State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

June 2, 2026

Senator John Thune
Senate Majority Leader
511 Dirksen Senate Office Bldg.
Washington, DC 20510

Senator Chuck Schumer
Senate Minority Leader
322 Hart Senate Office Bldg.
Washington, DC 20510

Representative Mike Johnson
Speaker of the House
521 Cannon House Office Bldg.
Washington, DC 20515

Representative Hakeem Jeffries
House Minority Leader
2267 Rayburn House Office Bldg.
Washington, DC 20515

Senator Marsha Blackburn
Senate Judiciary Committee
357 Dirksen Senate Office Bldg.
Washington, DC 20510

Senator Richard Blumenthal
Senate Judiciary Committee
503 Hart Senate Office Bldg.
Washington, DC 20510

Representative Brett Guthrie
House Committee on Energy
and Commerce Chairman
2161 Rayburn House Office Bldg.
Washington, DC 20515

Representative Frank Pallone
House Committee on Energy
and Commerce Ranking Member
2107 Rayburn House Office Bldg.
Washington, DC 20515

RE: H.R. 8413, The SECURE Data Act

Dear Majority Leader, Minority Leaders, Speaker, and Committee Members:

The undersigned state attorneys general, consumer protection offices, and privacy authorities write to express our opposition to H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act or the Act) and to reiterate our position that federal privacy law must not preempt stronger state law privacy protections. A robust federal data privacy law is one that maximizes protections for consumers by setting a floor, not a ceiling, to allow states to continue to innovate and quickly adapt to the ever-evolving technology industry.

States have long served as laboratories of democracy, developing innovative and effective policy solutions that have served as models for sister states and subsequent federal legislation. As the data economy has grown, states across the political spectrum have enacted thoughtful privacy legislation that meets the unique needs of their residents, including heightened protections for minors and sensitive consumer data, limits on how data may be used and retained, and requiring that businesses honor tools such as universal opt-out preference signals to make it easier for consumers to exercise their rights.

The SECURE Data Act would wipe out these meaningful protections and leave consumers with a privacy regime that makes it harder to exercise their rights, gives businesses more discretion on how to use and retain their data, and significantly limits enforcement remedies.

States must be allowed to rapidly respond to the evolving data landscape.

Preemption leaves the data privacy field frozen in time until Congress chooses to amend and update the law. Given the pace of technological advances, the Act's protections, minimal as they are, could quickly be rendered obsolete. Existing federal privacy frameworks such as the Health Insurance Portability and Accountability Act ("HIPAA")[1] and the Children's Online Privacy Protection Act ("COPPA")[2] have successfully protected consumers with balanced and limited preemption that sets a national floor and allows states to enact laws that respond to changes in businesses data collection and use that were not fully anticipated by federal law. For example, in 2013 California was able to amend its Confidentiality of Medical Information Act to apply its protections to businesses that offer software designed to maintain medical information, such as a fitness app that stores the consumer's diabetic diagnosis information. Ensuring that consumers are protected from new data uses and challenges posed by emerging technologies, such as AI, requires that states be allowed to legislatively innovate and respond in real time to privacy concerns.

Since 2018, twenty states have enacted comprehensive privacy laws. Over 100 million consumers have and are exercising important privacy rights and protections that the Act's broad preemption language could undermine. The Act's expansive preemption of state laws, rules, and regulations that "relate[] to the provisions" of the Act, could also be used to challenge longstanding privacy laws. The Supreme Court has characterized "related to" preemption language as "deliberately expansive,"[3] as a state law will "relate to" a federal law if it "has a connection with or a reference to" the same subject matter.[4] As a result, the Act could potentially

[1] 42 U.S.C. § 1320d-7.
[2] 15 U.S.C. § 6502(d).
[3] *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 383–84 (1992).
[4] *See Shaw v. Delta Air Lines, Inc.*, 463 U.S. 85, 96–97 (1983) (discussing the Employee Retirement Income Security Act of 1974's "relate to" preemption language); *Dan's City Used Cars, Inc.*

impact not just state comprehensive privacy laws, but also laws protecting the home addresses of judges and police officers,[5] laws protecting patients from disclosure of their medical information that might endanger them,[6] laws creating data broker registries,[7] data disposal laws,[8] data breach notification laws,[9] and even privacy torts that consumers have used to protect their rights for decades.

The Act would make it more difficult for consumers to express their privacy choices.

The Act does not require businesses to honor opt-out preference signals, an existing technology already mandated by twelve states and that has been widely adopted by industry.[10] Using opt-out preferences signals consumers can easily and instantaneously communicate their privacy preferences to businesses with a single step, rather than having to individually submit opt-out requests to each business they interact with. Moreover, because the Act tasks the Secretary of Commerce with performing a three-year study on "Universal Opt-Out Methods," but does not provide a method for adoption or implementation of opt-out preference signals, businesses would not be required to comply with opt-out preference signals until further Congressional action. Furthermore, a study is wholly unnecessary; opt-out preference signals have been in operation for years and already effectively allow consumers to exercise their rights.[11]

The Act weakens limits on businesses' use of consumer data.

The Act removes key guardrails on businesses' collection, use, and sharing of consumer data. Existing state laws provide consumers with foundational privacy protections by requiring data minimization, purpose limitations, and retention periods. While the Act contains a data minimization standard, this requirement only applies to data collection—and not to businesses' use, retention, or sharing of consumers data. The data economy is vast and interconnected, and

---

v. Pelkey, 569 U.S. 251, 260 (2013) (discussing the Federal Aviation Administration Authorization Act of 1994's "related to" preemption language).

[5] *E.g.*, Daniel's Law, N.J.S.A. 2C:20-31.1; N.J.S.A. 47:1-17; N.J.S.A. 47:1A-1.1, -5; N.J.S.A. 47:1B-1 to -3; N.J.S.A. 56:8-166.1 to -166.3.

[6] *E.g.*, California Confidentiality of Medical Information Act, 1981 Cal. Stat. ch. 782 (codified at Cal Civ. Code §§ 56 –56.37) (West 1981).

[7] *E.g.* Cal. Civ. Code §§ 1798.99.80 et seq.; ORS 646A.593; Tex. Bus. & Com. Code Ann. §§ 510.001 to 510.010; 9 V.S.A. §§ 2446; Conn. Public Act 26-64.

[8] *E.g.* Cal. Civ. Code §§ 1798.80; Md. Code Ann., Com. Law § 14-3502.

[9] Security Breach Notification Laws, National Conference of State Legislatures (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

[10] *See* US State Privacy Laws Map — All 20+ State Laws, https://privacylawmap.com/states.

[11] *See, e.g.,* Cal. Civ. Code § 1798.135(c); Conn. Gen. Stat. § 42-520(e)(1)(A)(ii) (effective Jan. 1, 2025); If You're A Publisher And You Don't Know What A UOOM Is, Then Read This, https://www.adexchanger.com/data-privacy-roundup/if-youre-a-publisher-and-you-dont-know-what-a-uoom-is-then-read-this/.

failing to require that businesses minimize their data use and sharing greatly increases the risks of data leakage and misuse. Similarly, while the Act contains a purpose restriction, it only prohibits processing "not reasonably necessary or compatible with the **disclosed purpose**" (emphasis added), which incentivizes businesses to flood their privacy policies with any-and-all possible uses of consumers' data.[12] In contrast, many state laws ensure that uses are tied to consumers' reasonable expectations and that data, and in particular sensitive data, may only be processed as reasonably necessary for the specific product or service requested by the consumer.[13] The Act also contains no limits on data retention, allowing businesses to keep consumers' data indefinitely, further increasing the risk that consumer data may be subject to data breaches and misuse.

The Act narrowly defines key terms and broadly defines the scope of exemptions to substantially limit consumers' data rights and companies' responsibilities.

While the Act purports to provide similar consumer personal data rights to those under existing state laws, the Act defines key terms much more narrowly. For example, the Act's definition of "sensitive data" excludes data regarding mental or physical health conditions unless that information discloses a "diagnosis"—this definition would exclude information on mental or physical health symptoms, ailments, or conditions that is currently considered sensitive under state law, meaning such information could be processed absent consumer consent.[14] Similarly, profiling in the Act only refers to "solely automated" decision-making, meaning that consumers would lose the right to opt out of profiling currently available under existing state law if there is human involvement at any point in the process, however slight.[15] And "biometric data" excludes data generated from photos, audio, or video, or other data that can be used to identify an individual, even though those mediums can and are used to generate biometric information on individuals.[16] The Act also increases the scope of potential exemptions by excluding any data that is "intermingled" with exempted data, any data held by for-profit colleges or nonprofit entities, and any "health records" data – irrespective of whether that data is protected by HIPAA.

---

[12] H.R. 8413, The Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (119th Congress), https://d1dth6e84htgma.cloudfront.net/SECURE_Data_Act_for_introduction_7c80a347ac.pdf.

[13] Cal. Civ. Code § 1798.100(c); Md. Code Ann., Com. Law §14-4707(a)(1) (limiting the collection and processing of sensitive data to what is "strictly necessary" to provide the specific product or service requested by the consumer).

[14] *See, e.g.*, Cal. Civ. Code § 1798.140(ae)(2)(B); Conn. Gen. Stat. § 42-515(38); Md. Code Ann., Com. Law §14-4701(i), (gg); ORS 646A.570(18)(a)(A).

[15] *See, e.g.*, Conn. Gen. Stat. § 42-520(a)(5)(C) (effective July 1, 2026); ORS 646A.570(16); ORS 646A.574(d)(C).

[16] *See, e.g.*, Cal. Civ. Code § 1798.140(ae)(2)(A); (24)(b); Conn. Gen. Stat. § 42-515(4); Md. Code Ann., Com. Law § 14-4701(d); ORS 646A.570(3)(b).

Additionally, the Act allows companies to charge consumers fees for asserting their privacy rights under certain circumstances, creating perverse incentives for data collection and privacy compliance and unjust barriers to the exercising of a consumer's basic rights to access, delete, and correct their personal data.

The Act weakens privacy enforcement and encourages non-compliance.

Finally, the Act greatly weakens states' enforcement abilities and incentivizes non-compliance in multiple ways. Most troublingly, the Act provides businesses with an ongoing 45-day notice-and-cure period—that does not sunset—for all violations of the law, encouraging businesses to delay compliance with the law until approached by enforcers. Indeed, as businesses across the country have already been complying with state law requirements that exceed the Act, a notice and cure period is neither necessary nor appropriate. Unlike existing state laws and similar federal consumer protection laws[17], the Act does not provide for civil penalties in actions brought by state authorities, weakening the deterrent effect of potential enforcement actions. And the Act's limitation of enforcement to the Federal Trade Commission and state attorneys general would deprive states of the ability to delegate and share enforcement responsibilities with other state agencies and regulators, such as the voter-created California Privacy Protection Agency.

In sum, the Act moves privacy rights in the wrong direction, leaving consumers worse off and with fewer protections. We respectfully urge you to reject this bill. Thank you for your consideration and attention to this issue.

ROB BONTA
California Attorney General

TOM KEMP
Executive Director of the CalPrivacy

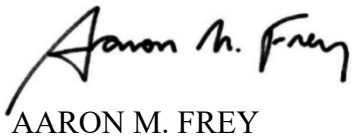
WILLIAM TONG
Connecticut Attorney General

KATHLEEN JENNINGS
Delaware Attorney General

MANA MORIARTY
Executive Director
State of Hawaii
Office of Consumer Protection

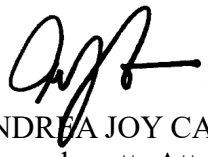
KWAME RAOUL
Illinois Attorney General

[17] 45 C.F.R. Part 160, Subpart D; 15 U.S.C. 6805.



AARON M. FREY
Maine Attorney General

ANTHONY G. BROWN
Maryland Attorney General



ANDREA JOY CAMPBELL
Massachusetts Attorney General

KEITH ELLISON
Minnesota Attorney General

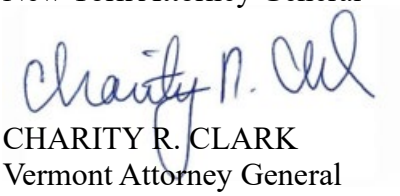
AARON D. FORD
Nevada Attorney General

JOHN M. FORMELLA
New Hampshire Attorney General

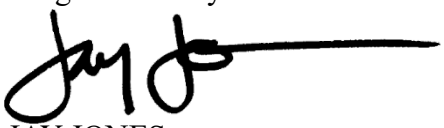
JENNIFER DAVENPORT
New Jersey Attorney General

LETITIA JAMES
New York Attorney General

DAN RAYFIELD
Oregon Attorney General



CHARITY R. CLARK
Vermont Attorney General



JAY JONES
Virginia Attorney General

NICOLAS W. BROWN
Washington Attorney General