes: (1) concern over how businesses use consumer data; and (2) support for a federal privacy bill. But despite this principal overlap, there was considerable breakdown on partisan lines. Republicans were generally more concerned with creating a single, federal standard, and also raised the risk that overly prescriptive regulations would adversely affect small businesses. Democrats were more concerned with creating enforceable consumer rights and reducing the burden on consumers to navigate complex privacy policies.

Senate

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

FTC Regulation

Privacy, Cyber & Data Governance

On February 27, the Senate Committee on Commerce, Science, and Transportation held its own hearing on privacy policy principles.

This hearing signaled bipartisan consensus that it is time for comprehensive federal privacy legislation and that the Federal Trade Commission (FTC) should be its primary enforcer. However, there were still notable partisan divisions. The split over preemption was more obvious than in the House, with Chairman Roger Wicker (R-MS) explicitly endorsing preemption and Ranking Member Maria Cantwell (D-WA) suggesting that preemption may be unnecessary. Additionally, Democrats generally inquired about specific privacy protections, whereas Republicans tended to focus on broad transparency principles.

NIST

The National Institute of Standards and Technology (NIST) is also focusing on privacy and is working to draft a Privacy Framework. On February 27, NIST released an analysis of the nearly 80 responses it received responding to its November request for information (RFI). And on the same day, NIST also released a Privacy Framework Working Outline – addressing some of the comments from the RFI responses – "for discussion purposes to promote input on the NIST Privacy Framework: An Enterprise Risk Management Tool."

In the analysis of the RFI responses, NIST noted that there was broad support for its development of the framework. Additionally, NIST found that commenters generally favored, *inter alia*:

- Regulatory compatibility: "the Framework should support organizations' ability to comply with a large range of legal responsibilities, including U.S. state and federal sector-specific laws and regulations and international regimes …";
- The basic NIST Framework attributes, including "common and accessible language, that it be adaptable, risk-based, outcome-based, technology-agnostic, non-prescriptive, and readily usable as part of an enterprise's broader risk management processes …"; and
- Inclusivity of emerging technologies, such as Internet of Things (IoT) and artificial intelligence.

In the Privacy Framework Working Outline, NIST explains that the Privacy Framework will, at a high level, be aligned with the Cybersecurity Framework. It will provide a "Privacy Framework Core" made up of functions, categories, subcategories, and informative references that will "present key privacy outcomes identified by stakeholders as helpful in managing privacy risk." The functions – which organize high-level data privacy activities related to data processing – are (1) identify; (2) protect; (3) control; (4) inform; and (5) respond.

The Outline also discusses the "Privacy Framework Profile," which is the "alignment of [the Privacy Framework Core] with the business requirements, risk tolerance, privacy objectives, and resources of the organization" and four "Privacy Framework Implementation Tiers," that "provide context on how an organization views privacy risk and the processes in place to manage that risk." The Profile and Tiers are intended to allow for risk management and flexibility, by helping an organization identify which functions, categories, and subcategories of the Privacy Framework are appropriate for its organizational needs.

NIST is hosting a series of workshops on the development of this Framework, with the next workshop scheduled for May 13-14 in Atlanta.

NTIA

On February 26, David J. Redl, the Assistant Secretary of Commerce for Communications and Information, gave remarks on privacy at the Mobile World Congress Ministerial Programme. In it, he outlined the National Telecommunications and Information Administration's (NTIA) thinking on privacy.

Broadly speaking, Secretary Redl noted the desire to create global interoperability but stressed that his goal was to create "a fundamentally American approach to privacy, built on the same bedrock principles that so many nations share." He also stressed "a sense of urgency and a desire for American leadership" on privacy.

In terms of specifics, he supported a preemptive, risk- and outcome-based approach, stating that:

- There is broad industry consensus on both domestic and global interoperability and correspondingly opposition to "a patchwork regulatory landscape within the U.S."
- "[F]ocusing on risks and outcomes is preferred to notice-and-consent approaches." He argued that a risk- and outcome-based focus was best because it does not create a check-the-box mindset or entrench large businesses at the expense of startups and small firms.

Lastly, he argued that privacy is bound up with cybersecurity, saying "you cannot have true privacy without secure network technology. We're ready to work together to ensure that our technology infrastructure is secure."

FTC

Also in February, the FTC rescheduled its privacy hearing, which had been postponed due to the government shutdown earlier this year. The hearing – which is part of the FTC's larger series of hearings on Competition and Consumer Protection in the 21st Century – is now scheduled for April 9-10. Explaining that its current and long-standing approach to privacy "needs to be examined in light of potential gaps in the Commission's existing authority, as well as new risks, new opportunities, and new knowledge," the FTC has posed a series of questions for public input, including:

- What are the actual and potential benefits for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these benefits?
- What are the actual and potential risks for consumers and to competition of information collection, sharing, aggregation, and use? To what extent do consumers today, or are consumers likely to, realize these risks?
- Should privacy protections depend on the sensitivity of data? If so, what data is sensitive and why? What data is not sensitive and why not?

- Should privacy protection depend on, or allow for, consumer variation in privacy preferences? Why or why not? What are the appropriate tradeoffs to consider? If desired, how should this flexibility be implemented?
- What are existing and emerging legal frameworks for privacy protection? What are the benefits and drawbacks of each framework?
- What are the tradeoffs between ex ante regulatory and ex post enforcement approaches to privacy protection?

Comments will be due on May 31.

California Consumer Privacy Act

On February 20, the California State Assembly held a legislative hearing on the California Consumer Privacy Act (CCPA). Many at the hearing raised concerns about the law, largely centered around the short turnaround for implementation, the potential negative economic impact of the law, and how the private right of action should function.

Relatedly, several bills have been introduced in California to amend or clarify the CCPA, including California Senator Hannah-Beth Jackson's SB 561 that is supported by the California Attorney General and would expand the law's private right of action, among other changes.

Lastly, the California Attorney General is in the preliminary stages of a rulemaking to create "procedures to facilitate consumers' rights under the CCPA and ... guidance to businesses for how to comply."

Comments were due March 8.

© 2019 Wiley Rein LLP

**Wiley Rein Law Clerk Boyd Garriott contributed to this article.*