Bipartisan Push for Federal Privacy Legislation: Will It Work This Time?

Insights
6.13.22

After a stalemate over federal consumer privacy legislation in the past few years, a draft bill was released on June 3 that signals a major step towards bipartisan support for federal consumer privacy legislation. The American Data Privacy and Protection Act (ADPPA) includes two major points of contention: federal preemption of state privacy laws and a private right of action for consumers. (We previously discussed these issues here). Already, five states – California, Colorado, Connecticut, Utah, and Virginia – have enacted their own consumer privacy laws, and over a dozen other states are considering passing similar laws. Businesses that are subject to these laws will have to deal with a hodgepodge of different standards and regulations across state lines. The ADPPA may solve this problem by creating a national framework for consumer privacy. What do you need to know about consumer privacy laws and the ADPPA?

What Are Consumer Privacy Laws?

At their core, consumer privacy laws aim to achieve three objectives:

1. Ensuring that consumers (which in some jurisdictions include employees and job applicants) are informed about what data is being collected from or about them and how the data will be used or shared.
2. Providing consumers some level of control over how data collected from or about them is used, shared, sold, and retained. This includes, for example, requiring consumer consent for certain uses or selling of their data, and empowering consumers with certain rights, such as the right to know what data is collected about them, the right to request deletion of their data, the right to opt out of the sale of their data, the right to correct their data, and the right to limit use and disclosure of sensitive personal data.
3. Regulating how businesses collect, maintain, retain, use, share, and sell consumer data, and imposing penalties and consequences for businesses that violate those rules.

State consumer privacy laws can get complicated, but all the rules and regulations ultimately come down to one of these three objectives. These laws also include various exceptions, such as for Protected Health Information that is regulated under HIPAA. Some of these laws, like the California Consumer Privacy Act (CCPA), extend the same consumer rights to employees and job applicants, presenting unique and unprecedented challenges for human resources departments.

Private Right of Action

If enacted, the ADPPA would create a private right of action that would be available four years after the bill's enactment. This means that – in addition to the possibility of enforcement by a government agency – individual consumers can sue the business for violations of the law. A consumer or class of consumers that wants to sue a covered entity must submit written notification to their state's attorney general and the Federal Trade Commission (FTC), which will decide whether to independently pursue the action or allow the private citizens to file their own lawsuit. Additionally, pre-dispute arbitration agreements or joint action waivers with respect to minors that limit the private right of action or other rights under the ADPPA would be unenforceable.

Federal Preemption

In its current version, the ADPPA would preempt state laws with a number of exceptions. The proposal would not preempt Illinois' Biometric Information Privacy Act and Genetic Information Privacy Act, the California Consumer Privacy Act's private right of action for data breaches, and laws that "solely address facial recognition technologies," as well as general consumer protection laws such as those regulating unfair business practices.

Covered Entities Under the ADPPA

The proposal applies to all "covered entities," defined as any entity or person that collects, processes, or transfers covered data or that controls, is controlled by, under common control with, or shares common branding with another covered entity. This is a stark departure from the criteria in the CCPA and other state consumer privacy laws for covered entities, which has typically been a minimum revenue threshold, annual collection of data about a minimum number of the particular state's residents, or based on how much of the business's revenue is derived from selling personal data. Instead, the ADPPA would essentially apply to all businesses that interact with covered data.

That said, while the ADPPA may apply to most businesses, the requirements it would impose are significantly reduced for entities that fit certain criteria under what we're calling the "small business exception." Businesses fall under the ADPPA's small business exception if, for the prior three calendar years, they (i) did not exceed $41 million in average annual gross revenues, or (ii) did not collect or process covered data of more than 100,000 individuals on average annually, or (iii) did not derive more than 50% of their revenue from transferring covered data during any of the prior three calendar years. This would exempt the business from having to respond to any consumer request (such as a request to produce a copy of the consumer's data) and having to hire a data security officer or data privacy compliance officer, as well as from other requirements. The proposed bill leaves room for the FTC to issue regulations providing more clarity on the full scope of this exception. But one thing seems clear – this will not be a full exemption from all the requirements of the ADPPA.

Does the ADPPA Apply to Employee Data?

Does the ADPPA Apply to Employee Data?

No. "Covered data" under the proposed ADPPA does not include de-identified data, employee data, or publicly available information. This is significant, especially if federal preemption remains in the bill, as it would render unenforceable all employee-related requirements in the CCPA except for the obligation to maintain reasonable security measures and the private right of action for data breaches.

What the ADPPA Requires

The ADPPA would prohibit covered entities from engaging in at least eight practices:

- Collecting, processing, or transferring social security numbers, except when necessary;
- Transferring geolocation information to a third party;
- Collecting, processing, or transferring biometric information;
- Transferring any password, except to a designated password manager or if the transfer is solely for the identification of passwords being re-used;
- Collecting, processing or transferring known nonconsensual intimate images;
- Collecting, processing, or transferring genetic information;
- Transferring an individual's aggregated internet search or browsing history; and
- Transferring an individual's physical activity information from a smart phone or wearable device.

Most of these restrictions can be waived through affirmative express consent of the consumer.

The ADPPA would also prohibit covered entities from engaging in data collection activities that discriminate on the basis of a protected class (such as race, color, religion, national origin, gender, sexual orientation, or disability) unless the collection is for the purpose of self-testing to prevent discrimination or diversifying an applicant, participant, or customer pool. This provision would not apply to private groups that are not open to the public.

To facilitate ongoing compliance with the ADPPA, covered entities (unless subject to the small business exception) would have to designate a privacy officer and a data security officer to implement data privacy and security programs. You should consider all relevant laws when developing your data collection policies and procedures, as well how to mitigate privacy risks to individuals under the age of 17 and privacy risks related to the company's products or services. You should consider implementing reasonable training and safeguards to promote internal compliance. Under the ADPPA, privacy policies would need to include a detailed and accurate representation of the entity's data collection activities and should be made publicly available in a clear and readily accessible manner.

If a consumer exercises any privacy rights guaranteed by the ADPPA, the covered entity cannot take adverse action against the consumer, such as terminating service or charging a higher price. The

ADPPA would further provide that if an individual submits a verified request to either access, correct, or delete their covered data, the request must be fulfilled unless the business falls into the small business exception. Covered entities would not be allowed to engage in targeted advertising towards individuals they know to be under the age of 17 and must allow all other consumers to opt-out.

The ADPPA would require all third-party data collecting entities to register with the FTC. They would also have to place a clear and conspicuous notice on their website or mobile application stating that the entity is a third-party collecting entity that also includes a link to the third-party collecting entity registry.

Large Data Holders

Under the proposed ADPPA, a "large data holder" is defined as a covered entity that, in the most recent calendar year, had annual gross revenues of $250,000 or more and collected, processed, or transferred either (i) the covered data of more than 5 million individuals or devices reasonably linkable to one or more individuals or (ii) the sensitive covered data of more than 100,000 individuals or devices reasonably linkable to one or more individuals. The ADPPA defines "sensitive covered data" as including information such as government-issued identifiers, financial account numbers, biometric and genetic information, precise geolocations, log-in credentials, and information of individuals under the age of 17.

Large data holders would have to provide consumers a short form notice of their data collection practices, including an overview of individual rights and disclosures to reasonably draw attention to data practices that may seem unexpected or that involve sensitive covered data. Within one year of enactment, the CEO and each privacy and data security officer of the large data holder would have to annually certify to the FTC that the business maintains reasonable internal controls and reporting structures to ensure compliance with the ADPPA.

General Exceptions

The ADPPA would provide that a covered entity may conduct data collection activities if reasonably necessary, proportionate, and limited to the any of the following purposes:

- Completing a transaction or fulfilling a service order;
- Performing inventory or network management;
- Debugging or repairing the system;
- Detecting or responding to a security incident;
- Protecting against fraudulent or illegal activity;
- Complying with a legal obligation;
- Establishing, exercising, or defending legal claims;

- Establishing, exercising, or defending legal claims;
- Preventing an individual from suffering harm where there is good faith belief that the individual is at risk of death or serious physical injury;
- Effectuating a product recall;
- Conducting public or peer-reviewed scientific, historical, or statistical research in the public interest; or
- Cooperating with an executive or state agency.

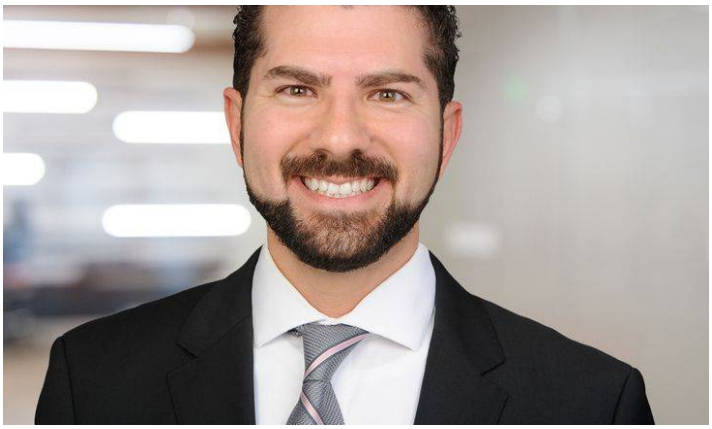
Status of the ADPPA

While the ADPPA represents a big step towards achieving comprehensive federal privacy legislation, the proposal has yet to garner bipartisan support in the Senate. Senator Maria Cantwell (D-WA), Chair of the Senate Commerce Committee, has criticized the ADPPA and is drafting a competing proposal. The draft bill also does not have support from any California member of Congress in either the House or Senate, even though most pending state consumer privacy legislation and this new federal proposal are heavily influenced by the California Consumer Privacy Act.

Fisher Phillips will continue to monitor this area and provide updates as appropriate. Make sure you are subscribed to Fisher Phillips' Alert System to get the most up-to-date information. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Privacy and Cyber Practice Group.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Jill Kleinkauf
Associate
949.798.2123
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber