Paul, Weiss

Client Memorandum

April 28, 2026

The SECURE Data Act: A New Federal Privacy Framework

On April 21, 2026, Representative John Joyce (R-Pa.) introduced the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act ("SECURE Data Act") in the House of Representatives.[1] The bill is the latest effort to establish a comprehensive national framework for consumer privacy rights and protection of personal data in the United States.[2] The SECURE Data Act attempts to forge a new path forward by applying nationwide the core elements of comprehensive U.S state privacy laws and introducing novel frameworks with respect to data security requirements and enforcement mechanisms.[3]

If enacted, the SECURE Data Act would represent a landmark shift in the American privacy landscape, replacing the current patchwork of state privacy laws with a single, preemptive federal standard precluding states from imposing additional or different privacy requirements.[4]

You Should Know

If enacted, the SECURE Data Act would have significant implications.

- **Streamlined Privacy Compliance, Expanded Scope**. The Act's preemption provision would consolidate applicable privacy requirements, allowing organizations to implement more streamlined compliance programs. The nationwide applicability of the Act would require organizations that did not previously operate in states with comprehensive privacy laws to assess its applicability and, if they meet the applicability thresholds, ensure compliance.

- **Potential Displacement of State-Law Data Breach Claims**. By broadly preempting any state law that "relates to" the Act, the SECURE Data Act may override many state statutory and common-law claims that are predicated on alleged failures to maintain reasonable cybersecurity or comply with state privacy standards. Notably, the Act's preemption language is not limited to state statutes or regulations and could be read to encompass common-law duties and standards developed through case law that "relate to" covered privacy or data-security requirements. This could significantly narrow or eliminate state data breach claims. Because the Act does not provide a private right of action, this shift could channel enforcement primarily to the regulators, such as the FTC, rather than private plaintiffs.

- **Additional Requirements Beyond Existing State Privacy Laws**. While the Act's core consumer rights track existing state laws, several provisions impose new or expand on existing obligations, including the voluntary codes-of-conduct framework, the data broker registration requirement, and cross-border data flow disclosures. With consumer privacy rights, data security, and data broker provisions taking effect just one year after enactment and remaining provisions in two years, organizations will need to move quickly to implement its requirements if the bill becomes law.

[1] Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, H.R. 8413, 119th Cong. (2026) § 1.
[2] *Id.* at § 2(f)(1).
[3] David Botero, *Federal privacy law: Analysis of comments to the US House privacy working group*, IAPP (Dec. 16, 2025), (available here).
[4] Adam Thierer, *Congress Has a Fresh Chance to Pass a Comprehensive Data Privacy Law*, R Street Institute (Apr. 22, 2026), (available here).

- **Novel Covered Nation Disclosure**. In a first-of-its-kind requirement, companies that transfer, process, store, or sell personal data to or in China, Russia, Iran, or North Korea (a "Covered Nation") will need to affirmatively disclose those data flows in their privacy notices.
- **Leveraging Existing GDPR Compliance**. Similar to most existing U.S. state privacy laws, the SECURE Data Act borrows key GDPR concepts, including the controller-processor framework, data minimization, purpose limitation, and opt-in consent for sensitive data. However, the Act is less prescriptive than its European predecessor, omitting requirements for data protection impact assessments, data protection officers, and cross-border transfer restrictions. Companies with global operations may be able to leverage existing GDPR compliance infrastructure as a starting point for compliance with the Act.
- **Presumption of Reasonable Cybersecurity**. Organizations adopting cybersecurity frameworks, such as NIST CSF or ISO/IEC 27001, may be able to take advantage of the Act's rebuttable presumption of compliance with the data security requirement, significantly reducing compliance work and enforcement exposure. Additionally, this may allow organizations to argue in civil litigation that their cyber-program was presumptively reasonable, protecting against negligence claims. Organizations should also monitor the development of Commerce Department-approved codes of conduct, which offer an alternative pathway to the same presumption.

Who Is Affected

Applicability and Scope

The SECURE Data Act applies to any person subject to the Federal Trade Commission Act or that is a common carrier subject to Title II of the Communications Act of 1934, such as for-profit partnerships and corporations engaged in or affecting U.S. commerce, provided they meet certain business and data-processing thresholds, with certain exemptions.[5] Specifically, a covered entity must satisfy both of the following conditions:

- The entity must conduct business in the United States or offer products or services to U.S. residents, or process or sell personal data of U.S. residents.
- The entity must meet one of the following:
  - collect and process personal data of more than 200,000 U.S. consumers annually (excluding payment-transaction-only data) and have annual gross revenue of $25 million or more (adjusted annually for inflation); or
  - collect and process personal data of 100,000 or more consumers annually (excluding payment-transaction-only data) and derive 25% or more of annual gross revenue from the sale of such personal data.[6]

The SECURE Data Act's dual applicability threshold based on the number of consumers whose data is processed and an organization's revenue is higher than the disjunctive thresholds used by most state privacy statutes. Accordingly, some organizations currently subject to state privacy laws would fall outside the federal law's scope.[7]

The bill exempts several categories of entities from its requirements, including federal, state and local governmental entities and financial institutions subject to Title V of the Gramm-Leach-Bliley Act.[8] Rather than exempting specific types of regulated data as state privacy laws generally do, the Act exempts from its scope entire categories of entities — including financial institutions, HIPAA-covered entities, and nonprofits.[9] This is a broader approach than existing state privacy laws, which typically exempt only the specific data governed by these federal regimes (e.g., protected health information under HIPAA, nonpublic personal information under the GLBA) while still subjecting the entity itself to state privacy requirements for any other personal data it processes.

The bill also exempts various categories of data, focusing primarily on data regulated under existing federal privacy regimes., including:

[5] *Id*. at § 13(a).
[6] *Id*.
[7] *Id*. at § 13(a).
[8] *Id*. at § 13(b).
[9] *Id*. at § 13(b).

- Protected health information under HIPAA
- Data subject to the Fair Credit Reporting Act
- Educational records covered by the Family Educational Rights and Privacy Act
- Nonpublic personal information under the Gramm-Leach-Bliley Act
- Employment and benefits administration data [10]

Practical Impacts/Key Requirements

Preemption of State Privacy Laws

The SECURE Data Act contains a broad preemption provision, providing that "[n]o State or political subdivision of a State may prescribe, maintain, or enforce any law, rule, regulation, requirement, standard, or other provision having the force and effect of law, if such law, rule, regulation, requirement, standard, or other provision relates to the provisions of this Act."[11] This language adopts a "ceiling" preemption approach, meaning that the federal law would serve as both a floor and a ceiling, precluding states from imposing additional or different privacy requirements that relate to the SECURE Data Act's subject matter. This approach has already drawn opposition from California, characterizing the Act as "substantially weaker" than state protections.[12]

Consumer Privacy Rights

The Act establishes a suite of consumer privacy rights that are broadly consistent with the rights granted under existing state privacy laws. These include the right to confirm whether a controller is processing their personal data and access a copy of that data (unless doing so would reveal a trade secret). Consumers also have the right to correct inaccuracies in their personal data, to delete personal data provided by or obtained about them, and to the extent technically feasible, to obtain a copy of their personal data in a portable and readily usable format. Consumers may also opt out of the processing of personal data for targeted advertising, the sale of personal data, and reliance on profiling to make decisions that have a legal or similarly significant effect on the consumer.[13]

The Act sets out a similar framework for controllers to respond to consumer requests as most existing state laws, with controllers required to respond within 45 days, with the possibility of extension.[14] Consumers may submit up to two requests to each controller per right per year free of charge and controllers may charge a reasonable fee or decline to act on additional or manifestly unfounded requests.[15]

The Act also establishes an appeals process, requiring controllers to respond to appeals within 60 days and, if the appeal is denied, to provide the consumer with a mechanism to contact the FTC or the relevant state attorney general.[16]

Sensitive Data and Protections for Children

The Act requires affirmative opt-in consent before the collection or processing of "sensitive data," a category that largely tracks existing state definitions but notably extends verifiable parental consent requirements to teens (individuals aged 13 to under 16), going beyond COPPA, which applies only to children under 13.[17] For children under 13, the Act defers to COPPA's consent framework for the sensitive-data requirement, but the remainder of the SECURE Data Act's obligations, including data minimization, privacy notices and data security, still apply in parallel.[18]

The Act replaces the opt-out or use-restriction approach used by most state laws with a stricter, affirmative opt-in consent standard for sensitive data. But this standard applies to a narrower category of personal data, omitting other categories of

[10] *Id.*
[11] *Id.* at § 15.
[12] California Privacy Protection Agency, *Letter to the Honorable Brett Guthrie & the Honorable Frank Pallone Regarding H.R. 8413, the SECURE Data Act*, (Apr. 27, 2026), available here.
[13] *Id.* at § 2(a)(1).
[14] *Id.* at § 2(c)(1).
[15] *Id.* at § 2(d).
[16] *Id.* at § 2(e).
[17] *Id.* at § 2(b).
[18] *Id.*; H.R. 8413 at § 16(35).

data, such as government-issued identifiers, financial account information, contents of mail and email, and union membership , that are considered "sensitive" under the CCPA.[19]

Data Brokers

The Act requires data brokers to post a conspicuous public notice identifying themselves as data brokers and informing consumers of their rights.[20] They must also register annually with the FTC, which must maintain a publicly available, searchable registry of all registered data brokers, disclosing the categories of personal data sold, any unauthorized access incidents, and links to their privacy policies.[21]

Controller and Processor Obligations

The Act imposes comprehensive obligations on both controllers and processors, with the bulk of the compliance burden falling on controllers. These obligations include:

- data minimization and purpose limitation requirements;
- restrictions on secondary uses of personal data;
- prohibitions on discriminatory processing; and
- disclosure requirements for data sales, targeted advertising and automated profiling.[22]

Controllers must also provide consumers with a clear and meaningful privacy notice disclosing, among other items, the categories of personal data processed, each processing purpose, how to exercise consumer rights, categories of data shared with other controllers or governmental entities and whether data is transferred to a "covered nation," with additional conspicuous disclosure obligations for data sales, targeted advertising and automated profiling.[23] Processors, in turn, must adhere to controller instructions, assist in meeting the Act's requirements and operate under written contracts that impose confidentiality obligations, data return or deletion requirements, compliance audit rights and flow-down obligations to subcontractors.[24]

Covered Nation Disclosure

The privacy notice required by controllers must specifically disclose whether any personal data is "transferred to, processed in, stored in, or sold" to a covered nation, which includes China, Russia, Iran, and North Korea.[25] No existing U.S. state privacy law imposes a comparable requirement.

Data Security

The Act requires controllers to establish, implement and maintain reasonable administrative, technical and physical data security practices appropriate to the volume, sensitivity and nature of the personal data.[26] This standard is consistent with existing state privacy law and the standard the FTC has long applied in cybersecurity enforcement actions under Section 5 of the FTC Act. However, the Act provides controllers with two pathways to a rebuttable presumption of compliance with the data security requirement.

- First, a controller may comply with a relevant code of conduct approved by the Secretary of Commerce under Section 8 of the Act (or obtain a relevant certification under the Global Cross Border Privacy Rules System).
- Second, a controller may establish data security practices that are "appropriate to the state-of-the-art" in administrative, technical and physical safeguards, including adherence to a "widely-accepted technical specification" or validation through a third-party attestation, and maintain a comprehensive data security program that "reasonably conforms to a relevant

[19] H.R. 8413 at § 2(b)(1).
[20] *Id.* at § 5(a)–(b).
[21] *Id.* at § 5(b)–(c).
[22] *Id.* at § 3
[23] *Id.* at § 3(g).
[24] *Id.* at § 6(a).
[25] *Id.* at §§ 3(g)(6), 16(11).
[26] *Id.* at § 4(a).

Federal or widely-accepted international risk management framework" for identifying, protecting against, detecting, responding to and recovering from data security events.[27]

The Act does not define what constitutes a qualifying technical specification or risk management framework. The precise contours of these safe harbors would likely be shaped by FTC guidance and enforcement practice over time.

Codes of Conduct and Cross-Border Data Flows

One of the Act's more novel features is its voluntary codes-of-conduct framework.

- Controllers or processors may submit proposed codes of conduct to the Secretary of Commerce for approval, provided the codes meet or exceed the Act's requirements.[28]
- Approved codes of conduct must provide for regular review and validation by an independent organization and include referral mechanisms to the FTC or state attorneys general for noncompliance.[29] Entities that comply with an approved code of conduct enjoy a rebuttable presumption of compliance with the Act's requirements.[30] Certification under the Global Cross Border Privacy Rules System is treated as participation in an approved code of conduct.[31]

Enforcement and the Private Right of Action

FTC and State Attorneys General

The SECURE Data Act does *not* include a private right of action for consumers.[32] However, the FTC is empowered to enforce the Act with the same jurisdiction, powers and duties as under the FTC Act, and any person who violates the Act is subject to FTC Act penalties. In addition, state attorneys general may bring enforcement actions.[33] Before initiating any enforcement action, the FTC or a state attorney general must provide the alleged violator with written notice identifying the specific provision alleged to have been violated.[34]

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Ian C. Richardson
+1-202-223-7405
irichardson@paulweiss.com

Jacobus "Janus" Schutte
+1-212-373-3152
jschutte@paulweiss.com

Audrey M. Paquet
+1-212-373-2397
apaquet@paulweiss.com

Associates Corey J. Goldstein and Cole A. Rabinowitz, and Law Clerks Noah E. Keith and Veronica A. McLean contributed to this Client Memorandum.

[27] *Id.* at § 4(b).
[28] *Id.* at § 8.
[29] *Id.*
[30] *Id.*
[31] *Id.* at § 8(f).
[32] Thierer, *supra* note 3.
[33] H.R. 8413 at § 12(b).
[34] *Id.* at § 12(c).