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

Congress Proposes Federal Privacy Legislation to Preempt Certain State Privacy Laws, Hearing Scheduled for Next Week

Article By:

Kristin L. Bryan

Shea Leitch

On Friday, three of the four leaders of the Congressional committees with principal jurisdiction over privacy provided for review draft privacy legislation (the American Data Privacy and Protection Act) that if adopted would preempt certain recently-passed state privacy laws. The bill, sponsored by House Energy and Commerce Chair Frank Pallone (D-N.J.), ranking member Cathy McMorris Rodgers (R-Wash.), and Sen. Roger Wicker (R-Miss.), ranking member of the Senate Commerce Committee, shares features of California's privacy legislation, as well as the GDPR. However, the legislation departs from these existing laws in important ways. In this post, we analyze some of the most important features of the legislation from both a compliance and litigation risk perspective, as what is on the horizon going forward.

Background

There were a number of privacy bills introduced in the House and Senate in 2021-2022. As one recent example, in February the Algorithmic Accountability Act of 2022 was introduced in the U.S. Senate by Sen. Rob Wyden to direct the Federal Trade Commission ("FTC") to promulgate regulations that require any "covered entity" to perform impact assessments and meet other requirements regarding automated decision-making processes. The bill would have required the promulgation of regulations on automated decision-making processes that implicate an "augmented critical decision process" – essentially, that result in any legal or other material effects – on a consumer.

Data privacy has also been a top-of-mind issue at the state level, with comprehensive privacy laws recently enacted in California, Colorado, Connecticut, Virginia, and Utah. Over 100 privacy bills were introduced in state legislatures in 2022 alone. This wave of activity included other states seeking to adopt broad privacy regimes (such as Florida's twice failed efforts) while others focused on privacy bills that were narrowly tailored to specific areas such as biometric privacy, AI, and facial recognition. This proliferation of state laws and their diverging regulatory requirements has led to increasing calls for the passage of a federal privacy law. A uniform federal law, if enacted, would provide business interests much-needed clarity while also ideally stemming the tide of putative class actions and other data privacy claims brought under various state laws.

Compliance Requirements

If passed, the American Data Privacy and Protection Act (the "Act") would codify several privacy best practices into federal law. Under the draft, businesses would be required to limit the collection, processing, and transfer of "covered data" to that which is "reasonably necessary, proportionate, and limited to" provide products or services to the individual, communicate with the individual, or perform another purpose permitted by the legislation. Sec. 101(a).

Prohibited Practices

The Act would place an outright prohibition on certain data processing activities if very limited exceptions—like the consent of the individual, exigent circumstances, or a search warrant—are not satisfied. Under the Act, the following activities would be prohibited:

- Processing of Social Security numbers, except where necessary for the extension of credit, authentication of the individual, or payment and collection of taxes.

- Transferring precise geolocation information to a third party, except to another device or service of the individual, with the individual's affirmative express consent, "through a conspicuous notice explaining the manner in which the precise geolocation information will be transferred with such a notice provided for in each instance in which such transfer is to occur absent a search warrant or exigent circumstances."

- Collecting, processing, or transferring biometric information, "except for data security, authentication, to comply with a legal obligation, to exercise or defend a legal claim, for law enforcement purposes, or with the affirmative express consent of the individual through a standalone conspicuous notice explaining the manner in which the biometric information will be collected, processed, or transferred with such a notice provided for each instance in which such collection, processing, or transferring is to occur."

- Transferring passwords, except to a password manager, a covered entity whose job it is to identify passwords being re-used across sites or accounts, without a search warrant or exigent circumstances.

- Collection, processing, or transferring "known nonconsensual intimate images," (what is sometimes referred to as "revenge porn"), "except for law enforcement purposes."

- Transferring "an individual's aggregate internet search or browsing history, except with the affirmative express consent of the individual through a standalone conspicuous notice," like that described above for biometric or precise geolocation information.

- Transferring an individual's physical activity information from a smartphone or wearable device, other than to another device or service of that individual with the affirmative express consent of the individual," as described above.

Sec. 102(a).

Individual Rights

Like existing privacy laws, the Act would provide individuals rights like the right to access (in human and machine-readable, portable formats), correction (including for completeness), and deletion. Sec. 203(a). The Act also includes the right to opt-out of targeted advertising (Sec. 204(d)), and also requires covered entities to obtain consent before processing "sensitive covered data." Sec. 204(a). Notably, the Act construes "sensitive" broadly, including the following categories not previously included in other privacy laws:

1. Clickstream data.

2. "Calendar and address book information, phone or text logs, photos, audio recordings, or videos maintained for private use on an individual's device."

3. Photos and videos showing "the naked or undergarment-clad private area of an individual."

4. Television, cable, or streaming content viewing information.

5. Information regarding individuals under 17.

6. "Any other covered data collected, processed, or transferred for the purpose of identifying the" sensitive data types.

In a more novel turn, the Act also includes the right to opt-out of data transfers to third parties. Sec. 204(c).

Privacy by Design

If passed, the Act would mandate that covered entities develop and implement a privacy program that accounts for applicable Federal, State, or local laws, rules, or regulations, mitigation of privacy risks to children, reduction of privacy risks arising from the products or services of the covered entity, and training for employees and staff. Sec. 103(a).

Privacy Notices

Many of the Act's requirements for privacy policies under the draft legislation mirror other laws. Departing from existing privacy laws, the Act also requires the privacy policy to include "the name of each third-party collecting entity to which the covered entity transfers covered data, and the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities[.]" Sec. 202(b)(4). Additionally, "large data holders" would be obligated to provide a short-form notice that is, "concise, clear, and conspicuous," "readily accessible, based on the way an individual interacts with the large data holder," and include an overview of the individual rights provided under the legislation. Sec. 202(e).

Preemption

In a welcome move for many businesses, the Act would preempt most state privacy laws. It provides that "[n]o State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of the law of any State, or political subdivision of a State, covered by the provisions of this Act,

or a rule, regulation, or requirement promulgated under this Act."

However, the Act would not preempt various targeted state statutes, including "consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices", laws regarding the privacy rights of employees or students, data breach notification laws, the Illinois Biometric Information Privacy Act, the California Consumer Privacy Act (except its provisions concerning security breaches) and the California Privacy Rights Act, and laws governing facial recognition, unsolicited email, telephone solicitations, and caller ID, among other matters. In practice, this means that the Act if enacted would explicitly preempt the new comprehensive privacy legislation enacted by Connecticut, Virginia, Utah, and Colorado.

Private Right of Action

The Act also contains a complex private right of action that allows "any person or class of persons who suffers an injury" due to a violation of the bill that could be addressed by its civil remedies to file suit in federal court. The Act's civil remedies however are limited to compensatory damages, injunctive and/or declaratory relief, and reasonable attorney's fees and litigation costs. Additionally, presumably in an effort to give the business community time to adjust to any new regulatory requirements, the Act includes a four-year delay on the availability of the private right of action. The Act also prohibits mandatory arbitration clauses, albeit for minors only.

Path Forward

On June 7, it was announced that a hearing on the Act has been scheduled for Tuesday, June 14, at 10:30 a.m. (EDT). However, it remains to be seen whether Senator Cantwell, the Chair of the Senate Commerce Committee, will lend her support to the Act (and what the Act's path forward will look like if Senator Cantwell's endorsement is not forthcoming). Senator Cantwell had previously supported other privacy bills (including one in 2019 that included a private right of action and would have established a "duty of loyalty" for companies that handle consumer data).

National Law Review, Volume XII, Number 160