wiley

ARTICLE

President's Controversial *Consumer Privacy Bill of Rights Act* Informs Federal Privacy Dialogue, but is Unlikely to Pass

March 2, 2015

On February 27th, the Obama Administration released the discussion draft of a "Consumer Privacy Bill of Rights Act," a legislative proposal that seeks to create a comprehensive framework for national consumer privacy. The proposal, first announced by President Obama during a January speech at the Federal Trade Commission (FTC), is part of the Administration's larger effort this year to focus on combating cyber threats while safeguarding consumer privacy and civil liberties. The bill is almost certainly a non-starter, critiqued already by all sides in the privacy debate. Less a serious legislative proposal, it is a vehicle to advance policy discussions in a time of widespread concern over data and cyber security.

The Bill Would Set Up a Complicated New Privacy Regime

The Consumer Privacy Bill of Rights Act expands upon a set of principles outlined by President Obama in 2012. The bill is an assortment of aspirational goals for the collection and handling of personal data. It sets expectations for a broad swath of "covered entities" to provide notice about the companies' collection and use of "personal data," as well as options for consumers to control their personal data. The bill defines personal data to include, among other things, names, email addresses, credit and debit card numbers, and biometric identifiers. "Covered entities" are those that collect, process, use or disclose personal data, subject to certain exceptions, including those that process personal data of fewer than 10,000 individuals or devices during any 12-month period or have 5 or fewer employees. The bill provides start-up companies with an 18-month exemption from its requirements.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Shawn H. Chang
Partner
202.719.4456
schang@wiley.law

Scott D. Delacourt
Partner
202.719.7459
sdelacourt@wiley.law

Practice Areas

Health Care
Internet of Things
Privacy, Cyber & Data Governance
Public Policy

The bill demands transparency, notice, and reasonable means for individuals to control their personal data. The bill requires clear disclosures about entities' privacy and security practices, including what data is collected and how it is used and secured. The bill mandates "reasonable" collection, retention, and use of personal data, determined by reference to a multi-factor assessment of relevant "context" considerations. In so doing, the President's bill sets substantive expectations for the security of personal data, including obligations to identify and protect against "foreseeable" risks. The bill also requires that individuals have options to assure the accuracy of personal data held by a covered entity.

In terms of compliance, a central feature of the bill is a novel "safe harbor" approach, in which covered entities would create their own "codes of conduct" for the collection, use and handling of personal data, supervised by Privacy Review Boards approved by the FTC. These codes would be subject to FTC review and a multi-stakeholder process convened by the Department of Commerce. If an approved code of conduct is complied with, it would be a defense to suits based on covered practices. The complex regime for the creation of these codes has been criticized as convoluted and impractical.

In terms of enforcement, the bill contemplates broad powers by the FTC under Section 5 of the Federal Trade Commission Act, and more limited action by state Attorneys General. It would limit civil penalties sought by the FTC to no more than $25,000,000.

The draft bill wades into some controversial territory. The President proposes giving the FTC rulemaking authority to set requirements for the safe harbor and approval of Privacy Review Boards. And the bill takes a position on preemption, narrowly preempting application to covered entities of state laws related to "data processing," while preserving state consumer protection laws and various laws, including those related to data breach notice, to the extent that claims are not based on a failure to comply with Consumer Privacy Bill of Rights Act of 2015.

While this bill, on its own, faces an uphill battle, it raises significant questions that will be addressed as debate continues in Congress. Some of the more noteworthy questions to watch going forward include:

- Preemption - will state law on privacy be preempted - and will the existing exception from preemption for state laws dealing with health and financial information remain?
- Overlaps with federal law - the bill essentially carves out entities and practices regulated by a wide variety of federal laws. Will these carve-outs remain - essentially continuing today's fragmented privacy environment?
- Will this proposal have any meaningful impact on industries heavily regulated for privacy today - primarily health care and financial services, along with communications?
- Will "enforceable codes of conduct" remain a part of the future of privacy regulation?
- Will de-identification provisions remain in the bill and provide appropriate support for useful means of de-identifying personal data for substantial public and private benefits?

- Will a resulting bill exempt (essentially) all government activities and the activities of government contractors?
- How will the idea of "context" evolve, and is this a viable means of defining appropriate behavior?
- Will Privacy Review Boards become an important element of a privacy regulatory regime?
- How will the mechanism for potential penalties evolve?
- Will the states and the federal government be able to agree on allocations of enforcement authority - or will everyone enforce everything?

Reaction is Highly Skeptical, but the Bill Could Influence Discussion About Privacy

On Capitol Hill, the draft bill was met with skepticism from both Congressional Republicans and Democrats. In a statement, House Energy and Commerce Committee Chairman Fred Upton (R-MI) and Commerce, Manufacturing, and Trade Subcommittee Chairman Michael Burgess (R-TX) stated that there are "some interesting elements included in the president's proposal, but we must tread carefully." The Committee's Democrats were more blunt, with Ranking Members Frank Pallone (D-NJ) and Janice Schakowsky (D-IL) calling a number of the bill's provisions "deeply problematic." They lamented that members and staff of the Committee with expertise in privacy policy were not permitted to participate in the drafting. In the Senate, Senator Ed Markey (D-MA), one of the most vocal voices in Congress on privacy issues, refused to back the draft bill and instead announced his intention to introduce his own bill to regulate data brokers.

In modeling the legislation after the 2012 Consumer Privacy Bill of Rights framework that went nowhere, the Administration understood its slim chances for passage. But the draft legislation is having its intended effect- spurring discussions about a comprehensive federal privacy regime. Such a regime is relevant because of several privacy and security initiatives under consideration. The White House earlier proposed a set of new cyber security and consumer protection measures and has helped generate momentum for some legislative action on Capitol Hill. For example, privacy and security bills aim to protect student data, strengthen public-private cyber information sharing, reform how data brokers collect and sell consumer information, and enhance data breach notification are all slated to be introduced later this year. In addition, several bills reforming the Electronic Communications Privacy Act have already been re-introduced this Congress.

In addition to spurring legislative activities on privacy and cyber security, the President's proposal could provide political cover for Members of Congress, especially Democrats, to endorse proposals earlier criticized by privacy advocates. For example, as highlighted by Ranking Member Pallone and Congressman Mike Doyle (D-PA) during a recent net neutrality hearing, a prior version of the President's draft would have consolidated the FCC and FTC's overlapping privacy jurisdiction over common carriers and cable providers. While that provision was removed, it is now known that the White House contemplated stripping the FCC of its privacy authority in favor of a FTC-only enforcement model. Furthermore, the final draft bill retains provisions generally unpopular with privacy groups, including preemption and limited penalties. Should such provisions emerge in other legislative vehicles, some lawmakers may be more inclined to offer their support, now that the President has endorsed them in principle.

Conclusion

Risks exposed by data breaches and cyberattacks have increased concern for consumer privacy and interest in uniform federal approaches. Legislation on cyber and data security has raised the profile of privacy issues. While Congress considers its options, federal efforts related to privacy and data security continue. This includes high-profile FTC enforcement proceedings examination of privacy and security throughout the economy, including the "Internet of Things." Technical efforts are underway at the National Institute of Standards and Technology on privacy engineering and other issues. And the National Telecommunications and Information Administration has been examining "big data" and the privacy implications of business practices.

In the context of ongoing discussions of privacy and security, the President's bill lays down aggressive and novel markers about consumer protection, and highlights many areas for future consideration. This proposal will not become law, but it is part of ongoing efforts on privacy across the federal government, aspects of which could impact the private sector.