Policy and Regulation Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Lawmakers Unveil Landmark Bipartisan Privacy Proposal

June 6, 2022

Key Points

- Three of the four bipartisan leaders of the House and Senate committees with jurisdiction over data privacy have struck a deal on a comprehensive federal bill, the American Data Privacy and Protection Act, marking the first such proposal to gain bipartisan, bicameral support.
- After years of disagreement on the correct approach to preemption and private right of action, and more recently arbitration, the three committee leaders have offered a compromise that may increase the likelihood of the legislation's success.
- The House Subcommittee on Consumer Protection and Commerce could hold a hearing on the bill as soon as June 14, followed by a subcommittee markup and a full committee markup, with the goal of having these items completed by August.
- However, despite significant progress made in negotiations, moving the legislation before the 2022 midterm elections remains a heavy lift, particularly without Chair Cantwell's support.

Introduction

On Friday, June 3, Energy and Commerce (E&C) Committee Chair Frank Pallone (D-NJ) and Ranking Member Cathy McMorris Rodgers (R-WA), along with Senate Commerce Committee Ranking Member Roger Wicker (R-MS), released a discussion draft of a comprehensive national data privacy and security framework—dubbed the American Data Privacy and Protection Act—marking the first comprehensive privacy proposal to gain bipartisan, bicameral support.

The bill is the product of years of negotiation, beginning in 2019 with the formal introduction of competing proposals in the Senate by Commerce Chair Maria Cantwell (D-WA) and Ranking Member Wicker (see prior alert here), and followed by the release of a bipartisan discussion draft in the House by E&C Committee staff. However, this draft did not contain legislative language on controversial provisions such as preemption and a private right of action, leaving the areas in brackets for stakeholder input, and bipartisan discussions tapered off with little progress, with House Republicans unveiling their own draft in 2021—the Control Our Data Act.

Contact Information

If you have any questions concerning this alert, please contact:

G. Hunter Bates
Partner
hbates@akingump.com
Washington, D.C.
+1 202.887.4147

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Ed Pagano
Partner
epagano@akingump.com
Washington, D.C.
+1 202.887.4255

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jennifer L. Richter
Partner
jrichter@akingump.com
Washington, D.C.
+1 202.887.4524

Arshi Siddiqui
Partner
asiddiqui@akingump.com
Washington, D.C.
+1 202.887.4075

James Romney Tucker Jr.
Partner
jtucker@akingump.com
Washington, D.C.
+1 202.887.4279

While Chair Cantwell does not currently support the new bipartisan proposal as a result of her preference for prohibiting covered entities from forcing their users into arbitration, in addition to her objection to the four-year delay in effect of the private right of action, she has begun to circulate a revised version of her privacy bill first unveiled in 2019—the Consumer Online Privacy Rights Act (S. 3195) to address this concern. However, the bill still contains a number of other key differences with the American Data Privacy and Protection Act, and it is unclear whether she will ultimately back this new agreement.

Key Provisions

As previously noted, the American Data Privacy and Protection Act strikes a compromise with regard to the longstanding sticking points of preemption and a private right of action, in addition to the issue of arbitration. The bill would generally preempt state privacy laws, although the language does provide for some exceptions, including with regard to the California Consumer Privacy Act's Section 150 (private right of action) and state laws relating to acts of fraud, unauthorized access to personal information or notification of unauthorized access to personal information. The preemption language would also carve out state trespass, contract or tort law. While the bill recognizes compliance with other federal statutes such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA) for purposes of the Act's privacy and data security requirements, other provisions such as executive certification would still be applicable.

The legislation would allow for enforcement by the Federal Trade Commission (FTC) and state attorneys general, also providing for a limited private right of action. Beginning four years after the date of enactment, individuals may generally bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief and reasonable attorney's fees and litigation costs. Individuals intending to bring such an action must provide 60 days' notice to the FTC and the attorney general in the state(s) where individuals are resident, and those agencies would then have 60 days to determine if they wish to independently take action. The measure also includes a 45-day right to cure.

The deal would also prohibit covered entities from enforcing pre-dispute arbitration agreements or joint action waivers with respect to minors, and pre-dispute joint action waivers for arbitration or administrative proceedings would also be precluded regardless of age. The bill would cover any entity that collects, processes or transfers covered data and is subject to the jurisdiction of the FTC, including nonprofits and telecommunications common carriers.

"Covered data" is defined as information identifying, linked or reasonably linkable to an individual or device linkable to an individual, carving out de-identified data, employee data or publicly available information. "Sensitive covered data" is defined to include the following:

- Information related to individuals under 17.
- Government-issued identifiers not required to be displayed in public such as social security and passport numbers; past, present and future health, diagnosis, disability or treatment information; financial account, debit card and credit card numbers along with any access code, password or credentials.
- Biometric information.

Francine E. Friedman
Senior Policy Counsel
ffriedman@akingump.com
Washington, D.C.
+1 202.887.4143

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Galen A. Roehl
Senior Policy Advisor
groehl@akingump.com
Washington, D.C.
+1 202.887.4224

Christopher A. Treanor
Counsel
ctreanor@akingump.com
Washington, D.C.
+1 202.887.4551

Taylor Daly
Policy Advisor
tdaly@akingump.com
Washington, D.C.
+1 202.416.5541

- Genetic information.
- Past or present precise geolocation information.
- Private communications such as voicemail, email, text or information identifying parties to communications.
- Any account or device log-in credentials.
- Information revealing race, ethnicity, national origin, religion, union membership status, sexual orientation or sexual behavior that violates an individual's reasonable expectations on disclosure.
- Information revealing online activities over time and across third party online services.
- Calendar, address book, phone, text, photos, audio and video recordings maintained for private use on a device.
- Photos or videos of naked or undergarment-clad private areas.
- Information revealing individuals access to or viewing of TV, cable or streaming media services.

Rather than solely relying on a "notice and consent" regime, and in an aim to avoiding placing the burden for privacy on the consumer, the bill utilizes "duty of loyalty" provisions, barring covered entities from collecting, processing or transferring covered data beyond what is reasonably necessary, proportionate and limited to provide specific products and services.

The measure establishes several user rights, including rights to access, correction, deletion and portability, as well as the right to opt out of the transfer of any covered data to a third party. Further, the bill stipulates that sensitive covered data may not be collected, processed or transferred to a third party without the express affirmative consent of the individual. Regarding targeted advertising, covered entities must also provide individuals with clear and conspicuous means to opt out.

Further, the bill imposes additional requirements and responsibilities on "large data holders," which are defined to include covered entities with gross revenues above $250 million that collected, processed or transferred covered data of over five million individuals or devices, or the sensitive covered data of 100,000 individuals or devices, in the most recent calendar year. These entities must provide short-form notices of their covered data practices, in addition to assessing their algorithms annually and submit annual algorithmic impact assessments to the FTC. Such entities would also be subject to additional corporate accountability requirements, including annually certifying that the company maintains reasonable internal controls and reporting structures for compliance with the Act.

With regard to data security, the legislation requires covered entities to implement and maintain data security practices and procedures that protect and secure covered data against unauthorized use and acquisition. In determining whether such protections are reasonable, factors such as the entity's size, complexity and activities related to covered data would be taken into consideration.

The American Data Privacy and Protection Act provides a carve out for certain small and medium-sized covered entities that, for the prior three years, (1) earned gross

annual revenues of $41 million or less, (2) did not collect or process the covered data of 100,000 individuals in a year, except for processing payments and (3) did not derive more than half their revenue from transferring covered data. These entities would be exempt from the Act's data portability requirements and most of the data security requirements, and they may also choose to delete, rather than correct, an individual's covered data upon receiving such a verified request.

The legislation would treat violations of the Act as violations of a rule defining an unfair or deceptive act or practice under the FTC Act, allowing the agency to obtain civil penalties for initial and subsequent violations. Within one year of enactment, the bill directs the FTC to establish a new bureau to carry out its authority under the Act that is comparable the current Bureaus of Consumer Protection and Competition. The measure also requires the creation of a Youth Privacy and Marketing Division at the FTC, which is directed to submit annual reports to Congress and hire staff that includes children's privacy experts.

Outlook

The E&C Subcommittee on Consumer Protection and Commerce could hold a hearing on the bill as soon as June 14, followed by a subcommittee markup and a full committee markup, with the goal of having these items completed by August.

Despite progress made in negotiations, the legislation remains difficult to move before the approaching 2022 midterm elections as Congress faces competing priorities of inflation, China competitiveness legislation and ongoing discussions of a new reconciliation package. However, Chair Cantwell's support for the legislation could help garner the momentum needed for the bill to gain traction this summer.

akingump.com