U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

June 3, 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy & Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy & Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
Committee on Energy & Commerce
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, DC 20515

The Honorable Janice Schakowsky
Ranking Member
Committee on Energy & Commerce
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, DC 20515

Statement for the Record by the U.S. Chamber of Commerce for Hearing Before the House Commerce, Manufacturing and Trade Subcommittee Entitled: Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law

Chairmen Guthrie and Bilirakis and Ranking Members Pallone and Schakowsky,

The U.S. Chamber of Commerce ("Chamber") thanks you for the opportunity to provide comment for today's hearing entitled "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law." For over a decade the Chamber has called on Congress to pass a strong, bipartisan, comprehensive privacy law that establishes one single national framework. HR 8413, the "SECURE Data Act" achieves this goal by establishing a uniform national standard, establishes clear, predictable enforcement mechanisms, and builds upon a bipartisan consensus approach to privacy that has been supported by over 2,500 Democrat and Republican state lawmakers.

I. The SECURE Data Act Establishes A Strong Uniform Standard

A national privacy framework must include strong federal preemption to eliminate the growing patchwork of state privacy laws. The current state-by-state approach creates confusion for consumers and imposes significant compliance

burdens on businesses, particularly small businesses. A 2022 report highlighted that a fragmented privacy landscape could cost the U.S. economy $1 trillion, with $200 billion of that burden falling on small businesses[1]. Just recently, the California Privacy Protection Agency finalized its California Consumer Privacy Act ("CCPA") cyber, risk assessment, and automated decision-making technology, and insurance rulemaking which was estimated to cost businesses at least $4.8 billion over 10 years—with small businesses incurring annual costs of $16,377.[2]

Without federal preemption, businesses are forced to navigate conflicting state laws, which increases litigation risks and compliance costs. This complexity disproportionately impacts small businesses, which often lack the resources to manage multiple regulatory regimes. The Chamber's *Empowering Small Business: The Impact of Technology on U.S. Small Business Report* highlights that 65% of small businesses fear increased litigation and compliance costs from out-of-state privacy and AI laws.[3]

Only through a fully preemptive federal privacy law can Congress provide needed clarity and consistency, enabling businesses to focus on innovation and growth while ensuring robust consumer protections.

To achieve the goal of strong preemption, a national privacy law must explicitly state that it preempts or supersedes state laws and regulations *related to* data privacy and security. Recent legislation like the American Privacy Rights Act failed to achieve this needed language by proposing to preempt merely what was "*covered by* "the national privacy law.

To provide the strongest preemption, as noted by a Congressional Research Service report, Congress should use stronger language than "covering" or "covered by" in order to achieve the goal of ending a patchwork.[4] According to the Supreme Court, "'Covering' is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[5] Under a "covered by" approach, Congress would have to insert in a national privacy law all the obligations and requirements that all states have in order to fully preempt what has been passed. This approach also does not account for future laws passed by states that do not match requirements to the federal approach.

---

[1] ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," (January 2022) available at https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.

[2] *See* Economic Impact Assessment for CCPA Updates, Cyber, Risk, ADMT and Insurance (2025) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_eis.pdf.

[3] **U.S. Chamber of Commerce.** *Empowering Small Business: The Impact of Technology on U.S. Small Business. 2025*, **U.S. Chamber of Commerce, 2025.** https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf

[4] Congressional Research Service "Federal Preemption: A Legal Primer," (May 2023) available at https://crsreports.congress.gov/product/pdf/R/R45825

[5] CSX Transportation, Inc. v. Easterwood, 507 U.S. 663 (1993.)

The SECURE Data Act adopts "related to" language which would be interpreted by courts that Congress intended for there to be a single set of rules as opposed to establishing preemption for a narrow subset of issues.

II. The SECURE Data Act Provides Clear and Predictable Enforcement Mechanisms

Effective enforcement of a national privacy law is critical to protecting consumers and ensuring compliance. The Chamber supports Congress vesting enforcement authority in appropriate federal agencies and state attorneys general. The SECURE Data Act correctly establishes enforcement authority with the Federal Trade Commission ("FTC") as well as state attorneys general. These agencies have the expertise and resources to enforce privacy laws effectively while maintaining a balanced approach that encourages compliance and innovation.

However, the Chamber strongly opposes private rights of action in privacy law. Private rights of action have historically led to abusive litigation, with plaintiffs' attorneys benefiting disproportionately from settlements while providing little relief to consumers. Such litigation diverts resources away from compliance and innovation, forcing businesses to focus on defending frivolous lawsuits rather than protecting consumer privacy.

Private rights of action codified in statutes also incentivize novel theories of law to pursue claims for activities that are routine and do not cause harm. For example, in recent years, plaintiffs' attorneys have looked to expand state wiretapping statutes, which were written to address telephone eavesdropping[6], to bring lawsuits against U.S. companies for routine and widely accepted online practices, including the use of cookies and other standard web analytics tools. These claims assert that long-standing technologies used to understand website performance, improve user experience, and support basic digital operations amount to unlawful "interception" under state wiretap laws[7]. There have been over 4000 of these types of suits filed nationwide, with over 2000 of these claims being made against retailers, healthcare facilities, and financial services firms.

Private rights of action also create inconsistent enforcement, as individual judicial districts may interpret privacy laws differently. This inconsistency undermines the goal of a uniform national standard and increases uncertainty for businesses.

---

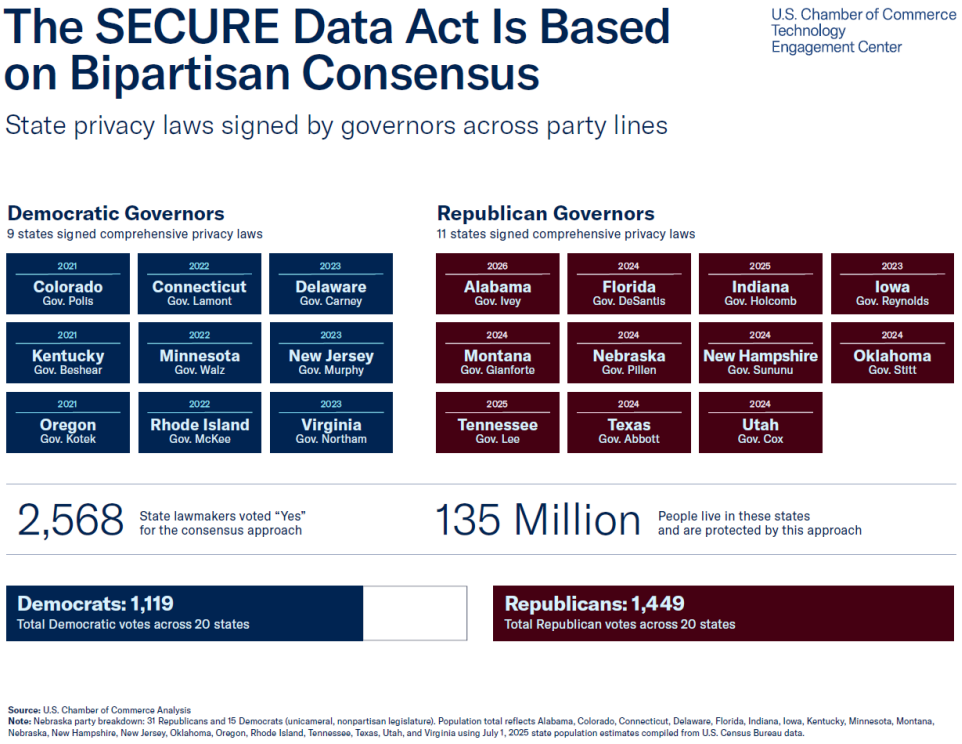
[6] See Amicus of U.S. Chamber of Commerce, Guiterez v. Converse (C.D. Cal January 22, 2025) *available at* https://www.uschamber.com/assets/documents/U.S.-Chamber-Coalition-Amicus-Brief-Gutierrez-v.- Converse-Inc.-Ninth-Circuit.pdf.

[7] Fisher Phillips. *Digital Wiretapping Litigation Map*. Fisher Phillips LLP, 31 May 2022, https://www.fisherphillips.com/en/resources-and-innovation/trackers-and-maps/wiretapping-litigation-map.

Instead, enforcement should remain with expert regulators who can provide consistent guidance and ensure that privacy laws are applied fairly and effectively.[8]

III. The SECURE Data Act Builds upon the strong and bipartisan Consensus Privacy Approach

The SECURE Data Act builds upon the strong and bipartisan Consensus Privacy Approach which has been enacted in 20 states including Virginia, Texas, New Jersey, Oregon, and Kentucky. The Consensus Privacy approach has been signed by 9 Democrat and 11 Republican governors. It was also supported by 1,119 Democrat and 1,449 Republican state lawmakers.



Not only does the SECURE Data Act build on bipartisan consensus, it builds upon a proven and workable model that establishes reasonable data minimization requirements, strong consumer rights and protections, and effective enforcement.

[8] *See* U.S. Chamber Institute for Legal Reform, "Ill Suited: Private Rights of Action and Privacy Claims," (2019) *available at* https://instituteforlegalreform.com/research/ill-suited-private-rights-of-action-and-privacy-claims/.

A. Data Minimization

The SECURE Data Act mirrors the overwhelming consensus of states on data minimization requirements. Data is a cornerstone of the modern economy and plays a critical role in addressing societal challenges. From improving public safety and healthcare to enabling financial inclusion and combating fraud, data-driven technologies have transformed how we solve complex problems.[9] Although data minimization is critical to safeguarding consumer privacy and security, standards that are too strict could impede innovation and the ultimate goal of protecting people and systems. States with the Consensus Privacy Approach have enacted a balanced and workable data minimization standard.

For example, states like Kentucky, Tennessee, Nebraska, Florida and Texas mandate companies limit data collection to what is "adequate, relevant, and reasonably necessary" related to a *disclosed* purpose.[10] By contrast, states like Maryland have enacted stricter data minimization requirements that only allow the collection or processing of data for "what is necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains."[11] Congress should avoid approaches with restrictions that prohibit the collection or processing of sensitive data – depriving consumers of the ability to consent - unless it "is strictly necessary to provide or maintain a specific product or service…"[12]

Such a strict data minimization approach could limit companies' ability to use personal data for important purposes such as anti-fraud protections, Know Your Customer, and other web-based security applications (used by federal programs to reduce theft of benefits and identity fraud). Data has also enabled law enforcement to stop criminal activity such as human trafficking and organized crime.[13]

B. The SECURE Data Act Mirrors, Not Diminishes, Protections Offered in States.

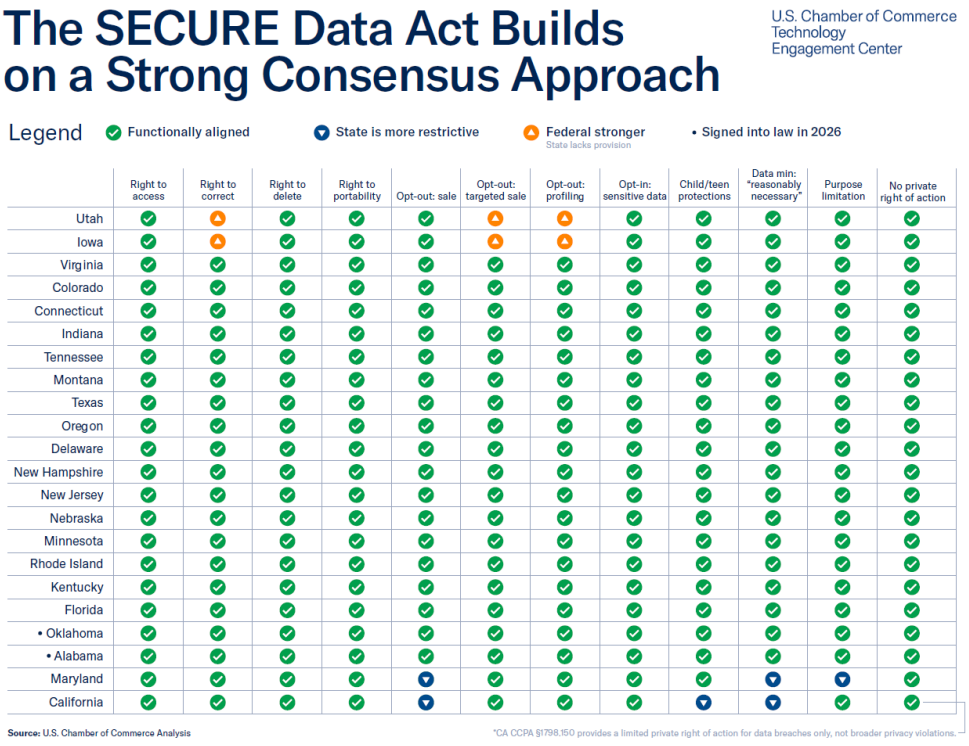
The SECURE Data Act mirrors the state Consensus Privacy Approach in that it provides consumers robust privacy protections including the right to:

- Know how data is used and collected;
- Obtain a portable version of their data;
- Delete personal data; and

[9] *See e.g.* U.S. Chamber of Commerce, "Data for Good: Promoting Health, Safety and Inclusion," (2020) *available at* https://www.uschamber.com/assets/documents/ctec_dataforgood_v4-digital.pdf.
[10] Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1) (emphasis added).
[11] Md. Code Ann. Comm. Law § 14-4606(B)(1)
[12] Id. at § 1404607(A)(1).
[13] *Supra* n. 9.

- Opt out of the use of data for targeted advertising across non-affiliated websites, the sale of data, and automated profiling in legally significant use cases like lending, employment, and housing.

The Consensus Privacy Approach, like the SECURE Data Act, requires companies to obtain consent from people before processing their sensitive personal data like racial, gender, biometric, and precise geolocation information. Both the Consensus Privacy Approach and SECURE Data Act also prohibit using personal data to illegally discriminate against protected classes and company retaliation against consumers exercising their privacy rights. In terms of enforcement mechanisms, SECURE Data mirrors the Consensus Privacy Approach by vesting enforcement solely with government agencies.



C. The SECURE Data Act Bolsters Protections

The SECURE Data Act also creates uniform privacy rights not embraced by all states. For example, some states do not provide an opt out for targeted advertising and automated profiling which the SECURE Data Act would provide all Americans. The bill would also create a consent requirement for processing data of minors younger than sixteen. Finally, the bill also establishes a national data broker registry that has not been adopted in the Consensus Privacy Approach but has been enacted in standalone laws in states like Vermont.

D. Necessary Exceptions

Although a reasonable data minimizaiton standard is necessary to promote innovation, states adopting the Consensus Privacy Approach have also provided explicit exceptions for data processing already being undertaken. For example, the Virginia Consumer Data Protection Act (VCDPA) excempts data regulated under FCRA and the Drivers Privacy Protection Act.[14] Additionally, the VCDPA excplity exempts data used to[15]:

- Comply with federal, state, or local laws;
- Comply with legal investigations;
- Cooperate with law enforcement;
- Investigate and defend against legal claims;
- Provide a product or service;
- Protect against threats to physical safety and protect life;
- Prevent, detect, and protect agianst security incidents and illegal activitiy; and
- Engage in research

IV. Conclusion

In conclusion, the U.S. Chamber of Commerce urges Congress to pass the SECURE Data Act because it includes strong federal preemption, provides a uniform standard for businesses and consumers, vests enforcement authority with appropriate Federal agencies and state attorneys general, and avoids private rights of action that lead to abusive litigation and inconsistent enforcement. The SECURE Data Act mirrors the state Consensus Privacy Approach, striking an appropriate balance on data minimization and consumer rights to protect privacy while enabling the beneficial uses of data to drive innovation and address societal challenges.

Sincerely,

Jordan Crenshaw

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

[14] Va. Code Ann §
[15] *Id.* At § 59.1-582.