wiley

ALERT

SECURE Data Act: U.S. House Introduces New National Privacy Framework

April 23, 2026

House Republicans have introduced a new data privacy bill aimed at establishing a unified federal standard for consumer data privacy while preempting the growing patchwork of state laws. The Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Act) was released on April 22, 2026 with support from the Chairs of the U.S. House Committee on Energy and Commerce and the U.S. House Committee on Financial Services.

Below is a high-level overview of the proposed bill, including key compliance considerations for companies currently subject to the patchwork of state privacy laws, which now includes 21 comprehensive privacy laws.

Key Takeaways

1. A Single, Preemptive National Privacy Standard

The SECURE Act represents the most significant development towards federal privacy efforts since the American Privacy Rights Act (APRA) introduced in 2024 and the American Data Privacy and Protection Act (ADPPA) introduced the year prior, neither of which saw a House floor vote. While the release of the SECURE Act is an important first step, there are numerous steps and obstacles to navigate before it may be adopted as law.

If enacted, the legislation would create a national privacy framework and would preempt state laws that "relate[] to" provisions found in the SECURE Act.

2. Scope of the SECURE Act

Authors

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

Crystal Tully
Special Counsel
202.719.4348
ctully@wiley.law

Alexandrine De Bianchi
Public Policy Advisor
202.719.3125
adebianchi@wiley.law

Kimberly S. Alli
Associate
202.719.4730
kalli@wiley.law

Practice Areas

Advertising Technology (AdTech) Data Privacy and Consumer Protection

Privacy, Cyber & Data Governance

State Attorneys General

State Privacy Laws

Telecom, Media & Technology

The SECURE Act would generally apply to an entity that (a) conducts business in the U.S. or offers for use or sale to a resident of the U.S. a product or service, or (b) processes or engages in the sale of personal data of a resident of the U.S., **and**

- Collects and processes personal data of more than 200,000 consumers annually (excluding personal data controlled or processed solely for the purpose of completing a payment transaction) and has an annual gross revenue of $25 million or more (as adjusted for CPI annually); **or**
- Collects and processes personal data of 100,000 or more consumers annually (excluding personal data controlled or processed solely for the purpose of completing a payment transaction) and derives 25% or more of its annual gross revenue from the sale of personal data.

The proposed bill excludes certain entities from coverage, including financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates, certain nonprofit organizations (limited exemption), and institutes of higher education. However, the bill would expressly cover common carriers subject to Title II of the Communications Act of 1934, which are otherwise exempt from FTC jurisdiction. In conjunction with releasing the SECURE Act, the U.S. House also released the draft Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act (GUARD Financial Data Act), which would amend the GLBA to modify privacy requirements applicable to financial institutions.

The proposed bill also excludes certain types of data from coverage, including health information protected under HIPAA.

3. Common Elements with the State Model

The SECURE Act incorporates many familiar elements and provisions from state privacy laws. Specifically, among other things, it would:

- Only govern information about individuals acting in an "individual or household capacity," and would exclude information about individuals acting "in a commercial or employment context." This approach tracks with all state comprehensive privacy laws that have been enacted to date, except for those enacted in California.
- Obligate controllers to (i) follow protocols for data minimization and limits on secondary uses, (ii) implement reasonable data security standards, (iii) contractually obligate processors to comply with specific requirements, and (iv) provide consumer notices.
- Require covered entities to honor specific consumer rights, including the rights of access, correction, and deletion, and to opt out of certain processing activities, including the sale of personal data, targeted advertising, and certain profiling activities.
- Require an opt-in for the processing of sensitive personal data (although the definition of sensitive personal data differs from the definition adopted by many states).

- Provide additional protections for children's and teens' personal data (although states take differing approaches to this data).

4. Divergence from the State Model

However, the bill departs from many state models in several key ways, for example:

- The bill does not include provisions to require a data protection impact assessment for activities deemed to be higher risk.
- It contemplates regulating data brokers as part of the general privacy framework, which may have the effect of preempting state laws specific to data brokers.
- It does not require compliance with a universal opt-out mechanism. Instead, it appoints the Secretary of Commerce authority to conduct a study about these mechanisms and publish a report on its findings within three years.

Additionally, the bill addresses "international data flows and the protection of personal data in international commerce" by proposing to grant the Secretary of Commerce certain powers to advise on these flows. It also gives the Secretary of Commerce the ability to recognize "codes of conduct" proposed by industry, and entities that comply with these codes of conduct would receive a rebuttable presumption of compliance with the SECURE Act. As noted above, the draft bill would explicitly preempt states from prescribing, maintaining, or enforcing state privacy laws that contain provisions that "relate to" provisions found in the SECURE Act.

5. Enforcement

The SECURE Act would establish the Federal Trade Commission (FTC) as the primary enforcement authority. The bill permits certain civil enforcement authority by state Attorneys General, and does not include a private right of action.

6. What's Next?

The SECURE Act next travels to the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, which will mark up the draft. Industry is likely to continue to weigh in on the Act's provisions during this process. If the proposal passes the subcommittee, it will move on to the full Energy and Commerce Committee for consideration.

***

Wiley's Privacy, Cyber & Data Governance team has helped entities of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Please reach out to any of the authors with questions.