Documents for the Record
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
June 3, 2026

Submitted by the Majority

1. Letter from Association for Competitive Technology to Chairman Brett Guthrie, Subcommittee Chairman Gus Bilirakis, Ranking Member Frank Pallone, Subcommittee Ranking Member Jan Schakowsky. Submitted by majority.

2. Data from Business Software Alliance. Submitted by majority.

3. Letter from Internet for Growth. To Chairman Guthrie, Ranking Member Pallone, and Members of the Committee. Submitted by majority.

4. Letter from Reason Foundation. To Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee. Submitted by majority.

5. Statement from The Nonprofit Alliance. Submitted by majority.

6. Data from Business Roundtable. Submitted by majority.

7. Letter from American Advertising Federation -Louisville. To Chairman Guthrie. Submitted by majority.

8. Letter from Thomas Schatz, President of the Council for Citizens against Government Waste. To House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade. Submitted by majority.

9. Letter from TechNet. To Subcommittee Chairman Bilirakis and Subcommittee Ranking Member Schakowsky. Submitted by majority.

10. Statement from AdvaMed Digital Health Tech. To House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade. Submitted by majority.

11. Letter from the National Multifamily Housing Council, National Apartment Association, and the Real estate Technology & Transformation Center. To Chairman Bilirakis and Subcommittee Ranking Member Schakowsky. Submitted by majority.

12. Letter from the Association of National Advertisers. To Chairman Gus Bilirakis, Vice Chairman Russ Fulcher, and Ranking Member Jan Schakowsky. Submitted by majority.

13. Statement from the American Property Casualty Insurance Association. Submitted by majority.

14. Letter from the Consumer Choice Center. To Chairman Bilrakis, Ranking Member Schakowsky, and Members of the Subcommittee. Submitted by majority.

Documents for the Record
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
June 3, 2026

15. Letter from the Information Technology Industry Council (ITI). To Chairman Guthrie, Ranking Member Pallone, Subcommittee Chairman Bilirakis, and Subcommittee Ranking Member Schakowsky. Submitted by majority.

16. Letter from The National Association of Wholesaler-Distributors (NAW). To Chairman Bilirakis and Ranking Member Schakowsky. Submitted by majority.

17. Letter from the National Insurance Crime Bureau (NICB). To Chairman Bilirakis. Submitted by majority.

18. Statement from Privacy for America. To Chairman Guthrie, Ranking Member Pallone, Subcommittee Chairman Bilirakis, and Subcommittee Ranking Member Schakowsky. Submitted by majority.

19. Letter from the 21st Century Privacy Coalition. To Chairman Guthrie, Ranking Member Pallone, Subcommittee Chairman Bilirakis, and Subcommittee Ranking Member Schakowsky. Submitted by majority.

20. Statement from America's Health Insurance Plans (AHIP). Submitted by majority.

21. Statement from American Action Forum (AAF). Submitted by majority.

22. Letter from Taxpayers Protection Alliance to Chairman Guthrie and Ranking Member Pallone. Submitted by the Majority.

23. Letter from National Business Coalition on Artificial Intelligence and Privacy to Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, and Ranking Member Pallone. Submitted by the Majority.

24. Letter from Ohio Attorney General to Chairman Guthrie. Submitted by the Majority.

25. Statement from American Bankers Association. Submitted by the Majority.

26. Letter from Network Advertising Initiative to Chairman Guthrie. Submitted by the Majority.

27. Letter from National Association of Truck Stop Operators and the Society of Independent Gasoline Marketers of America to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky. Submitted by the Majority.

28. Letter from Business Roundtable to Chairman Guthrie and Chairman Bilirakis. Submitted by the Majority.

29. Statement from U.S. Chamber of Commerce to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky. Submitted by the Majority.

Documents for the Record
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
June 3, 2026

30. Letter from U.S. Chamber of Commerce to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky. Submitted by Majority.

31. Letter from Merz Apothecary to Energy and Commerce Committee. Submitted by Majority.

32. Letter from ECi Stores to Energy and Commerce Committee. Submitted by Majority.

33. Letter from Firecracker Software to Energy and Commerce Committee. Submitted by Majority.

34. Letter from Developers Alliance to Energy and Commerce Committee. Submitted by Majority.

35. Letter from Chimani to Energy and Commerce Committee. Submitted by Majority.

36. Letter from Connected Commerce Council to Energy and Commerce Committee. Submitted by Majority.

37. Letter from Biotechnology Innovation Organization (BIO) to Chairman Guthrie and Ranking Member Pallone. Submitted by the Majority.

38. Letter from Computer & Communications Industry Association (CCIA) Consumer Technology Association (CTA) CTIA INCOMPAS NCTA—The Internet & Television Association NetChoice Software & Information Industry Association TechNet USTelecom—The Broadband Association to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky. Submitted by the Majority.

39. Letter from Security Industry Association to Chairman Guthrie, Ranking Member Pallone, Chairman Hudson, and Ranking Member Matsui. Submitted by Majority.

Submitted by the Minority

1. Letter from Center for AI and Digital Policy to Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky. Submitted by the Minority.

2. Letter from The Leadership Conference to Chairman Bilirakis and Ranking Member Schakowsky. Submitted by Rep. Clarke.

Documents for the Record
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade Hearing
June 3, 2026

3. Letter from State of California Office of the Attorney General to Senator Thune, Senator Schumer, Speaker Johnson, Minority Leader Jeffries, Senator Blackburn, Senator Blumenthal, Chairman Guthrie, Ranking Member Pallone. Submitted by the Minority.

4. California Privacy Protection Agency to Chairman Guthrie and Ranking Member Pallone. Submitted by Rep. Mullin.

June 1, 2026

The Honorable Brett Guthrie
Chairman
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Gus Bilirakis
Chairman
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, District of Columbia 20515

RE: ***Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law***

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

Thank you for the opportunity to submit testimony for the record on your hearing titled, *Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law*.[1]

The Association for Competitive Technology (ACT) represents small business innovators and startups in the software development and high-tech space in the United States and around the world. As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping consumers lead healthier lives. Today, the

[1] "Chairmen Guthrie and Bilirakis Announce Hearing on Establishing a Federal Data Privacy Law." *House Committee on Energy and Commerce*, energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-establishing-a-federal-data-privacy-law. Accessed 31 May 2026.

domestic app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[2]

The Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act) represents a thoughtful and balanced approach to protecting consumers' personal information and supporting small businesses in the digital economy. Small businesses increasingly operate in a digital economy where customers, business partners, and vendors expect strong privacy and cybersecurity practices. As a result, the framework Congress establishes for consumer privacy will shape the compliance expectations and marketplace standards all small businesses encounter, regardless of whether they meet the applicability thresholds detailed in the bill.

As the Committee debates this proposal, policymakers should ensure that any final bill reflects the Four Ps of Privacy: path to compliance, preemption, no private right of action, and protection against unauthorized access. First, the bill should offer small businesses a mechanism to achieve compliance that recognizes their size and limitations. Second, comprehensive federal privacy legislation should preempt the current patchwork of state privacy laws to establish a single uniform standard for protecting consumer privacy. Third, the bill should exclude a private right of action to protect small businesses from opportunistic litigation. Fourth, including strong cybersecurity provisions will ensure that consumer data entrusted to small businesses remains protected from hacking or misuse. As currently drafted, the SECURE Data Act advances each of these objectives by establishing a preemptive national framework that provides businesses with a clear path to compliance, promotes consumer protection, strengthens data security, and creates greater regulatory certainty.

Why Congress Should Enact a Comprehensive Federal Privacy Law

For small businesses, a federal privacy framework would provide meaningful certainty and predictability. Unlike large corporations with dedicated legal and compliance teams, small businesses often lack the time and resources necessary to track and comply with dozens of inconsistent state privacy laws. A single federal standard that preempts this state patchwork will enable small businesses to focus on serving customers, hiring employees, and growing their businesses instead of navigating a complex, costly regulatory landscape.

Moreover, a comprehensive federal privacy law would enable competition in the digital economy. Regulatory fragmentation disproportionately burdens smaller and newer market entrants, which typically have fewer resources to devote to compliance than their larger counterparts. By establishing a uniform set of rules, policymakers can reduce barriers to entry and create a more level playing field.

Finally, consumers would benefit from a federal comprehensive privacy law through the creation of consistent and enforceable privacy rights. Under the current state patchwork, consumers' privacy rights may vary depending on which state they live in. A national framework would ensure that consumers can receive and exercise the same protections regardless of their zip code and enable small businesses to better protect their customers.

---

[2] "State of the App Economy." *ACT | The App Association*, ACT | The App Association, actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf. Accessed 13 Jan. 2026.

Path to Compliance
Among the SECURE Data Act's strongest features is its voluntary code of conduct framework. This provision would enable small businesses who do not meet the applicability threshold to publicly self-certify their compliance with an approved and independently administered code of conduct designed to be cost-effective and appropriate for participants' size, risk profile, and operational limitations. In return, small businesses would receive a rebuttable presumption of compliance. This structure offers small businesses a clear, affordable, and credible path to demonstrating compliance with a recognized standard.

Publicly self-certifying to compliance also enables small businesses to compete in the digital economy. Many of ACT's members operate in a business-to-business marketplace where larger companies routinely require their vendors, processors, subcontractors, and service providers to meet specific privacy obligations before winning a contract. Public participation in an approved code of conduct offers a standardized way to prove readiness and compete for opportunities. In fact, in a 2026 Data and Privacy Benchmark Study, Cisco found that 96 percent of survey respondents reported that external, independent privacy certifications influence vendor selection decisions.[3] In a marketplace where privacy and security expectations increasingly influence purchasing decisions, a recognized certification provides small businesses with a competitive advantage.

Further, the code of conduct framework offers small businesses flexibility instead of a one-size-fits-all mandate. Because participation is voluntary, small businesses can assess whether an approved code of conduct aligns with their operations, customer base, and growth plans, and opt in accordingly. As a result, a business operating primarily in a single state can avoid taking on federal obligations that do not reflect its customers' expectations or business operations.

Preemption
Importantly, the SECURE Data Act includes a robust preemption standard that would replace the current patchwork of state privacy laws with a uniform national framework for comprehensive privacy protection. Establishing this single federal standard would provide consumers with consistent rights and protections while also giving small businesses a clear and predictable compliance environment.

To date, 22 states have enacted their own comprehensive privacy laws and two more are expected to do so within the coming weeks.[4] While many of these laws share a common structure, they differ in key provisions, including applicability thresholds, definitions, enforcement mechanisms, and obligations. Although state privacy laws set applicability thresholds to carve small businesses out, some states, such as Connecticut and Montana, have recently amended their laws to lower applicability thresholds and expand the number of businesses captured by their laws. As a result, even businesses that do not currently meet

[3] *Cisco 2026 Data and Privacy Benchmark Study*, www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2026.pdf. Accessed 31 May 2026.
[4] "S.71." *State House Dome*, legislature.vermont.gov/bill/status/2026/S.71. Accessed 1 June 2026.; "SB386," www.legis.la.gov/legis/BillInfo.aspx?s=26rs&b=SB386&sbi=y. Accessed 1 June 2026.

applicability thresholds must devote resources towards monitoring legislative updates and determining whether new changes will bring them within the scope of state comprehensive laws.

This increasingly fragmented regulatory landscape imposes significant costs on small- and medium-sized businesses. Instead of focusing on growth, hiring, and innovation, small businesses must expend limited time and resources on tracking legislative changes, obtaining legal guidance, and implementing compliance programs. In a 2022 report, the Information Technology and Innovation Foundation estimated that a 50-state privacy patchwork could impose up to $23 billion in compliance costs on small businesses.[5] By preempting the growing patchwork of state privacy laws with a single national standard, the SECURE Data Act would reduce unnecessary compliance burdens and allow small businesses to focus their resources on serving their customers and competing in the digital economy.

No Private Right of Action

The SECURE Data Act's enforcement framework effectively balances strong consumer protections with safeguards against unnecessary litigation. By empowering the Federal Trade Commission (FTC) and state attorneys general with enforcement authority instead of creating a private right of action, the bill ensures accountability against malfeasance while protecting small businesses from opportunistic litigation.

While well-intended, private rights of action can incentivize litigation without meaningfully advancing consumer privacy. In practice, private rights of action encourage "sue-and-settle" business models in which plaintiffs' firms file or threaten meritless lawsuits in order to extract settlements from businesses. While large businesses may be able to absorb these costs as routine expenses, small businesses often lack the financial resources to defend against baseless claims. Faced with the prospect of costly litigation, many small businesses may instead choose to settle such claims and pay opportunistic litigants.

A broad private right of action may also undermine the goal of establishing a single national framework for consumer privacy. Private rights of action can produce inconsistent judicial interpretations across jurisdictions, which ultimately creates uncertainty regarding compliance obligations and exposes small businesses to inconsistent legal standards. Over time, this fragmentation will replicate many of the challenges associated with the current state-by-state patchwork.

Instead of relying on a private right of action, the SECURE Data Act's enforcement model mirrors the models included in state privacy laws. Of the 22 states that have enacted comprehensive consumer privacy laws, only California includes a limited private right of action, primarily in the context of certain data breaches. Legislatures across the political spectrum have overwhelmingly chosen to empower attorneys general and other designated regulators with enforcement. By following this approach, the SECURE Data Act promotes consistent and effective enforcement of consumer privacy rights while avoiding the costs, uncertainty, and opportunistic litigation associated with a private right of action.

---

[5] Castro, Daniel, et al. *The Looming Cost of a Patchwork of State Privacy Laws*, www2.itif.org/2022-state-privacy-laws.pdf. Accessed 31 May 2026.

Protection Against Unauthorized Access
The SECURE Data Act appropriately includes strong cybersecurity requirements for businesses, and requires them to establish and maintain reasonable administrative, technical, and physical safeguards that are tailored to the volume, sensitivity, and nature of the data they process. By adopting this risk-based standard, the bill promotes strong cybersecurity practices that reflect the operational realities small businesses face across sectors.

Further, by linking a rebuttable presumption of compliance to adherence with an approved code of conduct, the SECURE Data Act creates meaningful incentives for businesses to adopt strong cybersecurity practices and invest in proactive data security measures. This framework enables small businesses to protect consumer data, promotes the adoption of effective cybersecurity measures, and allows enforcement resources to be focused on bad actors and genuinely deficient security practices.

Age Assurance Concerns
Section 2(b)(3) of the SECURE Data Act would prohibit a controller from processing any sensitive data of an individual between the ages of 13 and 15 without first obtaining "verifiable consent." Because this provision would impose a blanket prohibition on processing sensitive data pertaining to these individuals based on their age—absent verifiable consent from a guardian—age estimation and less privacy-intrusive forms of age assurance may be insufficient. As discussed further below, all controllers subject to the SECURE Data Act may face an obligation to conduct riskier forms of age assurance, such as age verification, either in-house or through a third-party processor.

Except when used to validate eligibility for discounts or similar benefits, age assurance techniques are typically deployed as a means of addressing age-related risks—either to restrict access by individuals under a certain age to content that poses foreseeable risks related to users' ages, or to direct individuals to age-appropriate experiences. Services that are not designed to make age-inappropriate content available or expose children and teens to age-related risks do not use age assurance techniques. Doing so presents privacy and security risks associated with age assurance, without providing an age-related risk mitigation benefit. Given the broad definition of "sensitive data" to any information that is "linked or linkable" to a teen, Section 2(b)(3)'s obligation appears to require all controllers that happen to have a teen as a user to conduct age verification. For example, if a 14-year-old downloads an app made by an ACT member, the ACT member would have to conduct age verification for all of their users in order to comply with this provision, regardless of whether they provide age-inappropriate content for 14-year-olds.

Section 2(b)(3)'s requirement to obtain "verifiable consent" from a parent of a teen would compound the privacy risks of age verification alone, by obligating all controllers with a teen user to associate teen profiles with parent profiles. The existing Children's Online Privacy Protection Act (COPPA) imposes a similar obligation to obtain "verifiable parental consent" from guardians of children under 13. As a practical matter, the requirements as applied are formidable for small businesses. COPPA's saving grace is that it only applies to services that are either intentionally directed to children under 13 or to services with "actual knowledge" of a child's under-13 status. This has helped prevent the application of COPPA's prohibitive compliance and liability regime to barber shops and restaurant chains with scheduling and

ordering apps. Unfortunately, Section 2(b)(3) would likely expand COPPA-style obligations to all apps on the stores and services on the internet. As a result, unintended liability exposure and compliance hurdles would hamper innovation and job creation by small business innovators, while also posing unnecessary privacy risks in the form of big data honeypots required to conduct age verification for all users and associating teen accounts with parent accounts. We urge the Committee to work with ACT on targeting any measures intended give parents more meaningful oversight of their teens' online experience, without producing these unintended consequences. The Parents Over Platforms Act (POPA, H.R. 6333), which the Subcommittee approved unanimously in December 2025, would be a good start with respect to apps on the major stores, since it would apply age assurance obligations in a risk-based manner to services that are differentiated between adults and minors.

Conclusion

As Congress debates the SECURE Data Act, it should preserve the key features that make the bill a balanced and workable framework: a clear path to compliance, robust preemption, regulator-led enforcement without a private right of action, and strong protections against unauthorized access. Together, these provisions would protect consumer privacy while ensuring that federal privacy legislation remains practical for the small businesses and startups that drive innovation in the digital economy.

Thank you for your time and consideration. We appreciate the Subcommittee's focus on federal comprehensive privacy legislation and welcome the opportunity to further engage as the legislative process moves forward.

Sincerely,

Morgan Reed
President
Association for Competitive Technology

Business Software Alliance

Models of State Privacy Legislation

Twenty-two states have enacted comprehensive consumer privacy laws that create new rights for consumers, impose obligations on businesses that handle consumers' personal data, and create new mechanisms to enforce those laws. Twenty-one of those states adopt the same basic structural model to protect consumer privacy. Some of those states have added greater substantive protections to that basic structural model while other states have adapted the same model to create narrower substantive protections, as reflected in the chart below. In contrast, California adopted a legislative model that creates a new state privacy agency charged with issuing regulations on more than 20 topics, including on issues addressed by statute in other states.

Included | Similar obligation included | More restrictive obligation included | Addressed in rulemaking | Provision expires | Partial exemption

	CA Model	Greater Substantive Protections									Baseline Protections										Narrower Substantive Protections		
	CA	CO	CT	DE	MD	MN	MT	NH	NJ	OR	AL	FL*	IN	KY	NE	OK	TN	TX	VA	IA	RI	UT
CONSUMER RIGHTS																							
Access																							
Correct																							
Delete																							
Portability																							
Opt out of Sale		[1]	[1]		[1]	[1]			[1]	[1]								[1]	[1]				
Opt out of Targeted Advertising																							
Opt out of Profiling			[2]			[2]																	
OBLIGATIONS ON CONTROLLERS																							
Affirmative consent required to process sensitive data																							
Reasonable security measures																							
Data minimization																							
Data protection assessments																							
Prohibition on obtaining consent through "dark patterns"																							
Prohibition on processing data in violation of anti-discrimination laws																							
Mandatory recognition of universal opt-out mechanisms																							
Prohibition on retaliating against consumers who exercise rights																							
Appeals process for consumer rights requests																							
OBLIGATIONS ON PROCESSORS																							
Specific obligations on processors, including to process data pursuant to a contract																							
Duty of confidentiality																							
Requirement to delete or return all personal data at the end of services																							
Provide necessary information to the controller for data protection assessments																							

* Florida's coverage thresholds are higher than those in other state privacy laws and apply to a more limited set of companies.

[1] Additional limits on selling certain sensitive data.

[2] Expanded profiling rights.

Last Revised May 2026

Included | Similar obligation included | More restrictive obligation included | Addressed in rulemaking | Provision expires | Partial exemption

	CA Model	Greater Substantive Protections									Baseline Protections									Narrower Substantive Protections		
	CA	CO	CT	DE	MD	MN	MT	NH	NJ	OR	AL	FL*	IN	KY	NE	OK	TN	TX	VA	IA	RI	UT
SCOPE OF LAW																						
Excludes employees		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Applies to nonprofits, in addition to businesses		■		▨	▨	▨	▨		■													
ENFORCEMENT																						
No private right of action for privacy violations	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Attorney General enforcement	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
New state agency created to enforce law	■																					
Agency rulemaking required	■	■							■			■										
Right to Cure	▨ expired 1/1/23	▨ expired 1/1/25[3]	▨ expired 12/31/24[3]	▨ expired 12/31/25	▨ expires 4/1/27	▨ expired 1/31/26	▨ expired 10/1/25	▨ expired 12/31/25	▨ expires 7/1/26	▨ expired 1/1/26	■		■	■	■	■	■	■	■	■		■
EFFECTIVE DATE																						
Effective Date	1/1/20 (CCPA)	7/1/23	7/1/23	1/1/25	10/1/25	7/31/25	10/1/24	1/1/25	1/15/25	7/1/24	5/1/27	7/1/24	1/1/26	1/1/26	1/1/25	1/1/27	7/1/25	7/1/24	1/1/23	1/1/25	1/1/26	12/31/23

* Florida's coverage thresholds are higher than those in other state privacy laws and apply to a more limited set of companies.

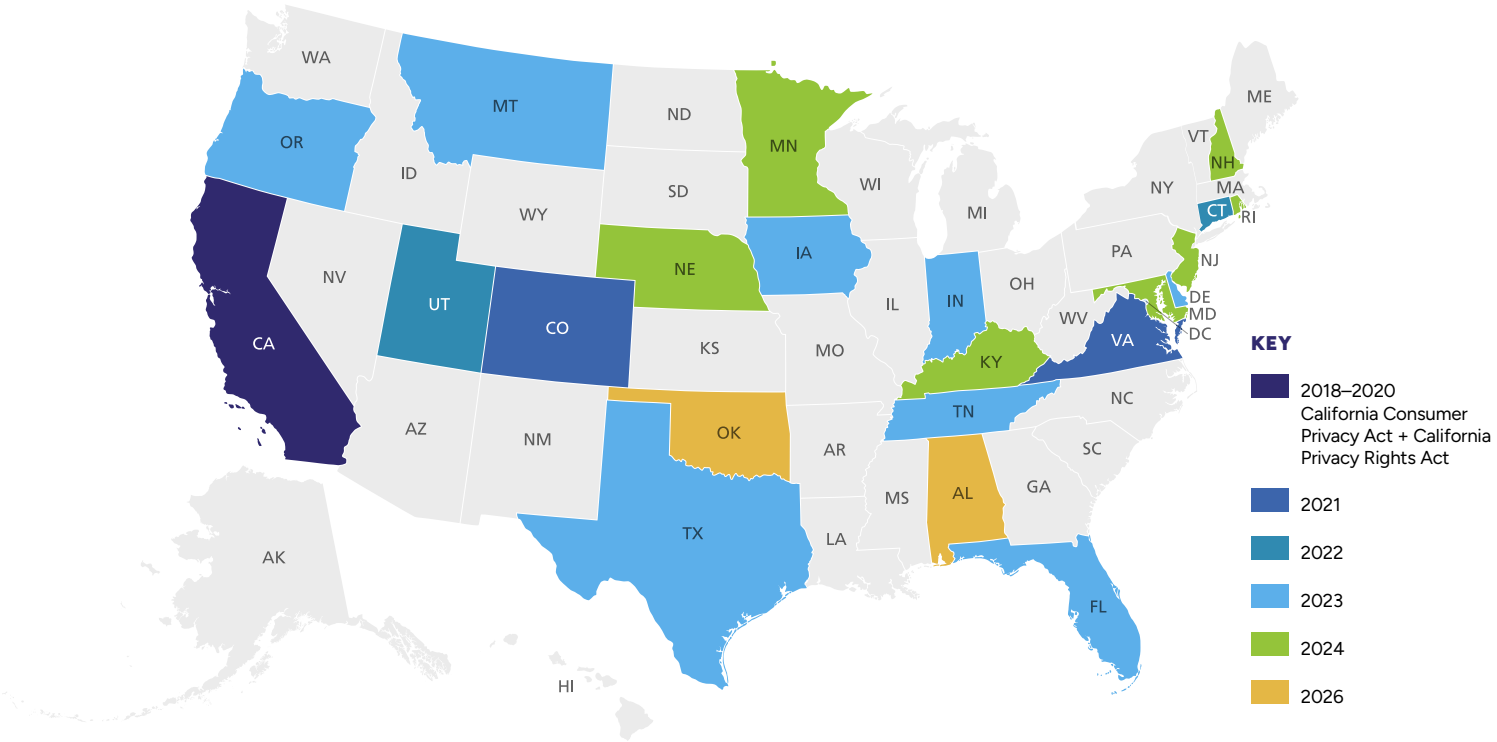
[3] Limited right to cure violations of child data obligations expired on 12/31/25 (in CT) and 12/31/25 (in CO).

AMENDMENTS			
CA	**2025** (fines) effective 6/30/25 **2024** (opt out rights, funds, neural data, health, personal information) effective 1/1/25 **2020** (exceptions and deidentified data) effective 9/25/20, (Prop. 24) effective 1/1/23 **2018** (clarifying changes) effective 9/23/18	MT	**2025** (broad) effective 10/1/25
CO	**2025** (sensitive data) effective 10/1/25 **2024** (neural data) effective 8/6/24, (biometrics) effective 7/1/25, (children) effective 10/1/25	NH	**2024** (rights, notices) effective 1/1/25
CT	**2025** (broad) effective 7/1/26 **2023** (children, health) effective 7/1/23 to 10/1/24	NJ	**2026** (exceptions) effective 1/1/26
KY	**2026** (automatic content recognition) effective 7/1/27 **2025** (profiling) effective 1/1/26	OR	**2025** (sensitive data and kids) effective 1/1/26
MD	**2026** (government use of data) effective 10/1/26 **2026** (immigration) effective 7/1/26	TX	**2025** (AI) effective 1/1/26
		UT	**2026** (motor vehicle manufacturers) effective 1/1/27 **2025** (rights, social media) effective 7/1/26 **2024** (AI) effective 5/1/24
		VA	**2026** (geolocation data) effective 7/1/26 **2025** (social media) effective 1/1/26 **2024** (children) effective 1/1/25

Business Software Alliance

Federal Privacy Legislation Can Build on State Privacy Laws

Twenty-two states have enacted their own privacy laws, but there remains no uniform federal law to safeguard consumers' personal data nationwide. A federal privacy law would bring consistency to existing protections, create broad and long-lasting privacy safeguards for consumers, and advance US leadership.



Congress can build on the work of states and adopt a federal privacy law that: (1) provides consumers rights over their personal data, (2) requires companies to handle personal data responsibly, and (3) adopts a strong, consistent approach to enforcement.

Consumer Rights

A federal privacy law should give consumers important rights over their personal data, including to:

- Access, correct, delete, and port their personal data
- Opt out of:
  - sale,
  - targeted advertising, and
  - certain types of profiling

Obligations on Businesses

A federal privacy law should require companies that handle consumers' personal data to do so responsibly, including to:

- Obtain consent for processing sensitive data
- Adopt reasonable security measures
- Require impact assessments for specific activities

It should also reflect the different roles and responsibilities of controllers and processors.

Strong Enforcement

A federal privacy law should be enforced by federal and state agencies working together.

- The Federal Trade Commission has a long history of addressing consumer privacy.
- Allowing state attorneys general to enforce the law adds 50+ enforcement agencies.

How Can Federal Privacy Legislation Build on State Privacy Laws?

Twenty-one of the 22 states with consumer privacy laws use the same structural model to protect consumer privacy. While states adapt this model by adding and removing substantive protections, these laws create a common framework that Congress can build on to create a uniform, nationwide privacy law.

CONGRESS CAN BUILD ON THE WORK OF STATES AND ADOPT A FEDERAL PRIVACY LAW THAT:

Provides consumers rights over their personal data,

Requires companies to handle personal data responsibly, and

Adopts a strong, consistent approach to enforcement.

Consumer Rights

All 22 state privacy laws create new rights for consumers in their personal data. These include:

- **Right to access personal data:** 22 states
- **Right to correct personal data:** 21 states
- **Right to delete personal data:** 22 states
- **Right to data portability:** 22 states
- **Right to opt out of sale:** 22 states
- **Right to opt out of targeted advertising:** 21 states
- **Right to opt out of certain types of profiling:** 19 states

Obligations on Businesses

All 22 state privacy laws create obligations for businesses to handle consumers' personal data responsibly. All 22 also reflect the fundamental distinction between controllers, which are the companies that decide when and why to collect a consumer's personal data, and processors, which handle that personal data on behalf of another company and pursuant to their instructions.

State privacy laws assign important—and distinct—obligations to both controllers and processors, based on their different roles.

CONTROLLERS MUST:

- **Obtain consent to process sensitive data:** 18 states
- **Adopt reasonable security measures:** 22 states
- **Conduct data protection assessments for certain activities:** 18 states
- **Recognize universal opt out mechanisms:** 11 states
- **Not retaliate against consumers who exercise their rights:** 22 states

PROCESSORS MUST:

- **Process data pursuant to a contract:** 22 states
- **Be subject to a duty of confidentiality:** 22 states
- **Delete or return all data at the end of services:** 20 states
- **Provide information a controller needs to conduct data protection assessments:** 17 states

Notably, state privacy laws focus on *consumer* privacy. Twenty-one states expressly exclude employees.

Enforcement

All 22 laws create a role for the state's attorney general to enforce the privacy law. The laws have:

- **No private right of action for privacy violations:** 22 states
- **Right to cure violations:** 21 states (10 sunset)
- **Rulemaking required:** 4 states
- **New state agency created to enforce law:** 1 state

For more information comparing state privacy laws, see BSA's Models of State Privacy Legislation.

Business Software Alliance

Controllers and Processors: A Longstanding Distinction in Privacy

Modern privacy laws have coalesced around core principles that underpin longstanding privacy frameworks. For example, leading data protection laws globally incorporate principles of notice, access, and correction. They also identify appropriate obligations for organizations in fulfilling these rights, making important distinctions between companies that decide how and why to process personal data, which act as **controllers** of that data, and companies that process the data on behalf of others, which act as **processors** of such data. Privacy and data protection laws worldwide also assign different obligations to these different types of entities, reflecting their different roles in handling consumers' personal data.

The concepts of controllers and processors have existed for more than forty years. These roles are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework, and ISO 27701.

The History of Controllers and Processors

1980: OECD PRIVACY GUIDELINES

The OECD Privacy Guidelines launched the modern wave of privacy laws, building on earlier efforts including a 1973 report by the US Department of Health, Education and Welfare that examined privacy challenges posed by computerized data processing and recommended a set of fair information practice principles.[1]

The OECD Guidelines, adopted in 1980, define a "**data controller**" as the entity "competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf."[2]

Comments to the 1980 Guidelines recognize "[t]he term 'data controller' is of vital importance" because it defines the entity "legally competent to decide about the contents and use of data."[3]

1981: COUNCIL OF EUROPE CONVENTION 108

The Council of Europe in 1981 opened for signature the first legally binding international instrument in the data protection field. Convention 108 defined a "**controller of the file**" as the person "competent . . . to decide" the purpose of automated files, as well as "which categories of personal data should be stored and which operations should be applied to them."[4]

1995: EU DATA PROTECTION DIRECTIVE

The 1995 EU Data Protection Directive, which previously formed the basis of privacy laws in EU member countries, separately defined both controllers and processors.[5] **Controllers** were defined as the natural or legal person that "determines the purposes and means of the processing of personal data," while **processors** were defined as a natural or legal person "which processes personal data on behalf of the controller."

2005: APEC PRIVACY FRAMEWORK

The APEC Privacy Framework builds on the OECD Privacy Guidelines and provides guidance on protecting privacy, security, and the flow of data for economies in the APEC region. It was endorsed by APEC in 2005 and updated in 2015. The Framework defines a **controller** as an organization that "controls the collection, holding, processing, use, disclosure, or transfer of personal information," including those instructing others to handle data on their behalf. It does not apply to entities processing data as instructed by another organization.[6]

2011: APEC CROSS-BORDER PRIVACY RULES (CBPR) SYSTEM

All 21 APEC economies endorsed the Cross-Border Privacy Rules (CBPR) System in 2011, creating a government-backed voluntary system designed to implement the APEC Privacy Framework.[7] The CBPR system is limited to **data controllers**. In 2015, APEC created a separate Privacy Recognition for Processors ("PRP") System to help controllers identify qualified and accountable **processors**.[8]

2016: EU GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation replaced the 1995 Directive, maintaining the definition of **controller** as the entity that "determines the purposes and means" of processing personal data, and the definition of **processor** as the entity that "processes personal data on behalf of the controller."[9] It was adopted in 2016 and took effect in 2018.

2018: COUNCIL OF EUROPE MODERNIZED CONVENTION 108

Convention 108 was modernized in 2018, revising the definition of **controller** and adding a definition of processor. A controller is the entity with "decision-making power with respect to data processing."[10] A **processor** "processes personal data on behalf of the controller."[11]

2019: ISO 27701

The International Organization for Standardization published ISO 27701 in 2019, creating the first international standard for privacy information management. ISO 27701 allocates obligations to implement privacy controls based on whether organizations are controllers or processors. It recognizes that a **controller** determines "the purposes and means of processing"[12] while **processors** should ensure that personal data processed on behalf of a customer is "only processed for the purposes expressed in the documented instructions of the customer."[13]

2025: US STATE PRIVACY LAWS

In the United States, 20 states have enacted comprehensive consumer privacy laws. All of these laws distinguish between **controllers** or businesses that determine the purpose and means of processing, and **processors** or service providers that handle personal information on behalf of the controller or business.

According to a March 2021 report, **more than 84%** of countries responding to an OECD questionnaire define "data controller" in their privacy legislation.[14]

Controllers and Processors: A Distinction Adopted Around the World

Privacy laws worldwide draw from longstanding privacy frameworks, recognizing the distinction between controllers and processors and assigning different responsibilities to these different entities based on their different roles in processing personal data. The chart below identifies some of the countries with national privacy or data protection laws that reflect the roles of controllers and processors.

JURISDICTION	CONTROLLER	PROCESSOR
Brazil[15]	**Controller:** A "natural person or legal entity . . . *in charge of making the decisions* regarding the processing of personal data."	**Processor:** A "natural person or legal entity . . . that processes personal data in the name of the controller."
Cayman Islands[16]	**Data Controller:** A "person who, alone or jointly with others *determines the purposes, conditions and manner* in which any personal data are, or are to be, processed …."	**Data Processor:** Any person "who processes personal data *on behalf of* a data controller but, for the avoidance of doubt, does not include an employee of the data controller."
European Union[17]	**Controller:** A natural or legal person that "alone, or jointly with others, *determines the purposes and means of processing* personal data…."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."
Faroe Islands[18]	**Controller:** A natural or legal person that "alone or jointly with others, *determines the purposes and means of the processing* of personal data."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."
Hong Kong[19]	**Data User:** A person who "either alone or jointly or in common with other persons, *controls the collection, holding, processing or use of the data.*"	**Data Processor:** A "person who: (a) Processes personal data *on behalf of* another person; and (b) *Does not process the data for any of the person's own purposes.*"
Kosovo[20]	**Data Controller:** A natural or legal person that "alone or jointly with others, *determines purposes and means of personal data processing.*"	**Data Processor:** A natural or legal person that "processes personal data for and *on behalf of* the data controller."
Malaysia[21]	**Data Controller:** A person "who either alone or jointly or in common with other persons processes any personal data or *has control over or authorizes* the processing of any personal data, but *does not include a data processor.*"	**Data Processor:** A person "who processes the personal data solely *on behalf of* the data user, and *does not process the personal data for any of his own purposes.*"
Mexico[22]	**Data Controller:** An individual or private legal entity "*that decides on the processing* of personal data."	**Data Processor:** The individual or legal entity that "alone or jointly with others, processes personal data *on behalf of* the data controller."
Philippines[23]	**Personal Information Controller:** A person or organization "*who controls the collection, holding, processing or use of personal information*, including a person or organization *who instructs another person or organization* to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes a person or organization who performs such functions as instructed by another person or organization."	**Personal Information Processor:** A natural or juridical person "to whom a personal information controller may *outsource* the processing of personal data pertaining to a data subject."
Qatar[24]	**Controller:** A natural or legal person "who, whether acting individually or jointly with others, *determines how Personal Data may be processed and determines the purpose(s)* of any such processing…."	**Processor:** A natural or legal person "who processes Personal Data for the Controller."
Singapore[25]	**Organisation:** Any individual, company, association or body of persons, corporate or unincorporated, whether or not: (a) formed or recognized under the law of Singapore or (b) resident, or having an office or a place of business, in Singapore.	**Data Intermediary:** An organisation "which processes personal data *on behalf of another organisation* but does not include an employee of that other organisation."

JURISDICTION	CONTROLLER	PROCESSOR
South Africa[26]	**Responsible Party:** A public or private body or any other person that "alone or in conjunction with others, *determines the purpose of and means for processing* personal information."	**Operator:** A person who "processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party."
Thailand[27]	**Data Controller:** A person or juristic person "*having the power and duties to make decisions* regarding the collection, use, or disclosure of the Personal Data."	**Data Processor:** A person or juristic person who "operates in relation to the collection, use, or disclosure of Personal Data *pursuant to the orders given by or on behalf of the Data Controller*."
Turkey[28]	**Data Controller:** A natural or legal person "who *determines the purposes and means of processing* personal data."	**Data Processor:** A natural or legal person "who processes personal data *on behalf of* the data controller upon its authorization."
Ukraine[29]	**Personal Data Owner:** A natural or legal person who "*determines the purpose of personal data processing, the composition of this data and the procedures for its processing.*"	**Personal Data Manager:** A natural or legal person who is "granted the right by the personal data owner or by law to process this data *on behalf of* the owner."
United Kingdom[30]	**Controller:** A natural or legal person that "alone or jointly with others, *determines the purposes and means* of the processing of personal data."	**Processor:** A natural or legal person that "processes personal data *on behalf of* the controller."

Endnotes

1 Dept. of Health, Educ., & Welfare, Records, Computers, and the Rights of Citizens (1973), https://aspe.hhs.gov/reports/records-computers-rights-citizens.

2 OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, § 1(a) (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

3 *Id.* at Explanatory Memorandum, § IIB, para. 40.

4 Council of Europe, Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, art. 2(d), Jan. 28, 1981, ETS No. 108, https://rm.coe.int/1680078b37.

5 Directive 95/46/EC, art. 2(d)-(e), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML.

6 APEC, APEC Privacy Framework (2015), § II.10, https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf.

7 *See* APEC, 2011 Leaders' Declaration, https://www.apec.org/meeting-papers/leaders-declarations/2011/2011_aelm; http://cbprs.org/privacy-in-apec-region/.

8 *See* APEC Privacy Recognition for Processors ("PRP") Purpose and Background, https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf.

9 EU General Data Protection Regulation, art. 4(7)-(8), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

10 Council of Europe, Modernised Convention for the Protection of Individuals With Regard to the Processing of Personal Data, art. 2(d), May 17-18, 2018, ETS No. 108, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

11 *Id.* at art. 2(f).

12 Int'l Org. for Standardization, International Standard ISO/IEC 27701 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines 1, 4-5, 29-55 (2019).

13 *Id.* at 43.

14 OECD, Report on the Recommendation of the Council Concerning Guidelines Governing Protection of Privacy and Transborder Flows of Personal Data, 16 (2021), https://www.oecd.org/sti/ieconomy/privacy.htm.

15 Law No. 13,709, Aug. 14, 2018, art. 5 VI-VII (as amended by Law No. 13,853, July 8, 2019, Official Journal of the Union [D.O.U.] July 9, 2019), https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

16 Data Protection Act (2021), § 2, https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf.

17 EU General Data Protection Regulation, art. 4, 2016 O.J. (L 119), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC.

18 Act on the Protection of Personal Data No. 80 (2020), §§ 6(6)-(7), https://dat.cdn.fo/media/opccxh1q/act-on-the-protection-of-personal-data-data-protection-act-act-no-80-on-the-7-june-2020.pdf?s=LA6IqXBchs1Ryn1Kp9h3KSPuFog.

19 Personal Data (Privacy) Ordinance, (1996) Cap. 486, § 2(1), https://www.elegislation.gov.hk/hk/cap486. See https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.

20 Law No. 06/L-082 on Protection of Personal Data (2019), art. 3, §§ 1.11, 1.14, https://www.dataguidance.com/sites/default/files/law_no._06_l_-082_on_protection_of_personal_data_0.pdf.

21 Act 709 Personal Data Protection Act 2010, § 4, https://ilo.org/dyn/natlex/docs/ELECTRONIC/89542/102901/F1991107148/MYS89542%202016.pdf as amended in 2024, https://www.pdp.gov.my/ppdpv1/wp-content/uploads/2024/11/Act-A1727.pdf.

22 Federal Law on Protection of Personal Data Held by Private Parties, art. 3, XIV & IX, Official Gazette July 5, 2010, https://www.dataguidance.com/legal-research/federal-law-protection-personal-data-held.

23 Data Privacy Act of 2012, Rep. Act No. 10173, §§ 3(h)-(i) (Aug. 15, 2012), https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/#:~:text=11.,transparency%2C%20legitimate%20purpose%20and%20proportionality.

24 Law No. 13 of 2016 Personal Data Privacy Protection, art. 1, https://www.dataguidance.com/sites/default/files/law_no._13_of_2016_on_protecting_personal_data_privacy_-_english.pdf.

25 Personal Data Protection Act 2012, as amended, § 2(1), https://sso.agc.gov.sg/Act/PDPA2012.

26 Protection of Personal Information Act, 2013, Act 4 of 2013, Chap. 1, https://popia.co.za/.

27 Personal Data Protection Act, B.E. 2562 (2019), § 6, https://cyrilla.org/es/entity/sl9175g71u?page=1.

28 Law on Protection of Personal Data No. 6698 (2016), art. 3(g), 3(i), https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.

29 Law of Ukraine on Personal Data Protection (2010) (as amended), art. 2, 4(4), https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.

30 UK General Data Protection Regulation 2016 (as amended), c. 1, art. 4(7)-(8), https://www.legislation.gov.uk/eur/2016/679. *See also* UK Information Commissioner's Office, Who Does the UK GDPR Apply To?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/.

internet for growth

June 1, 2026

The Honorable Brett Guthrie
Chairman
House Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

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

Dear Chairman Guthrie, Ranking Member Pallone, and Members of the Committee:

On behalf of Internet for Growth, a nationwide coalition of small businesses, entrepreneurs, and creators, I write to express our support for the Committee's efforts to advance a workable national consumer privacy framework that protects Americans while preserving the affordable digital tools small businesses use to grow and compete in today's economy.

Our members rely on digital advertising, marketing, social media, e-commerce, streaming, email, and related online services to interact with customers and build their businesses. Meanwhile, consumers increasingly expect meaningful control over their information, including rights to access, correct, delete, and opt out of certain data uses, while also valuing the affordability, convenience, and personalization enabled by responsible data-driven services online. We support legislation that establishes a more consistent national framework for transparency, accountability, and consumer rights while reducing uncertainty for businesses operating across state lines.

Our coalition's "Main Street's Digital Mandate" voter research found overwhelming bipartisan recognition that digital tools are now essential infrastructure for small businesses and consumers alike. Ninety-four percent of voters said digital tools are important for small business survival, while 89% said they would be concerned if small businesses had to cut back or close because of rising advertising costs. Eighty-five percent said restrictions on digital advertising could reduce access to free online content and services, and 90% said regulation would likely lead small businesses to raise prices.

Across our coalition, members consistently describe digital advertising and online services as essential tools for reaching customers and competing in markets that were once difficult or impossible to access, including a New Jersey digital marketing and creative services firm that grew from early social media and digital campaign work into a business serving public, nonprofit, and private-sector clients, and a baker and floral designer in Los Angeles who built her business and customer base through online platforms and social media. Federal legislation is particularly important as some states have begun to consider lowering applicability thresholds in ways that will increasingly require smaller businesses to devote substantial resources to complex multi-state privacy compliance.

Strong privacy protections and a strong digital economy are not mutually exclusive. We believe the SECURE Data Act represents a constructive foundation for broader bipartisan engagement on a workable national privacy framework, and we appreciate the Committee's leadership on this important issue.

Sincerely,

Brendan Thomas

Brendan Thomas

Executive Director
Internet for Growth

CC: House Energy & Commerce Committee

About Internet for Growth

Internet for Growth is a nationwide coalition of small businesses, entrepreneurs, and creators who depend on digital advertising, media, and marketing to reach customers, grow revenue, and create jobs. We advocate for policies that preserve access to affordable, data-driven tools powering economic growth in every corner of the country.

Reason Foundation Letter on H.R. 8413, SECURE Data Act

Prepared for: Members of the
Subcommittee on Commerce, Manufacturing and Trade
Committee on Energy and Commerce
U.S. House of Representatives

Prepared by: Richard Sill, Technology Policy Analyst
Reason Foundation

Date: June 1, 2026

Dear Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee,

Thank you for holding a markup on H.R. 8413, the SECURE Data Act, legislation intended to establish a comprehensive national privacy and data security framework. Reason Foundation would like to offer our perspective to the committee on this important legislation. Thank you in advance for your consideration.

Reason Foundation's Technology Policy Project provides pro bono consulting to public officials and stakeholders to help design and implement artificial intelligence (AI), digital free speech, data security and privacy, child online safety, and tech industry competition policies. Our team brings practical, market-oriented strategies to help foster innovation, competition, and consumer choice through technology policies that work.

The SECURE Data Act represents a thoughtful step forward addressing a problem that has developed over more than a decade of congressional inaction. State privacy laws have created a fragmented landscape with inconsistent compliance obligations and uneven consumer protections across jurisdictions.[1] By establishing a uniform national framework, the bill would bring needed consistency while preserving the core protections that have emerged across the states.

The bill builds on the familiar architecture of state privacy laws.[2] It provides consumers with baseline protections, including the rights to access, correct, delete, and port personal data. It also gives individuals the ability to opt out of targeted advertising, the sale of personal data, and certain profiling decisions. In addition, it incorporates widely adopted concepts such as opt-in consent for sensitive data, defined roles for controllers and processors, and enforcement by both the Federal Trade Commission

[1] Comments of Will Rinehart to the House Committee on Energy and Commerce's Request for Information on a Data Privacy and Security Framework (Apr. 14, 2025), https://www.aei.org/research-products/testimony/the-fragmented-privacy-landscape/.
[2] Jordan Francis, "Anatomy of a State Comprehensive Privacy Law," Future of Privacy Forum (Dec. 2025), https://fpf.org/wp-content/uploads/2025/12/FPF-Anatomy-of-a-State-Comprehensive-Privacy-Law-Report.pdf.

and state attorneys general. The legislation reflects the direction many states have already been moving rather than introducing a fundamentally new model.

At the same time, the SECURE Data Act addresses a central weakness in the current system. Its preemption provision would replace overlapping state regimes with a single national standard.[3] For businesses, this would create a clearer and more predictable compliance environment. For consumers, it would ensure consistent protections regardless of where they live. This kind of harmonization reflects a more limited government approach by reducing duplication, compliance burdens, and regulatory overlap while improving the effectiveness of privacy protections by eliminating conflicting requirements.

The SECURE Data Act adopts a more restrained and workable enforcement model than prior federal proposals, such as the American Data Privacy and Protection Act (ADPPA)[4] and the American Privacy Rights Act (APRA),[5] by not including a private right of action. This approach is preferable because it would rely on enforcement by expert agencies rather than opening the door to large volumes of private lawsuits, which can increase costs, create legal uncertainty, and divert resources away from compliance. By emphasizing agency oversight, the bill promotes consistent enforcement while reducing the risk of excessive and fragmented litigation.

Overall, we believe the SECURE Data Act takes the core elements of the existing state privacy consensus and places them within a unified federal framework. With its emphasis on standardizing privacy law and providing regulatory clarity, the bill offers a pragmatic path forward in an area that has long lacked federal coordination.

Sincerely,

Richard Sill
Technology Policy Analyst
Reason Foundation

[3] Daniel Castro et al., "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation (Jan. 2022), https://www.congress.gov/118/meeting/house/115376/documents/HHRG-118-IF17-20230301-SD021.pdf.
[4] American Data Privacy and Protection Act, H.R. 8152, 117th Cong., 2nd Sess. (2022).
[5] American Privacy Rights Act of 2024, H.R. 8818, 118th Cong., 2nd Sess. (2024).

The Nonprofit Alliance (TNPA) is proud to endorse the SECURE Data Act (H.R. 8413). Since its founding, TNPA has supported the development of a comprehensive national data privacy framework that provides clarity, consistency, and strong protections for consumers, nonprofits, and the businesses that support charitable organizations.

TNPA believes the current patchwork of state privacy laws creates significant operational and compliance challenges for nonprofit organizations and their service providers. Navigating varying state requirements requires substantial investments in legal review, compliance systems, and staff capacity — resources that would otherwise support mission-driven programs, charitable outreach, and services in communities across the country. For charitable organizations that depend on responsible donor engagement and data stewardship, regulatory certainty is especially important.

The SECURE Data Act includes several priorities supported by TNPA, including a strong federal preemption standard to reduce conflicting state requirements, an exemption for nonprofit organizations, and the absence of a private right of action. These provisions help ensure that charitable resources are directed toward serving communities and beneficiaries rather than duplicative compliance costs and litigation exposure.

We especially appreciate the work of the House Energy and Commerce Data Privacy Working Group, including Chairman Guthrie, Representative Joyce, and their staff, for engaging stakeholders throughout this process. TNPA submitted a formal response in April 2025 outlining the nonprofit sector's priorities and appreciates the thoughtful consultation process conducted over many months with nonprofit organizations, commercial partners, and other stakeholders.

Nonprofits rely on the trust of donors, members, volunteers, and beneficiaries. Establishing a clear and workable national privacy framework helps organizations protect that trust while allowing them to continue serving communities effectively and efficiently. TNPA joins a wide range of nonprofit, business, and association stakeholders that have called for a uniform national privacy standard.

We look forward to continuing to engage as the bill advances through the regular order process.

About The Nonprofit Alliance: *The Nonprofit Alliance (TNPA) is a national association representing approximately 400 nonprofit organizations and mission-driven service providers committed to protecting and strengthening the nonprofit sector. TNPA members represent diverse charitable missions, including health, human services, veterans, faith-based organizations, conservation, and children's services. TNPA also includes trusted commercial partners that help nonprofits with fundraising, compliance, technology, and donor engagement. Since 2018, TNPA has served as a unifying voice to promote, protect, and strengthen the nonprofit sector.*

Business Roundtable

A National Data Privacy Standard Is Good for American Businesses and Consumers

A single national standard works

Business Roundtable supports a clear nationwide data privacy standard that protects consumers no matter where in the U.S. they live or travel, makes data practices easier to understand and reduces the uncertainty of a 50-state patchwork for employers, innovators and businesses.

1
National Standard

Data privacy is a top priority of American voters of every background

86% of Americans believe data privacy should be governed by federal law.

73% of Americans support federal preemption, including large majorities across party lines.

Only **14%** of Americans think that data privacy should only be regulated by the states.

The SECURE Data Act strikes the right balance

Provides consumers with meaningful control over their information

Draws on effective, proven state privacy frameworks developed on a bipartisan basis

Fully preempts state laws, ending a confusing and harmful patchwork approach

Allows innovative and beneficial uses of data by businesses while protecting consumers

Empowers the FTC to enforce consumer privacy law

Ensures enforcement role for state attorneys general

Stand with American Businesses, Innovators and Consumers
Support the SECURE Data Act

May, 2026

american advertising federation
louisville

Dear Representative Guthrie:

We write to express support for the Committee's recently released bill, H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Act), on comprehensive privacy legislation. The SECURE Act reflects a thoughtful and balanced approach to safeguarding individuals' privacy interests while preserving the benefits enjoyed by millions of Americans in their role as consumers in the data-driven economy.

American Advertising Federation-Louisville is the unifying voice for advertising in Central and Western Kentucky. We represent all aspects of the advertising industry, including clients, advertising agencies, the media, and suppliers. AAF-Louisville is one of over 150 local advertising federations across the country affiliated with the American Advertising Federation.

The SECURE Act rightly acknowledges the essential role that responsible, data-driven advertising plays in sustaining local businesses and the communities they serve. Small and mid-sized businesses depend on the ability to use data to reach customers effectively and compete with larger competitors. For example, a local retailer may rely on targeted outreach to inform customers nationwide about seasonal products, such as fall offerings like apple cider-scented candles. Additionally, a restaurant may use data to identify potential tourists to their city and engage them with tailored promotions, such as a "buy one, get one 50% off" entree offer during their visit.

These are not abstract practices, and businesses use data in practical, everyday tools that drive foot traffic, customer loyalty, and local economic growth at a scale that would not be possible without data. Preserving the ability to engage in these activities, with clear and reasonable guardrails, is critical, to ensure that businesses retain the tools they need to remain competitive, innovate, and continue to be pillars of vibrant local economies. In turn, consumers benefit from greater choice, improved services, and a more dynamic marketplace.

We appreciate the Committee's leadership on this important issue and encourage you to support and advance the SECURE Act.

Sincerely,

AAF-Louisville

Statement for the Record
Thomas A. Schatz
President
Council for Citizens Against Government Waste

Before the
House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives

June 3, 2026

Examining Legislation To Establish A Federal Comprehensive Privacy and Data Security Law

Mr. Chairman and members of the committee, my name is Thomas A. Schatz, and I am the president of the Council for Citizens Against Government Waste (CCAGW). I appreciate the opportunity to provide testimony for the record for the June 3, 2026, hearing, "Examining Legislation To Establish A Federal Comprehensive Privacy and Data Security Law."

CCAGW is a private, nonpartisan, nonprofit organization representing more than one million members and supporters nationwide. Founded in 1984, CCAGW is the lobbying arm of Citizens Against Government Waste (CAGW), which was established to follow up on the implementation of the recommendations of President Ronald Reagan's Private Sector Survey on Cost Control, also known as the Grace Commission, to eliminate waste, fraud, abuse, mismanagement and inefficiency in government.

As the subcommittee considers data privacy legislation, CCAGW encourages members to support the SECURE Data Act and move it through the subcommittee as introduced. The bill in its current form meets all the criteria for a comprehensive data privacy framework at the national level, providing much needed certainty and consistency for consumers and the companies that hold their information. The legislation is thorough in its protection of consumer rights, while also co-opting the best examples from the states, allowing the bill to preempt state laws without exceptions.

CCAGW has been promoting policies related to privacy since 2001, and beginning in 2016, began calling for a comprehensive national consumer data privacy framework to be enacted.

Data privacy is something that most people want but then do not pay attention to until their information is compromised. During the 117th Congress the House of Representatives considered but did not pass legislation that would have provided a national framework for consumers and businesses on how data should be protected. H.R. 8152, the American Data Privacy and Protection Act (ADPPA), would have created a single set of federal rules.[1] However, that legislation was not without its flaws.

[1] American Data Privacy and Protection Act, H.R. 8152, 117th Congress, Second Session (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152.

CCAGW's July 19, 2022, letter to the House Energy and Commerce Committee was critical of the bill's exemptions from preemption of several existing state laws, the inclusion of a private right of action, and an expansion of the Federal Trade Commission's authority, considering that agency's abandonment of the consumer welfare standard during the last administration and its abject disregard for the economic impact of its proceedings on privacy, non-disclosure agreements, and merger applications.[2]

CCAGW had hoped that the 118th Congress would renew the effort to enact a data privacy bill but following hearings before the House Energy and Commerce Subcommittee on Innovation, Data, and Commerce on March 1, 2023, and on April 27, 2023, to discuss data privacy, a comprehensive consumer data privacy bill like ADPPA was not introduced before Congress adjourned.[3]

The creation of the House Data Privacy Working Group in the 119th Congress led to the April 23, 2026, introduction of H.R. 8413, the SECURE Data Act, by House Energy and Commerce Vice Chairman John Joyce (R-Pa.), who leads the Data Privacy Working Group.[4]

The SECURE Data Act includes provisions that have been previously adopted by states like Colorado, Connecticut, Kentucky and Virginia rather than states that have more restrictive and burdensome requirements. Currently, there are 21 states that have comprehensive data privacy laws, with another bill in Louisiana waiting for Gov. Jeff Landry's signature.

The pre-emption provision of H.R. 8413 makes federal law supersede state laws, eliminating the patchwork of state laws that could cost businesses up to $1 trillion over 10 years and continue to cause confusion for consumers.[5] H.R. 8413 also does not include a private right of action, leaving enforcement of the bill to the Federal Trade Commission and the state attorneys general and saving taxpayers and businesses from endless and potentially frivolous litigation.

H.R. 8413 also includes several provisions from the six principles for date privacy submitted by CAGW in 2018 to the National Telecommunications and Information Administration: 1) A National Privacy Framework; 2) Consumer Choice and Control; 3) Transparency; 4) Data

---

[2] Council for Citizens Against Government Waste, "Letter to House Energy and Commerce Committee Regrading H.R. 8152, the American Data Privacy and Protection Act," July 19, 2022, https://ccagw.org/legislative-affairs/ccagw-sends-letter-to-house-energy-and-commerce-committee-regarding-h-r-8152-the-american-data-privacy-and-protection-act/.

[3] House Committee on Energy and Commerce, "Innovation, Data, and Commerce Subcommittee Hearing: "Promoting U.S. Innovation and Individual Liberty through a National Standard for Data Privacy," March 1, 2023, https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-promoting-u-s-innovation-and-individual-liberty-through-a-national-standard-for-data-privacy; "Innovation, Data, and Commerce Subcommittee Hearing: "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information," https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information.

[4] SECURE Data Act, H.R. 8413, 119th Congress, Second Session (2026), https://www.congress.gov/bill/119th-congress/house-bill/8413.

[5] Daniel Castro, Luke Dascoli, Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology & Innovation Foundation (ITIF), January 24, 2022, https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

Minimization and Contextuality; 5) Flexibility; and 6) Data Security and Breach Notification.[6] In addition, many of the core provisions of the bill have already been enacted by state legislatures across the country as noted in a May 15, 2026 ITIF article, including de-identified and public data; consumer choice for data use; consumer data rights; protection from automated decisions; reasonable data security; general notice and transparency; data minimization; purpose limitation; no private lawsuits; and opportunity to cure.[7]

CCAGW urges the subcommittee to adopt the SECURE Data Act as currently written and introduced and reject efforts to undo the national framework like eliminating state law pre-emption and adding a private right of action . The bill provides strong protections of consumer data privacy. H.R. 8413 would eliminate confusion and provide a standard that consumers and the companies that hold their information can rely on regardless of where they live or work. For these reasons, I strongly urge your support for this bill.

[6] Thomas Schatz, "Comments to NTIA on Developing the Administration's Approach to Consumer Privacy," Citizens Against Government Waste, November 8, 2018, https://ccagw.org/comments-to-ntia-on-developing-the-administrations-approach-to-consumer-privacy/.

[7] Ash Johnson, " State Privacy Laws Show the SECURE Data Act's Merits and Political Appeal," ITIF, May 15, 2026, https://itif.org/publications/2026/05/15/state-privacy-laws-show-the-secure-data-acts-merits-and-political-appeal.

TECHNET
THE VOICE OF AMERICAN INNOVATION

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

June 2, 2026

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade
House Committee on Energy
and Commerce
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, and Trade
House Committee on Energy
and Commerce
Washington, D.C. 20515

Re: SECURE Data Act

Dear Chairman Bilirakis and Ranking Member Schakowsky:

On behalf of TechNet, I write in advance of the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade's June 3, 2026, legislative hearing, "Establishing a Federal Data Privacy Law," to express our support for H.R. 8413, the *Securing and Establishing Consumer Uniform Rights and Enforcement Over Data Act* ("*SECURE Data Act*").

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes over 100 dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over five million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet has long supported a comprehensive federal privacy framework that protects consumers, strengthens trust in the digital economy, and provides clear and consistent rules of the road for businesses operating across the United States. By providing individuals with meaningful rights regarding the collection, use, and sharing of their data, the legislation reflects the principle that consumers should have confidence in how their information is handled and the ability to make informed choices about its use. These protections are increasingly important as technology continues to evolve and data-driven services become a larger part of everyday life.

Operating under the current patchwork of state privacy laws is increasingly unsustainable for consumers and businesses alike. Americans deserve strong privacy protections regardless of where they live, while businesses need a predictable national framework that enables innovation and investment. The *SECURE Data Act* represents

an important step toward achieving these goals and demonstrates that strong consumer protections and continued innovation need not be competing priorities.

Federal privacy legislation can only succeed if it meaningfully replaces, rather than adds to, the growing patchwork of state privacy requirements. Without strong preemption of state laws, consumers will continue to face inconsistent rights and protections, while businesses will remain subject to a complex web of overlapping and sometimes conflicting legal obligations. A single national standard would provide regulatory certainty, facilitate compliance, and ensure that privacy protections evolve through a coherent federal framework rather than fifty different approaches. Strong preemption does not mean less accountability; it means that consumers, businesses, and regulators all operate under the same clear rules and enforcement framework.

As Congress continues to evaluate federal privacy legislation, TechNet remains committed to working with policymakers on both sides of the aisle to develop durable, technology-neutral frameworks that protect consumers, support innovation, and reinforce American leadership in the digital economy. We note and are encouraged by the dialogue surrounding these issues and hope this week's legislative hearing contributes to a bipartisan process that results in meaningful privacy protections for all Americans.

Sincerely,

Linda Moore
President and CEO

1301 Pennsylvania Avenue, NW
Suite 400
Washington, D.C. 20004
P :: 202.783.8700
F :: 202.783.8750
W:: AdvaMed.org

AdvaMed Statement for the Record: Subcommittee on Commerce, Manufacturing, and Trade Hearing "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law"

June 3, 2026

AdvaMed appreciates the Subcommittee on Commerce, Manufacturing, and Trade holding this hearing on developing a national data privacy and data security standard. AdvaMed, the Medtech Association, is the world's largest trade association representing medical technology innovators. Our mission is ensuring greater access to lifesaving medical technologies, treatments, and diagnostic tools for patients and providers. AdvaMed's member companies range from large multinational manufacturers to small startups developing the next generation of technologies improving patient outcomes, expanding access to care, and strengthening the health care system.

The use of personal health data in the medical technology sector differs significantly from the use of personal information in many other sectors of the economy. Medical technologies rely on health data to support patient treatment, monitor device performance and safety, improve product effectiveness, conduct research, comply with regulatory requirements, and advance the development of new therapies and diagnostics. These activities often occur within complex regulatory environments that already include extensive privacy, security, safety, and quality requirements, and AdvaMed members take seriously their obligation to ensure the appropriate use and privacy of personal health data in their care.

AdvaMed strongly supports protecting individuals' privacy and maintaining robust safeguards for personal information. Patients and consumers must have confidence their information is handled responsibly, securely, and transparently. At the same time, policymakers should recognize the collection, use, and sharing of health-related information often serves critical purposes fundamental to patient care, medical innovation, public health, product safety, and regulatory compliance. AdvaMed therefore supports efforts to establish a consistent national framework that provides meaningful privacy protections while accounting for the unique characteristics of health care and medical technology. These purposes include patient treatment and related activities, product monitoring and safety activities, research, product development and improvement, regulatory and payer compliance, participation in value-based care arrangements, and other activities that support public health and improved patient outcomes. A well-designed federal framework can enhance consumer trust, reduce regulatory fragmentation, and promote innovation benefitting patients.

AdvaMed appreciates the Committee's leadership on this important issue. We look forward to continuing to work with members of the Energy and Commerce Committee and other stakeholders to advance a comprehensive federal privacy and data security framework that strengthens consumer trust while supporting patient care, medical innovation, and the continued development of life-saving technologies.

Attachment – AdvaMed U.S. Federal Privacy Legislation Policy Recommendations

June 2, 2026

The Honorable Gus Bilirakis
Chairman, Subcommittee on Commerce, Manufacturing and Trade
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member, Subcommittee on Commerce, Manufacturing and Trade
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schkowsky:

On behalf of the members of the National Multifamily Housing Council (NMHC), the National Apartment Association (NAA), and the Real Estate Technology and Transformation Center (RETTC), we thank you for convening the hearing entitled "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law." Thank you for the opportunity to share insight on the need of a long-overdue federal data privacy standard that protects consumers and American businesses, including rental housing firms and our technology partners.

Rental housing owners and operators, and their service providers, rely heavily on sensitive personal data about rental applicants, residents and employees to run their day-to-day business. Given the sensitivity of the information that rental housing operators rely on and the ever-expanding cyber threat landscape we face, our industry has placed a high priority on strengthening defenses against vulnerabilities and protecting sensitive data and consumer privacy. In fact, rental housing firms are committing tremendous resources to this cause.

The relationship between a resident and the housing provider may span years and involve the collection and use of various types of information. Consumer data contained in resident screening reports and held by housing operators and their service providers is crucial in accounting for rental history, tenure and payment data, which make up an important part of a resident's profile. These data points can also serve as tools to improve a resident's housing opportunities in the future.

SECURE Data Act and the GUARD Financial Data Act

We commend the leadership for releasing the companion bills, the SECURE Data Act and the GUARD Financial Data Act, to continue the longstanding conversation about creating a national data privacy standard. NMHC, NAA, and RETTC strongly support the establishment of a comprehensive federal data privacy framework. Further, we believe the creation of this framework is more urgent than ever as it must precede the imposition of any additional regulations on the use and development of AI technologies.

As our organizations have consistently said in the past, a fragmented regulatory approach in data management, security and technology risks stifling innovation and increasing compliance costs. This ultimately undermines the benefits these systems and technologies offer to renters and housing providers alike. As policymakers consider how federal financial regulators are supporting the use of new technologies, we urge you to support a balanced framework that safeguards innovation. The

existing legal landscape in housing already offers strong protections, and any new regulations should build on that foundation without undermining technological progress.

Rental Housing Data Privacy Priorities

As the Subcommittee on Commerce, Manufacturing and Trade considers the legislation, NMHC, NAA, and RETTC would like to take the opportunity to highlight our priorities in this space. We believe that these priorities should serve as a starting point for any other federal data privacy and security measure:

- **Federal Preemption:** A clear federal preemption is necessary to provide clarity for rental housing firms and their technology partners. The current patchwork of state laws creates a significant compliance burden for rental housing firms and leaves consumers vulnerable to mistakes and unintended consequences. This is particularly true given the constantly evolving nature of state data privacy and security laws. As our organizations have consistently said in the past, a fragmented regulatory approach in data management, security and technology risks stifling innovation and increasing compliance costs. This ultimately undermines the benefits these systems and technologies offer to renters and housing providers alike.
- **Flexible and Scalable National Standard:** A data privacy and protection standard will benefit from taking into consideration the data collected and the size of the company. NMHC, NAA, and RETTC believe that any enforcement regime must provide for a flexible and scalable national standard for data security, privacy and breach notification that takes into account the needs and available resources of small businesses, as well as large firms and the sensitivity of the data in question.
- **The Ability to Continue to Perform Essential Business Functions:** Entities may have an essential business need to engage with consumer data and should be mindful of data minimization. Rental housing firms must maintain the right to collect, use and retain sensitive information necessary for business operations. This is particularly important to ensure the safety and security of residents and employees through prospective resident screening while also ensuring compliance with regulatory requirements such as reporting under the Fair Housing Act.
- **Reasonable Time Frame to Respond to Consumers:** Any data privacy and protection enforcement should provide for adequate time for rental housing firms to respond to inquiries. Given the complexities of verifying any privacy or protection request and responding accurately, rental housing firms need sufficient time to carry out any request, with the option for an extension if necessary.
- **Third Party/Assignment of Financial and Legal Liability:** There is an important distinction between covered entities, service providers and third parties. We believe that service providers must hold responsibility for their own security and privacy safeguards. Liability for any third-party/service provider security lapse or privacy violation must not shift to rental housing firms or other primary consumer relationship holders. Often, businesses of all sizes are faced with the reality of being forced to accept boilerplate contractual language when contracting with a service provider or supplier. For example, while one large company may have the market share and financial leverage to negotiate and demand certain security protocols, the vast majority of American businesses do not. The responsibility for overseeing a third party's data security program and consumer privacy safeguards should remain with the party that is collecting, using and retaining sensitive information—not with rental housing companies or other firms that rely on third-party services.

- **Clarity in Regulatory Authority:** To provide clarity and certainty to apartment firms, a single federal agency should be responsible for data privacy and protection rulemaking and enforcement. Further, Congress should establish the scope of any federal regulator's authority. Entities that must comply with new data privacy and security regulations will need education, flexibility and the right to cure in the event of a possible violation.
- **Preserving Innovation:** As policymakers seek to determine how to best regulate AI and other emerging technologies, they should be cautious not to stifle innovation or inhibit the development of tech-driven, pro-consumer solutions. That said, it is also imperative for Congress to protect consumers, businesses, and national security from the growing threat of cybercrime. The most effective way to achieve both of these goals is through focusing on the development of a robust, flexible, and scalable federal data security and privacy standard.

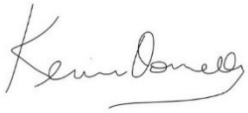
Conclusion

We appreciate the policymakers' focus on fostering innovation and ensuring a coherent, forward-looking approach to financial policy. We urge the subcommittee to continue their bipartisan work to achieve federal policy that protects consumers, allows business uses of AI and other emerging technologies to continue and avoid a duplicative and complex regulation that could inadvertently drive housing costs higher. NMHC, NAA, and RETTC stand ready to work with policymakers to support responsible innovation that improves efficiency, resilience, and affordability in rental housing.

Sincerely,

Sharon Wilson Géno
President
National Multifamily Housing Council

Bob Pinnegar
President and Chief Executive Officer
National Apartment Association



Kevin Donnelly
Executive Director and Chief Advocacy Officer
Real Estate Technology & Transformation Center

June 2, 2026

The Honorable Gus Bilirakis, Chairman
The Honorable Russ Fulcher, Vice Chairman
The Honorable Jan Schakowsky, Ranking Member
U.S. House of Representatives
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, DC 20515

Re: Statement for the Record in Support of H.R. 8413, the SECURE Data Act

Dear Chairman Bilirakis, Vice Chairman Fulcher, and Ranking Member Schakowsky:

On behalf of the Association of National Advertisers ("ANA"), we write to express support for H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act ("SECURE Data Act" or "Bill"). We appreciate that you are holding a hearing on this important legislation and encourage the Subcommittee on Commerce, Manufacturing, and Trade to favorably advance the Bill.

The ANA is the definitive voice of the marketing industry. Since 1910, we have set and advanced the agenda for marketing transformation, connecting over 1,600 member companies to an influential global network, insights and resources that drive growth. Our members represent 20,000 brands and $400 billion in annual marketing investment. Through industry-leading research, the CMO Growth Council, and our proprietary Growth Agenda and Practices, the ANA empowers marketers to shape the future of marketing and create lasting impact for their organizations and the industry. ANA members have long implemented and advocated for consumer privacy protections including as a founding member of Privacy for America—a broad coalition of trade associations and companies working with Congress to pass comprehensive privacy legislation.

The SECURE Data Act is a commonsense bill that builds upon consensus approaches from state consumer privacy laws to establish key privacy protections for all U.S. consumers, regardless of their state of residence. The Bill's approach is the result of months of the House Privacy Working Group's thoughtful consultation with hundreds of stakeholders to develop a clear federal framework that would create critical consumer privacy protections while preserving responsible data uses that support the modern economy. Specifically, the Bill would:

- **Establish a uniform set of rights for all U.S. consumers that mirrors state privacy laws.** Nearly half of all U.S. states have enacted consumer privacy laws that give consumers certain rights over personal data processed by businesses. These states have coalesced around a set of core rights that should be available to consumers, including rights to access, correct, delete, and port data, as well as the ability to opt-out of certain data uses such as the use of data for targeted advertising, data sales, profiling, or certain automated decisions. The SECURE Data Act would build upon the important bipartisan work already done by states to extend these key rights to all U.S. consumers, ensuring that individuals nationwide can exercise the same rights no matter where they live.

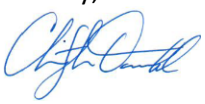
- **Preserve routine and responsible data uses that unlock immense benefits for consumers and the economy.** Existing state consumer privacy laws uniformly preserve beneficial data uses—including data-driven advertising—that help businesses to spur innovation, develop new beneficial products and services, and support robust competition in today's fast-growing online marketplace. Advertising is a cornerstone of the U.S. economy, with one study estimating that, in 2024 alone, advertising supported more than 29 million jobs and $10.4 trillion in annual sales—more than 20 percent of the U.S. Gross Domestic Product ("GDP").[1] Small and start-up businesses especially rely upon data-driven advertising to connect with audiences and compete effectively with more established market players.[2] Consumers similarly reap significant benefits from the vast amount of free and low-cost information and content subsidized by online advertising, with one study estimating that each consumer derives more than $30,000 in annual value through the low-cost information and services made available on the ad-supported Internet.[3] Similar to existing state privacy laws, the SECURE Data Act would continue to permit these responsible data uses that fuel competition and the modern U.S. economy.

- **Support robust enforcement mechanisms, including industry self-regulatory efforts that protect consumers.** The SECURE Data Act would provide for strong enforcement by coupling FTC enforcement authority with state attorney general enforcement that aligns with the enforcement approach adopted by state consumer privacy laws. Moreover, the Bill would recognize that industry self-regulation already provides important protections for consumers. The ANA has long championed industry self-regulation related to privacy, including through enforcement of the *ANA Ethics Code of Marketing Best Practices* ("Ethics Code").[4] The SECURE Data Act would help support ongoing industry efforts by allowing approved codes of conduct to create a rebuttable presumption of compliance, which could help standardize compliance across the market and focus enforcement on bad actors.

* * *

Thank you for your consideration of our views as you contemplate ways to best provide privacy protections to consumers while preserving the beneficial data uses that fuel the modern economy. Please do not hesitate to contact us with any questions regarding this submission.

Sincerely,



Christopher Oswald
Group Executive Vice President & Head
of Law, Ethics, and Government Relations
ANA

CC: Members, U.S. House of Representatives Committee on Energy and Commerce

---

[1] *See* S&P GLOBAL, THE ECONOMIC IMPACT OF ADVERTISING ON THE US ECONOMY 2024-2029 at 4 (Aug. 2025) [hereinafter "ECONOMIC IMPACT OF ADVERTISING"], located here

[2] *See* J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 8-9 (2022), located here.

[3] *See id.* at 2.

[4] ANA, Ethics Code of Marketing Best Practices, 6 (last modified April 30, 2025), available here; *see also* ANA, ANA Ethics Compliance Report: January-December 2025, 49, available here (describing enforcement actions).

U.S. House Energy and Commerce

Subcommittee on Commerce, Manufacturing, and Trade

"Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law"

June 3, 2026

Statement of the American Property Casualty Insurance Association

The American Property Casualty Insurance Association (APCIA) respectfully submits this statement to the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade Subcommittee hearing entitled, "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law." APCIA's more than 1200 member companies write more than 67 percent of all the property casualty insurance in the U.S. with the common mission to advance private competitive insurance markets to protect consumers, businesses, and communities.

Insurers[1] operate within a complex and evolving landscape of federal and state privacy laws and regulations, which carefully balance consumers' increasing demand for convenience and personalized service with legitimate privacy concerns. Privacy protections for insurance consumers are already well-established under the Gramm-Leach-Bliley Act (GLBA)[2] and a series of National Association of Insurance Commissioners (NAIC) model laws, including the Insurance Data Security Model Law,[3] the Insurance Information and Privacy Protection Model Act,[4] and the Privacy of Consumer Financial and Health Information Regulation.[5]

[1] In this context, "insurers" refers not only to insurance carriers but also to reinsurers, managing general agents, third-party administrators, and other entities that play a critical role in the insurance ecosystem and are subject to the same robust regulatory framework.

[2] *Gramm-Leach-Bliley Act*, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6827).

[3] *Insurance Data Security Model Law*, Nat'l Ass'n of Ins. Comm'rs, Model Law No. 668 (2017) (enacted in 26 states).

[4] *Insurance Information and Privacy Protection Model Act*, Nat'l Ass'n of Ins. Comm'rs, Model Law No. 670 (1980) (as amended) (enacted in 17 states).

[5] *Privacy of Consumer Financial and Health Information Regulation*, Nat'l Ass'n of Ins. Comm'rs, Model Regulation No. 672 (2000) (as amended) (adopted in some form by 41 states, with variations in certain jurisdictions).

Enforced by state insurance regulators, these existing regulations provide a comprehensive and well-structured framework for consumer privacy and data security.

Unlike industries where consumer data is monetized, insurers primarily use personal information to assess risk, pay claims, and provide essential protection to individuals, businesses, and communities. Given the highly sensitive nature of insurance data, insurers invest millions annually in cybersecurity programs and information security measures to safeguard policyholder information. Any federal privacy framework must recognize these distinctions and ensure that insurers are not subject to the same rules as industries that use consumer data for unrelated commercial purposes.

As the Subcommittee considers federal privacy legislation, any changes impacting insurers should be addressed within the existing GLBA framework, rather than through an entirely new regulatory regime. To that end, our preferred outcome is a comprehensive, preemptive federal law that aligns with existing federal and state insurance-sector-specific laws, excludes a private right of action, and leaves enforcement to state regulators with insurance expertise. **APCIA supports H.R. 8413, the SECURE Data Act because it includes a full GLBA exemption for the insurance sector to ensure that state insurance regulators remain the primary enforcement authority for insurers. More importantly, APCIA supports the SECURE Data Act because it does not include a private right of action. We also support H.R. 8398, the GUARD Financial Data Act, which updates GLBA and is compatible with SECURE Data Act.**

Ultimately, any federal privacy framework impacting insurers should incorporate four key elements: strong federal preemption; workable compliance requirements; enforcement by state insurance regulators; above all, no private right of action.

I. Roles and Responsibilities

A federal comprehensive data privacy and security law should appropriately distinguish between the different roles entities play in handling consumer data. However, it should not require one party (e.g., a controller) to impose contractual obligations on another party (e.g., a processor) as a means of enforcement. Doing so would inappropriately deputize controllers as enforcers of federal law and create unnecessary compliance burdens. Instead, each regulated entity should be held directly accountable for meeting its legal obligations, ensuring consistent enforcement and avoiding compliance gaps.

To account for different roles in the digital economy, a federal law should adopt commonly understood definitions of controllers and processors, such as those used in the EU General

Data Protection Regulation (GDPR)[6] and similar U.S. state laws. However, it should avoid incorporating terms of art from state laws, such as "Third Party" or "Contractor" under the California Consumer Privacy Act (CCPA),[7] as these definitions have created confusion and inconsistencies across jurisdictions. Additionally, the distinction between controllers and processors should not impact core data security requirements—all entities handling sensitive personal information should be required to implement appropriate security safeguards, regardless of their role in the data lifecycle. The primary differences in obligations should be in areas such as notice and consumer data deletion requirements, where the entity with the direct consumer relationship has a greater responsibility.

Furthermore, any federal privacy law should align with existing, well-established sector-specific privacy frameworks, such as the GLBA and the NAIC Insurance Data Security Model Law. Financial institutions, including insurers, already operate under rigorous data protection standards that have been refined through decades of regulatory oversight. Moreover, to avoid conflicting obligations, a federal law should fully preempt state-level privacy laws within its scope.

Additionally, liability and enforcement should follow a clear and predictable structure. Entities should be responsible only for the parties with which they have direct contractual relationships. A controller should not bear sole responsibility for the actions of distant third-party processors. Instead, each processor should be accountable for its own subcontractors, with indemnification requirements ensuring that non-breaching parties are protected in the event of a data breach caused by another party.

A federal privacy law should also take a risk-based approach by recognizing the practical realities of different business sizes and data-handling capacities. Smaller organizations should not face the same regulatory burden as large entities, while larger organizations should not be disproportionately impacted by impractical compliance obligations. A scaled approach will ensure strong consumer protections without imposing unnecessary burdens on businesses of varying sizes and operational complexities.

By ensuring clear, role-based obligations, alignment with existing privacy laws, strong federal preemption, and a risk-based approach, a federal privacy framework can enhance consumer protections while ensuring practical and effective compliance across industries.

---

[6] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, 2016 O.J. (L 119) 1.

[7] *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (2020).

II. Personal Information, Transparency, and Consumer Rights

Any federal privacy law should establish clear, workable standards that protect consumer privacy while allowing businesses, including insurers, to operate efficiently. An effective framework must balance strong consumer protections with the operational realities of highly regulated industries like insurance. It should align with existing federal privacy laws, such as GLBA, to prevent conflicting or duplicative compliance obligations. To that end, it should exclude employment and business-to-business (B2B) data, and take a risk-based approach that prioritizes operational needs while providing meaningful consumer protections. At the same time, the law should be structured to avoid unintended consequences that could impose inconsistent or broader privacy mandates on HR functions. It should also preserve the ability of financial institutions to market their products and services to consumers with appropriate safeguards.

Definitions of personal and sensitive information should be carefully crafted to avoid unnecessary complexity and ensure consistency with existing federal privacy laws. Privacy disclosures should be clear, practical, and designed to provide consumers with meaningful information without creating undue compliance burdens. While heightened protections may be appropriate for certain categories of sensitive data, any additional requirements should reflect the risk associated with misuse and should not interfere with essential insurance functions such as underwriting, claims handling, and fraud prevention.

III. Existing Privacy Frameworks & Protections

The growing patchwork of U.S. privacy laws creates significant challenges for businesses, especially those operating across multiple states. Varying definitions, exemptions, and enforcement mechanisms result in inconsistent consumer rights and costly compliance burdens. For example, state breach notification laws differ in defining protected data, notification triggers, and reporting requirements. Insurers face added complexity due to the previously mentioned insurance specific NAIC model laws, which sometimes conflict with broader state regulations.

A similar trend is emerging with state-level comprehensive privacy laws, many modeled after the CCPA. Currently, around 19 states[8] have enacted privacy legislation, yet their treatment of financial institutions and GLBA-regulated data varies significantly. Some states exempt all

[8] California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Montana, Maine, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia.

financial institutions subject to GLBA,[9] others extend exemptions to affiliates,[10] which is the approach APCIA supports. Some limit exemptions strictly to GLBA-covered data.[11] Other states have taken an alternative approach by exempting GLBA-covered data while also providing a broader exemption for the insurance industry.[12] State laws also vary with respect to the inclusion of employee and B2B data, further complicating compliance. Additionally, laws such as Washington's *My Health My Data Act*[13] and *Illinois' Biometric Information Privacy Act*[14] introduce further regulatory divergence, making it increasingly difficult for businesses to maintain a uniform approach to data privacy.

The growing complexity of state-by-state privacy regulations underscores the need for a single, harmonized federal privacy framework. However, to be effective, federal legislation must fully preempt state laws within its scope. Without strong federal preemption, a federal law would fail to resolve inconsistencies and instead add another layer of regulation on top of an already burdensome compliance landscape. A true national standard should establish clear, uniform rules that apply consistently across all states, giving consumers a predictable understanding of their rights and businesses a practical compliance structure.

Another critical issue is the lack of differentiation across industries in many state privacy laws. Most privacy laws target the data practices of the technology and advertising sectors, yet insurers, who use personal data primarily to assess risk and serve policyholders, are often swept into these broad regulatory schemes. A federal privacy law must recognize these distinctions, ensuring that insurers are not subject to the same regulations as industries that monetize consumer data.

For the insurance sector, privacy protections are already well-established through the GLBA and states' adoption of NAIC model laws, which are enforced by state insurance regulators and have been refined through years of regulatory oversight and market conduct examinations. Insurers must also comply with the Fair Credit Reporting Act (FCRA),[15] which governs the use of consumer reports in underwriting and claims, ensuring transparency and consumer rights in adverse decisions. Insurance regulation has historically been delegated to the states through the McCarran-Ferguson Act,[16] a principle reaffirmed by GLBA and the

[9] For example, the *Texas Data Privacy and Security Act*, Tex. Bus. & Com. Code §§ 541.001–.303 (2024).
[10] For example, the *Utah Consumer Privacy Act*, Utah Code Ann. §§ 13-61-101 to -404 (2023).
[11] For example, the *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199 (2020).
[12] For example, the *Minnesota Consumer Data Privacy Act*, Minn. Stat. §§ 325M.01–.09 (2024) and the *Oregon Consumer Privacy Act,* Or. Rev. Stat. §§ 646A.570–.589 (2024).
[13] *My Health My Data Act*, Wash. Rev. Code §§ 19.373.010–19.373.900 (2023).
[14] *Biometric Information Privacy Act*, 740 Ill. Comp. Stat. 14/1 et seq. (2008).
[15] *Fair Credit Reporting Act*, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified at 15 U.S.C. §§ 1681–1681x).
[16] *McCarran-Ferguson Act,* 15 U.S.C. §§ 1011–1015 (2018).

Dodd-Frank Act.[17] Any federal privacy law should align with this established regulatory framework rather than impose redundant or conflicting requirements.

If Congress moves forward with a broad federal privacy and security law, it must include a full GLBA exemption to ensure that state insurance regulators remain the primary enforcement authority. A full GLBA exemption means the law would not apply to financial institutions or their affiliates governed by the GLBA, nor to personal data that is collected, processed, sold, or disclosed in compliance with the GLBA. Additionally, any federal privacy and security framework should incorporate four key elements to provide clarity, consistency, and effective oversight. First, there should be no private right of action, as litigation-driven enforcement increases costs for businesses and consumers while creating regulatory uncertainty. Second, strong federal preemption is essential, ensuring that a uniform national standard overrides state-level privacy laws to prevent further regulatory fragmentation. Third, compliance requirements must be clear, practical, and tailored to different industries, rather than imposing a rigid, one-size-fits-all approach. Finally, enforcement should remain with state insurance regulators, who possess the expertise and established authority to oversee insurers' compliance with privacy and security laws effectively.

A federal privacy framework should simplify compliance, reduce inconsistencies, and provide clarity for consumers and businesses. However, for the insurance industry, the GLBA framework is already working effectively, and any new law should not disrupt this well-established system. Federal legislation should harmonize privacy protections across industries while preserving the unique, state-based regulatory framework for insurers.

IV. Data Security

A foundational goal of any federal comprehensive privacy law should be to enhance data security for consumers while ensuring a consistent and effective regulatory framework. As with data privacy, a federal approach to data security for insurers should have: no private right of action; strong federal preemption; workable requirements; and enforcement for insurers by state insurance regulators.

Insurers have long operated under strict data security requirements, investing millions of dollars annually in robust security programs to safeguard consumer data. To enhance security across all industries, a federal law should require all businesses to implement technical and organizational security measures that are commensurate with their risk, regardless of their size or sector. A risk-based approach ensures that data security

[17] *Dodd-Frank Wall Street Reform and Consumer Protection Act*, Pub. L. No. 111-203, § 502, 124 Stat. 1376, 1580 (2010).

obligations are appropriately scaled—preventing overregulation of small businesses while ensuring that companies handling large volumes of sensitive data maintain stringent protections.

Additionally, there should be clear mechanisms for verifying compliance with federal security requirements. Currently, insurers are often expected to ensure that their partner vendors comply with data security regulations, yet many smaller vendors still lack appropriate controls. Insurers should not be responsible for ensuring the compliance of their business partners; instead, accountability should rest with the entities subject to the regulations.

By establishing a single, national standard for data security, ensuring a risk-based approach to compliance, and reinforcing direct government oversight, a federal privacy and security law can meaningfully improve consumer data security while reducing compliance complexity for businesses.

V. Artificial Intelligence

While artificial intelligence (AI) intersects with privacy and data security, it is a distinct issue that should be addressed separately. AI use by insurers is primarily regulated at the state level and that should remain the case, in that state regulators have a relatively uniform set of standards and guidelines for insurers' use of AI. AI can offer significant benefits for insurance consumers, such as improved risk assessment, better customer experience, and faster claims settlement. To ensure these advantages are not hindered, any federal AI legislation should defer to state insurance regulatory standards, which have already proven effective and allow for the flexibility needed as AI technology evolves.

While AI presents new challenges, it is essential that existing state regulatory standards, such as those governing unfair discrimination, remain in place and are not replaced by new concepts like "bias" that do not align with current insurance codes. AI should be treated as a tool, with existing state insurance laws on ratemaking, underwriting, and claims adjudication continuing to apply, regardless of whether decisions are made by humans or AI.

It is also important to note that state insurance commissioners are already thoroughly addressing AI through the NAIC Model Bulletin on AI.[18] Twenty-three states[19] have adopted it formally and it has become a *de facto* national standard.

The NAIC Bulletin provides comprehensive guidelines for the use of artificial intelligence in the insurance industry, focusing on preventing unfair discrimination, good governance, accountability, and consumer protections. It emphasizes the importance of using AI in compliance with existing laws, ensuring non-discriminatory outcomes, and maintaining data quality and privacy. The NAIC Bulletin encourages innovation while ensuring that AI systems do not compromise consumer protection and regulatory standards. In summary, it is critical to maintain the effective balance established by the NAIC Bulletin after years of expert stakeholder input representing many different perspectives.

VI. Accountability & Enforcement

APCIA supports a single federal agency dedicated to privacy and security to ensure consistent enforcement and minimize conflicting interpretations. However, for insurers, enforcement must remain at the state level, where regulators have deep expertise in insurance practices and established oversight under GLBA, ensuring predictable outcomes, industry expertise, and consumer-focused oversight.

Above all, we emphasize our strong opposition to any private right of action. A private right of action would exacerbate the already overly litigious environment in the United States, imposing significant costs on businesses and consumers alike. It would significantly increase litigation, further burdening businesses, especially small and medium-sized entities, with costly legal defenses and settlements. The U.S. tort system costs businesses and families $529 billion per year—amounting to $4,323 per household—while less than 60 cents of every dollar actually goes toward compensating plaintiffs.[20] Introducing a private right of action into a federal privacy framework would drive up litigation and insurance costs for consumers—without delivering meaningful benefits.

---

[18] *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers*, Nat'l Ass'n of Ins. Comm'rs (2023).

[19] Alaska, Arkansas, Connecticut, Delaware, District of Columbia, Illinois, Iowa, Kentucky, Maryland, Massachusetts, Michigan, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, Oklahoma, Pennsylvania, Rhode Island, Vermont, Virginia, Washington, and West Virginia.

[20] *Costs and Compensation of the U.S. Tort System*, Institute for Legal Reform, US Chamber of Commerce at https://instituteforlegalreform.com/research/costs-and-compensation-of-the-u-s-tort-system/ (adjusted for GDP and population growth).

Additionally, safe harbors, such as encryption, obfuscation, and anonymization, should be incorporated to incentivize compliance, offering rebuttable presumptions of compliance for businesses demonstrating strong data security practices.

Conclusion

The insurance industry has long prioritized consumer privacy and operates under a robust regulatory framework that balances consumer protection with operational efficiency. As the Subcommittee explores federal privacy legislation, APCIA urges that any changes affecting insurers be addressed within the existing GLBA framework, rather than through a new and duplicative regulatory structure. Should the Working Group pursue a broader federal privacy law, a full GLBA exemption for the insurance sector is essential to maintain state insurance regulators as the primary enforcement authority. Ultimately, any federal privacy framework impacting insurers should incorporate four key elements: no private right of action; strong federal preemption; workable compliance requirements; and enforcement by state insurance regulators.

We appreciate this opportunity to provide feedback and look forward to continued collaboration in shaping a practical, effective privacy and security framework that benefits both consumers and the insurance industry.

Thank you,

The American Property Casualty Insurance Association

Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law

JAMES CZERNIAWSKI, Head of Emerging Tech Policy, Consumer Choice Center

Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade

United States House of Representatives

June 3rd, 2026

Dear Chair Bilrakis, Ranking Member Schakowsky, and Members of the Subcommittee:

On behalf of the Consumer Choice Center, we write to thank you for holding this hearing today. Here at the Consumer Choice Center, we have argued on behalf of consumers around the country for a unified national data privacy framework in order to better protect consumers and position businesses to be successful. Any such framework should be crafted in a way that both empowers consumers and allows our country's world-leading dynamic digital economy to continue delivering value to consumers in the goods and services they use every day. We write to express our support for H.R. 8413, the *SECURE Data Act,* introduced by Representative Joyce. We believe this legislation strikes that balance.

Currently, American consumers and businesses alike are forced to navigate a fragmented patchwork of state-level data privacy laws that are confusing for both consumers and businesses and present various challenges. This balkanized approach imposes significant regulatory compliance burdens that disproportionately harm startups and small to medium-sized businesses. In establishing a clear federal threshold with robust preemption, H.R. 8413 makes compliance smoother for all parties and ensures that all Americans are protected by a singular, coherent set of data rights that is not dependent on the state in which a consumer resides.

HR 8413 correctly builds upon some practical components of existing privacy frameworks enacted in some states. In allowing consumers to access, correct, and delete their data, coupled with the ability to opt out of targeted advertising, the legislation puts consumers in the driver's seat. It is an

important step to see all this accomplished without an overly prescriptive mandate that runs the risk of significantly disrupting the digital ecosystem that consumers are interacting with daily, providing access to many low-cost goods and services.

Importantly, HR 8413 correctly avoids allowing for a private right of action. History has shown that private rights of action can lead to a predatory ecosystem fueled by lawyers looking to line their pockets. Any privacy framework legislation should avoid creating an ecosystem that encourages practices that encourage such behavior, as it only takes money away from creators making goods and services that Americans enjoy, all without providing any serious privacy enhancements or actual remedies for consumers.

It is for these reasons that we ask the Subcommittee to advance HR 8413, the SECURE Data Act. We stand ready to be a resource and work with the Subcommittee to ultimately pass a legislative solution so the country can finally have a uniform, pro-consumer privacy framework.

Sincerely,

James Czerniawski

Head of Emerging Technology Policy

Consumer Choice Center

ITI Promoting Innovation Worldwide

June 3, 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
United States House of Representatives
Washington, DC 20515

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

On behalf of the Information Technology Industry Council (ITI), I respectfully submit this letter for the record for the Subcommittee on Commerce, Manufacturing, and Trade's June 3 hearing, "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law." ITI is a global technology trade association representing the companies that design, build, and deliver the AI models, hardware, semiconductors, software, data centers, cloud services, networking solutions, and applications that make up the American technology stack.

Comprehensive federal data privacy and security rules are critical to build American consumer trust online and enable responsible data-driven innovation and economic growth. ITI has been a long-time leading supporter of a unified, preemptive U.S. consumer privacy and security framework that establishes a clear national privacy standard.

ITI welcomes the *SECURE Data Act*, which provides a clear, horizontal U.S. consumer privacy framework building on the bipartisan consensus model for data privacy legislation developed in states across the country. The *SECURE Data Act* rightly draws on the consensus framework established across 21 of the 22 state consumer privacy laws which broadly follow the same risk-based model and structure to take an effective and balanced approach to core privacy law provisions, including by providing common definitions and exemptions, strong consumer rights, and clearly defined controller and processor obligations. Crucially, the *SECURE Data Act* establishes strong data rights and protections for consumers while enabling responsible innovation and U.S. leadership in data security and the development of AI and future technologies.

By expanding on state legislation, Congress can extend tested privacy protection to every American, regardless of which state they live in, and establish a clear national standard that enables businesses

United States
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe
Rue Froissart 95, 1040
Brussels, Belgium
+32 (0)2 321 10 90

info@itic.org
www.itic.org
@iti_techtweets

operating across state lines to build one privacy compliance program, rather than dozens of conflicting ones. ITI applauds the work done by the members of the Energy and Commerce Committee's Privacy Working Group to apply the lessons learned from state privacy laws to the *SECURE Data Act*.

Beyond the core data privacy protections in the *SECURE Data Act,* the bill recognizes the importance of continued American technology leadership globally by formalizing the Commerce Department's long-standing role in advancing cross-border data flows. Cross-border data flows are essential to the functioning of the modern economy and to ensuring that U.S. companies across all sectors can continue to compete and lead globally.

Importantly, the *SECURE Data Act* tasks the Department of Commerce with addressing foreign data localization restrictions, which are becoming increasingly common. These data localization proposals are often aimed at U.S. companies and pose a challenge to the competitiveness of the U.S. technology industry across the world. By strengthening Commerce's role in countering these proposals, the *SECURE Data Act* would help ensure that the U.S. is better positioned to push back against harmful foreign data localization measures and other digital trade barriers. ITI also welcomes the bill's recognition of the Global Cross-Border Privacy Rules System as an important international framework to promote trusted data transfers across jurisdictions.

By helping address foreign data localization requirements and strengthening the Department of Commerce's role in advancing trusted cross-border data flows, the *SECURE Data Act* would help ensure that the U.S. technology stack remains the global default. At the same time, by building on tested, bipartisan state data privacy laws, the bill would strengthen privacy protections for Americans and provide companies with the certainty of a clear nationwide privacy standard. ITI appreciates the significant work done to craft the *SECURE Data Act,* and we look forward to working with Republicans and Democrats in Congress to enact a strong national privacy law.

Sincerely,

John Miller
Executive Vice President of Policy & General Counsel
Information Technology Industry Council (ITI)

NATIONAL ASSOCIATION OF WHOLESALER-DISTRIBUTORS

June 2, 2026

The Honorable Gus Bilirakis
Chairman
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2322 Rayburn House Office Building

The Honorable Jan Schakowsky
Ranking Member
Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2322 Rayburn House Office Building

Dear Chairman Bilirakis and Ranking Member Schakowsky:

The National Association of Wholesaler-Distributors (NAW) is writing to express strong support for provisions included in the *Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act)* which would establish a much-needed single federal privacy standard across the United States.

NAW represents the $8 trillion wholesale distribution industry comprised of employers of all sizes, industry trade associations, partners, and stakeholders spanning all sectors of distribution. Our industry employs over 6 million workers in the United States accounting for approximately 1/3 of the U.S. GDP. There are more than 250,000 wholesale distribution companies that operate across North America, including all 50 states. Wholesaler-distributors rely on a strong surface transportation infrastructure to ensure resilient and efficient supply chains that deliver essential goods throughout the nation.

The SECURE Data Act is an important step to resolve the emerging patchwork of state privacy laws that make compliance costly and difficult. NAW also applauds the inclusion of many of the wholesale distribution industry's data privacy and security priorities, which include:

- Clear definitions and parameters for data controllers, processors and third parties;
- A risk-based approach to AI by creating an opt-out for higher-risk automated decision-making tools;
- A "code of conduct" framework for organizations to demonstrate legal compliance and a 45-day cure period for violations of the law;
- Enforcement authority through federal and state regulators without a private right of action;
- The preemption of state privacy laws, which has led to a patchwork of burdensome compliance requirements for multi-state wholesaler-distributors.

NAW supports the SECURE Data Act and urges lawmakers to advance this bill through the committee process and on the full House of Representatives.

Sincerely,

Brian Wild
Chief Government Relations Officer
National Association of Wholesaler-Distributors

June 1, 2026

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House Committee on Energy & Commerce
2123 Rayburn House Office Building
Washington, DC 20515

Re: H.R. 8413 – SECURE Data Act

Dear Chairman Bilirakis:

On behalf of the National Insurance Crime Bureau (NICB), I write to express our appreciation for the Committee's open and collaborative efforts leading to the introduction of the SECURE Data Act (H.R. 8413). NICB applauds the balance struck by the legislation, which ensures fraud-fighters like NICB can continue in our mission of combating insurance crimes that needlessly raise costs on all Americans.

With an almost 115-year history, NICB is the nation's premier non-profit organization exclusively dedicated to detecting, preventing, and deterring insurance fraud and related crimes through intelligence-driven operations. While NICB provides value to our members through education and subject matter expertise, we also serve a significant public benefit by helping stem the estimated billions of dollars in economic harm that insurance crime causes every year.[1] Key to this work is the ability for industry, regulators, and law enforcement to timely exchange information—pursuant to state reporting obligations—that helps disrupt organized crime and fraud networks.

Consistent with data privacy laws already enacted in 20 states across the country—spanning red and blue states—as well as with Congress's previous comprehensive data privacy legislation,[2] the SECURE Data Act acknowledges NICB's mission and the pro-consumer benefits of protecting the responsible exchange of information to combat insurance fraud, financial exploitation, and related crimes. In this regard, the SECURE Data Act strikes an appropriate and well-established balance to protect both privacy and public safety.

NICB is grateful for the Committee's work to ensure that the SECURE Data Act

[1] According to the Federal Bureau of Investigation, insurance fraud is estimated to reach more than $40 billion per year, costing the average U.S. family between $400 and $700 annually in the form of increased premiums. *See* Insurance Fraud, Federal Bureau of Investigation, *available at* https://www.fbi.gov/stats-services/publications/insurance-fraud.
[2] *See* American Privacy Rights Act of 2024 (H.R. 8818, 118th Congress).

maintains the balance struck by 20 states to date, and we stand ready to provide any additional information.

Please contact me if we can provide any additional information or if you or your staff have any questions.

Respectfully,

Kyle T. McCollum
Vice President
Strategy, Policy, and Government Affairs
National Insurance Crime Bureau

cc: The Honorable Jan Schakowsky
The Honorable Brett Guthrie
The Honorable Frank Pallone

June 2, 2026

The Honorable Brett Guthrie
Chair
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus Bilirakis
Chair
House Energy and Commerce, Commerce, Manufacturing and Trade Subcommittee
2306 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
House Energy and Commerce, Commerce, Manufacturing and Trade Subcommittee
2408 Rayburn House Office Building
Washington, DC 20515

Re: Statement for the Record in Support of H.R. 8413, the SECURE Data Act

Dear Representatives Guthrie, Pallone, Bilirakis, and Schakowsky:

Privacy for America is a coalition of trade organizations and companies representing a broad cross-section of the American economy. Our membership includes entities in the travel, hospitality, media, entertainment, retail, financial services, advertising, data services, and market research industries, as well as many others. We thank you for holding a hearing on H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (hereinafter referred to as the "SECURE Data Act" or "bill"). Privacy for America appreciates the Committee's work to advance a serious, practical, and durable national privacy law. The Committee's work and the bill it developed reflect what consumers, businesses, regulators, and policymakers across the country already understand: Consumers in America need meaningful privacy protections, and Congress must pass a comprehensive national privacy law. We highlight in this letter why Congress should act now to advance the bill.

A national privacy law is urgently needed. Today, privacy protections depend too heavily on where a person lives. Residents of many states already have access to rights to know, access, correct, delete, port, and opt out of certain data practices. But right now, millions of Americans in other states are left without comparable protections. If this framework is working to protect Americans in nearly half of the country, it should be extended to everyone in the country. Privacy should not be dependent on geography, and companies should not be forced to navigate a growing patchwork of overlapping and increasingly inconsistent obligations. A single federal privacy standard gives consumers strong protections and businesses clear rules.

The SECURE Data Act reflects the consensus approach to protecting consumers' privacy that has emerged across the states. Over the past several years, states have enacted comprehensive privacy laws that share a common architecture. Building on the proven foundation established by states, the SECURE Data Act does not start from scratch. Instead, it takes the consensus framework that worked and makes it available nationwide.

The SECURE Data Act recognizes that strong privacy protections and responsible data use are not opposing goals. Data powers essential services consumers rely on every day, including fraud prevention, cybersecurity, customer support, research, analytics, personalization, accessibility, and advertising. A national privacy law should protect consumers from harmful or unexpected uses of data without preventing businesses from providing the services consumers request and expect. That balance is especially important in advertising, which is not merely a business model but a key part of the modern economy. Responsible, data-driven advertising helps businesses of all sizes reach customers, funds low-cost or no-cost online services that consumers value and drives down prices through competitive markets. At a time of growing affordability pressures, Congress should avoid rules that unintentionally increase costs, reduce competition, or make it harder for small and emerging businesses to reach consumers. The SECURE Data Act strikes the right balance by providing meaningful transparency and empowering consumers with opt-out rights while allowing responsible advertising and other vital data practices to continue.

Privacy for America strongly supports the bill's recognition of codes of conduct as an effective method for privacy enforcement. Once Congress passes a law, implementation and enforcement requires more than statutory text; it requires workable implementation standards that can be understood, implemented, audited, and updated as technology evolves. Codes of conduct can translate legal requirements into practical compliance programs, promote accountability across sectors, independently enforce those standards, and help regulators identify bad actors. By providing for independent administration and enforcement, government certification, public-facing commitments, and referral to the FTC or state attorneys general where appropriate, the bill creates an innovative mechanism to improve compliance and strengthen enforcement.

H.R. 8413 would establish the right enforcement model to protect consumers. The bill preserves a central role for state attorneys general, who have long been important privacy and consumer protection enforcers, while adding federal enforcement by the Federal Trade Commission. That combination gives the law both national consistency and state accountability. Just as important, the bill reflects the state consensus against creating a broad private right of action. Privacy law should be enforced by public authorities with expertise, discretion, and accountability and not through endless lawsuits that can produce inconsistent outcomes and abusive litigation, without improving consumer protection.

* * *

The Committee has done the hard work of listening, identifying common ground, and producing a bill that reflects the mainstream of American privacy law. Now Congress should pass it. Privacy for America urges the Committee to advance H.R. 8413 and move comprehensive federal privacy legislation toward enactment.

Sincerely,
Privacy for America

CC: Representative John Joyce, M.D., Vice Chair of the Energy and Commerce Committee
Members, House Commerce, Manufacturing and Trade Subcommittee

June 3, 2026

The Honorable Brett Guthrie
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus Bilirakis
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairmen and Ranking Members:

On behalf of the 21st Century Privacy Coalition ("Coalition"), we write to express our strong support for H.R. 8413, the SECURE Data Act.[1] The Coalition has long advocated for the enactment of a comprehensive national privacy and data security law that creates a holistic framework for the entire online ecosystem based upon the sensitivity of data rather than the type of entity collecting, using, or sharing such data. The SECURE Data Act provides meaningful protections for consumers and certainty for businesses, and is consistent with the approach taken in the majority of states that have enacted comprehensive privacy laws.

The SECURE Data Act establishes a robust set of consumer rights, including the right to access and confirm the processing of personal data, correct inaccuracies, delete personal data, and opt out of processing for targeted advertising and the sale of personal data. The legislation also requires affirmative consent before processing sensitive data, with heightened protections for children under 13 (consistent with the Children's Online Privacy Protection Act) and for teens under 16, including a requirement for verifiable parental consent. These provisions reflect a sensitivity-based consent model that the Coalition believes is appropriate for today's digital economy.

In addition to protecting consumers' privacy rights, the legislation requires controllers to implement reasonable administrative, technical, and physical safeguards appropriate to the volume, sensitivity, and nature of the data they process. This requirement ensures that consumers' information will be protected from the data breaches that unfortunately occur with increasing frequency.

The Coalition particularly supports the SECURE Data Act's preemption provisions. The bill's broad state preemption is warranted because the legislation provides strong protections nationwide for consumers, obviating the need for individual states to adopt such protections. Consumers should enjoy the same protections regardless of where they live, work, or visit, and the existing state patchwork of privacy laws provides inconsistent protections for consumers.

[1] The Coalition is comprised of many of the nation's leading communications companies, and our member-companies have a significant interest in fortifying the trust of consumers in their online experiences and confidence in the privacy and security of their personal information.

H.R. 8413 also rightly preempts the Communications Act and Federal Communications Commission ("FCC") regulations. This provision would effectively displace the outdated FCC regulatory regime, replacing it with the comprehensive, technology-neutral framework established by the SECURE Data Act.

The bill would empower the Federal Trade Commission ("FTC") to enforce privacy protections for the entire online ecosystem. The legislation also recognizes that State Attorneys General can complement FTC enforcement. The bill further includes a right to cure, requiring that the FTC or a State Attorney General provide written notice identifying the specific alleged violation and wait at least 45 days before initiating an action, which will encourage the recipient to remedy the alleged violation quickly.

This legislation represents a thoughtful, comprehensive approach to consumer privacy and data security that would replace the current patchwork of outdated, sector-specific rules—including the FCC's regime—with a modern, uniform national standard. By establishing consistent rules of the road enforced by the FTC and State Attorneys General, the SECURE Data Act will protect consumers and promote innovation.

Sincerely,

/s/
Blanche Lincoln
Co-Chair

/s/
Maureen Ohlhausen
Co-Chair

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004
T 202.778.3200
F 202.331.7487
ahip.org

Statement for Hearing on
"Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law"

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

June 3, 2026

AHIP is the national trade association representing the health insurance industry. AHIP's members provide healthcare coverage, services, and solutions to more than 200 million Americans through public programs such as Medicare and Medicaid, employer-sponsored insurance, and the individual insurance market.

As the Subcommittee turns its focus to advancing federal privacy legislation, AHIP welcomes the opportunity to present the perspective of health plans on the importance of protecting consumer health information. Health plans are committed to maintaining robust privacy and cybersecurity practices that protect their enrollees' personal health information (PHI). As new technologies emerge and the healthcare system continues to evolve, AHIP urges the Subcommittee to consider the points in this statement to help give Americans peace of mind that their PHI is secure.

Health Plans and Fostering Safe, Trusted Access to Health Information
As technology continues to advance – especially considering the rapid growth of artificial intelligence – and health information becomes more available through digital platforms and third-party applications, health plans are strengthening their role in reinforcing consumer confidence and trust while maintaining consumer access to reliable, convenient access to health information. To underscore this commitment, in 2022, AHIP's Board of Directors and Chief Medical Officers released core guiding priorities and a detailed roadmap to further protect the privacy, confidentiality, and security of consumer health information.[1] Central to these guiding priorities is the principle that "**personal health information should be protected no matter who holds the data**."

Information sharing and new tools to improve consumer experience can be used to gain more insights into individual and population health, combat fraud and abuse, and improve administrative efficiency. They can also pose privacy risks that every organization holding health and healthcare data must work together to mitigate. That's why health plans are committed to

[1] https://www.ahip.org/news/press-releases/ahip-outlines-priorities-and-roadmap-for-protecting-privacy-and-security-of-consumer-health-information

strengthening access to PHI through innovative digital technologies, empowering Americans to make informed decisions while protecting their privacy, confidentiality, and security.

AHIP believes a national privacy framework is needed to ensure that healthcare data, no matter who holds it, is subject to robust protections. Today, if a patient requests that a provider or health plan share PHI under the Health Insurance Portability and Accountability Act (HIPAA) with a third-party application, such protections do not apply. For example, such information can then be sold at an individually identifiable level as long as it is noted somewhere in the often lengthy and complicated terms and conditions. Non-HIPAA regulated third-party apps and services that collect, use, disclose, or store individuals' health and health-related information must also be held to the same high privacy and security standards as health plans and providers.

Federal Legislation Recommendations

AHIP urges any federal privacy legislation to fill the substantial gap in the national privacy framework, particularly with respect to heath information that is not subject to the HIPAA Privacy & Security Rules, with a comprehensive solution that avoids a 50-state approach that is cumbersome, costly, and confusing.

Moreover, the HIPAA Privacy & Security Rules already provide highly regulated and robust standards for the confidentiality of protected health information held by health plans and insurers, providers and clearinghouses. Any new privacy law should *supplement* the existing HIPAA framework, *not supplant it*, helping to avoid unnecessary duplication and administrative waste that can drive up costs across the healthcare system. The HIPAA Privacy & Security Rules provide a model that has stood the test of time, evolved as needed, and should remain the governing framework for health plans and healthcare providers – enforced and interpreted by HHS, not the FTC.

AHIP also opposes the establishment of a private right of action in any federal privacy law. A new enforcement mechanism creating a private right of action adds unnecessary costs and confusion to a long-standing, effective, and uniform national system of privacy protections, data security, and consumer notice with respect to health information.

Conclusion

AHIP thanks the Subcommittee for its attention to the importance of developing comprehensive federal consumer data privacy legislation. As Congress considers these issues, AHIP appreciates the opportunity to offer its perspectives on advancing a consistent, national approach that builds on existing enforcement mechanisms, preserves the HIPAA Privacy & Security Rules as the foundation for protecting health information held by plans and providers, strengthens protections for health data not currently covered by HIPAA, and avoids a patchwork of conflicting state laws. AHIP looks forward to continuing to work collaboratively with the Subcommittee to advance practical, balanced policy solutions that protect consumers in a more affordable healthcare system that reduces waste and maximizes value.

Insight

Securing Comprehensive Privacy Reform: The Federal Fix to the Patchwork Problem

NICK KROSSE | JUNE 2, 2026

Executive Summary

- The United States is the only major economy without a comprehensive consumer data privacy law; in the absence of such a federal framework, states have enacted a patchwork of data privacy laws that increase compliance costs for businesses both large and small.
- The SECURE Data Act is the latest congressional proposal to create a comprehensive federal data privacy standard for consumers in every state, while preempting the state patchwork of data privacy laws and creating a mechanism to develop industry-specific codes of conduct backed up by Federal Trade Commission and state attorneys general enforcement.
- While critics argue the bill offers insufficient protections relative to the strongest state privacy laws, the existing state patchwork puts businesses in the position of having to focus on navigating minor differences in state laws rather than protecting privacy; a better approach would be to enact a single federal standard with incentives for industries to adopt stronger codes of conduct backed by government enforcement.

Introduction

In the past decade, as technology increasingly mediates our daily lives, demand for data privacy laws has grown across developed economies. The United States is the only G20 economy without a national privacy law covering every industry. In this gap, 21 states have enacted comprehensive privacy laws, leading to a patchwork of laws that are increasingly costly for businesses to coherently comply with.

In the wake of previous failed attempts to pass a national comprehensive data privacy law, the House Energy and Commerce Committee is currently considering the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act). The bill establishes a federal privacy standard based on existing provisions in state privacy laws, creating a baseline set of rights and expectations for all consumers nationwide. It furthermore preempts state privacy laws and contains innovative provisions allowing the creation and registration of voluntary industry-specific codes of conduct that must meet or exceed the act's requirements.

The bill faces opposition from congressional Democrats and consumer groups, which argue that the framework offers insufficient protections for consumers, excessively preempts state privacy laws, and lacks a private right of action. But the existing state patchwork puts businesses in the position of having to focus on navigating minor differences in state laws rather than protecting privacy. A better approach would be to enact a single federal standard with incentives for industries to adopt stronger codes of conduct backed by government enforcement.

Background

With the growth of the internet and computing in the past few decades, our daily lives have increasingly been mediated through technology. From 2000 to 2025, the percentage of Americans adults reporting that they use the internet grew from 52 percent to 96 percent. In 2025, 91 percent of American adults reported owning a smartphone, up from 35 percent in 2011. The "Internet of Things" (IoT) has connected many everyday household items to the internet as well: In 2024, households and businesses were using 18.5 billion IoT devices worldwide, more than double the 7 billion in use in 2018.

This increase in internet usage and connected devices has also necessitated and allowed for the generation and collection of more consumer data. Often, this data generation and collection benefits consumers. For example, consumer data can reduce search and matching costs for consumers and businesses through targeted advertising. It can also help to prevent fraud, enable faster product innovation, and make goods and services lower-cost, free, or even just available to begin with. But consumers face risks as well, particularly from data breaches, or even data being misused after being acquired legally.

In the wake of a spate of data breaches in the latter part of the past decade, demand for comprehensive privacy laws swept developed economies, starting with the European Union's General Data Protection Regulation (GDPR) internationally and the California Consumer Privacy Act (CCPA) in the United States. At the federal level, several, mostly industry-specific, privacy laws exist that predate the recent push for general privacy laws

covering the entire economy. The most industry-agnostic federal law concerning privacy is the Federal Trade Commission (FTC) Act, which merely forbids companies from engaging in "unfair and deceptive practices" as a general matter. While Congress has considered several proposals for a comprehensive federal privacy law since 2018, no proposal has yet been voted on by either chamber, much less passed.

The Patchwork Problem

In the vacuum created by Congress' inaction, 21 states have enacted comprehensive privacy laws. The first, as mentioned above, was California's CCPA, passed by voters through a ballot initiative in 2018, and subsequently amended by a second ballot initiative in 2020. The CCPA was the first law at the state or federal level to establish general consumer data access, deletion, correction, and collection opt-out rights, alongside a web of data transparency, minimization, security, and monitoring requirements on businesses large and small. The California Consumer Privacy Rights Act, which amended the CCPA, also established a new agency, the California Privacy Protection Agency (CPPA), to enforce the CCPA. The CCPA granted that agency (and before it, the state attorney general) broad rulemaking authority, which has allowed the CPPA to expand the reach of the CCPA even further. Unlike any of its subsequent counterparts in other states, the CCPA also governs employee and business-to-business data and gives consumers a narrow private right-of-action over data breaches.

Beginning with Virginia and Colorado in 2021, several states began passing comprehensive privacy laws based on the "Washington Privacy Act" model. This model abstractly provides the same kinds of rights to consumers and imposes similar obligations on businesses as the CCPA, albeit with important practical differences in these core rights and obligations. No state law based on the Washington Privacy Act model provides a private right of action for consumers, instead relying on enforcement by the respective state's attorney general, and only a few authorize any rulemaking by state agencies. Twenty states ultimately adopted this model, although each state has passed this model with its own variations on the underlying definitions, rights, and obligations.

Two recent state laws based on the Washington Privacy Act model are illustrative of the patchwork problem. Maryland's Online Data and Privacy Act introduces a new data minimization standard that is even stricter than California's and bans the sale of sensitive data even with customer consent. Minnesota's Consumer Data Privacy Act requires that businesses maintain an inventory of data that has been collected and processed. Both laws demonstrate that even while 20 of the 21 states with a comprehensive privacy law has modeled it on similar rights, obligations, and definitions, the insertion or alteration of one provision by a state can dramatically increase compliance costs in terms of money, time, and

risks. Furthermore, it shows that interstate companies can no longer simply comply with the strictest state regime, as different states may have stricter requirements on different margins.

The Federal Fix

Following two failed attempts to pass a comprehensive federal privacy framework over the past two congresses, the House Energy and Commerce Committee is now examining the SECURE Data Act as a potential federal, economy-wide privacy framework. The SECURE Data Act is based on the Washington Privacy Act model used by all but one state with a comprehensive privacy law. It contains provisions covering consumer rights and business obligations that align with provisions enacted by states controlled by both Democrats and Republicans. While it does not contain some of the stricter provisions from versions such as Maryland's or Minnesota's, it goes further than most state laws in other ways. For example, it creates the first registry of "data brokers" (companies that collect personal information from third parties rather than directly from consumers) to make it easier for consumers to exercise rights created under the law. It also raises the age required for obtaining parental consent for processing sensitive data to 16 from the current 13 in the federal Children's Online Privacy Protection Act (COPPA).

The SECURE Data Act also preempts all state comprehensive privacy laws, ensuring one national baseline for all sectors of the economy. Having a single national standard to comply with reduces costs associated with duplication of compliance efforts where state laws vary. This is particularly true for small businesses, which, due to varying applicability thresholds at the state level, may have to comply with privacy laws in states where they do not regularly operate but may have few customers. While critics object that this will leave states without a role in regulating privacy, it empowers attorneys general to enforce the law alongside the FTC, still giving states a critical role in protecting their residents. Furthermore, nearly 30 states covering more than 40 percent of the U.S. population have no comprehensive privacy law; The legislation would give those state attorneys general new tools to protect their citizens.

Additionally, the SECURE Data Act offers an innovative mechanism by which industries can develop their own voluntary codes of conduct to be overseen by independent third parties and submit them to be enforced by the FTC. Companies that adhere to these guidelines will be given a rebuttable presumption that they are not violating the law. But if companies fail to adhere to the guidelines they agreed to, the FTC and state attorneys general can use their enforcement powers under the Act to ensure compliance and obtain relief for consumers.

What constitutes good practices for data collection, security, and privacy is dependent on the context in which the data will be used, which is more likely to vary based on industry-specific use cases rather than geography. For example, the automotive and advertising industries have very different use cases for consumer data: The former is concerned with helping customers diagnose mechanical problems or call emergency services, while the latter connects buyers and sellers more efficiently. Both serve different needs for consumers and need to approach issues of collection and minimization differently. U.S. federal privacy law already reflects this with its current sector-based approach to privacy. Furthermore, the legislation's inclusion of independent third-party overseers as well as the backstop of enforcement through FTC and state attorneys general are both critical to ensure the success of this mechanism. Through this innovative provision, the SECURE Data Act would provide consumers with a consistent baseline of privacy expectations to rely on across the economy while also giving flexibility to different industries to adapt to changing technological and social circumstances.

Critics of the legislation also object to the lack of a private right of action for consumers to bring lawsuits against companies they believe are violating or have violated the act themselves. Yet no existing state comprehensive privacy law has a general private right of action for consumers (as noted above, California has a limited private right of action for data breaches). Furthermore, many of the existing industry-specific federal privacy laws also lack general private rights of action, including those that cover health and financial information (except for credit reports). For those that do, because the actual financial damages individuals experience from privacy violations tend to be relatively small (often not exceeding the low thousands), a significant portion of awards end up being paid out in attorney's fees and other court costs, without any of the general enforcement benefits that FTC or state attorney general suits provide.

Legislative Outlook

The SECURE Data Act is being considered by the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade. While it has been endorsed by Republican leadership on the committee, objections from Democratic leadership on the committee demonstrate that it may face an uphill battle in garnering enough support to pass both chambers of Congress. Regardless of whether it succeeds where previous attempts have failed, the underlying principles it contains are essential components of any future federal privacy law. Privacy concerns transcend geographic constraints and instead are driven more by the context in which the data will be used. The SECURE Data Act fixes the web of compliance created by the state patchwork and replaces it with a baseline that all consumers can expect across the economy, and gives industries,

small businesses, and federal and state enforcers the tools to develop more robust protections for consumers based in actual data use cases.

TAXPAYERS PROTECTION ALLIANCE

June 2, 2026

The Honorable Brett Guthrie
Chairman
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone, Jr.
Ranking Member
House Committee on Energy and Commerce
2323 Rayburn House Office Building
Washington, DC 20515

Dear Chair Guthrie, Ranking Member Pallone, and members of the Committee,

The Taxpayers Protection Alliance (TPA) is a non-profit, non-partisan organization dedicated to advocating responsible and transparent government policies that prioritize growth, prosperity, and liberty. On behalf of taxpayers whom we represent across the nation, we write to encourage the Committee on Energy and Commerce to remain committed to the well-crafted provisions of the SECURE Data Act[1] as the bill receives a hearing on Wednesday, June 3,[2] and continues through the process of becoming law.

The SECURE Data Act is a worthy proposal to begin the process of negotiation and, ultimately, enactment of a federal data privacy standard. In the modern digital economy—which transcends state and, often, national borders—a single federal framework is a crucial step to ensure businesses and consumers have the clarity and consistency needed for a flourishing digital economy.

Preserving Preemption

America's state-based—so-called "patchwork"—approach has caused an explosion of varying, and sometimes conflicting, privacy standards with which businesses must comply. This exposes businesses to significant regulatory risks and ballooning compliance costs while creating even more confusion among users about what rights they hold over their data. While TPA is a strong advocate of federalism, data privacy and the digital economy present clear issues of interstate commerce in which the federal government should intervene. The internet transcends state borders, and the storage, processing, and transferring of data is an interstate activity.

The confusion and inefficiency fueled by the patchwork approach has sparked calls from industry, consumer groups, and academics for a federal data privacy law that preempts (completely, or with only the most narrow, targeted exceptions) existing state-level regulations and provides needed clarity and certainty. A uniform, nation-wide standard of privacy gives users clarity that their rights are the same regardless of where they move or travel to; companies will have a clear, direct set of obligations and a single regulator to answer to. A federal standard would also curtail the existing race-to-the-bottom effect, in which states such as California that enact the most prescriptive and stringent regulations are rewarded with the power to dictate de-facto national standards. In the equilibrium created by the current patchwork approach, companies default to adopting the most stringent state-level standard to minimize the

[1] https://www.congress.gov/bill/119th-congress/house-bill/8413/text
[2] https://energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-establishing-a-federal-data-privacy-law

compliance costs that follow from interstate confusion and variation. One of the chief virtues of the SECURE Data Act is its strong preemption, which should be maintained as the bill's particulars continue to be negotiated.

Disclosures and Informed Consent

Another important element of the SECURE Data Act is its provisions relating to disclosures and informed consent. Congress should focus instead on ensuring consumers have access to the information—delivered in a clear, transparent way—that they need to make informed decisions. A key aspect of the digital economy is that it does not necessarily rely in the traditional exchange of tangible goods for monetary compensation. Instead, it allows for the monetization of data, often in the form of observing users' demonstrated preferences and behavioral patterns. In turn, users are usually compensated with access to services at little or no cost. As noted in landmark papers such as "The Economics of Privacy," consumers often choose to allow the monetization of their data for free or low-cost services, while also at times being "willing to pay a price premium to purchase goods from more privacy-protective merchants."[3] Tradeoffs are a fact of digital economic life, which Americans must navigate in a way that best suits their needs. Nonetheless, users' data and digital footprints have become a key currency and enabler for both companies and the users themselves. When both parties freely agree to a trade of data for services, both benefit.

However, most users of digital services tend to be unaware of the conditions by which this exchange happens. Sometimes, they are unaware that such a transaction took place at all. Often, digital platforms (including social media, retail, and others) only offer users lengthy and confusing terms and conditions, meaning that users often lack an accurate depiction about what kinds of data are being collected, how they are being stored and processed, how long they are held for, or how they can be sold to third parties. The problem is not the underlying data economy but the lack of transparency, without which consumers cannot make informed choices.

If Americans find it worthwhile to trade information about themselves, their preferences, or their online habits for cheap/free online services, it is not the place of lawmakers to gainsay them. However, this choice should be made with knowledge of what transaction they are making, which the SECURE Data Act does much to ensure. Consumers should be protected from their data being taken without their knowledge, not from their own decision to hand over their data if they believe that to be the right choice. Congress should not promote a discrete outcome—like reducing the amount of data shared with platforms—but rather promote informed consumer choice. Americans should be free to weigh the costs and benefits for themselves. Consumers have that right to make their own choices.

This approach will balance the interests of privacy and maintaining cheap or free access to digital services. Congress should account for the important role the data-driven advertising industry plays in providing affordable goods and services to consumers. If data-driven advertising is stifled, users will receive less personalized and less useful digital services and will likely see significant price increases for services that are now provided for free or at low cost. The SECURE Data Act's disclosure provisions allow users to make their own choices and keep the digital economy intact.

[3] https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf

Avoiding Burdensome Regulatory Schemes

The dangers of burdensome privacy regulation can be observed in other countries. More notably, the European Union (EU) passed the first major comprehensive data privacy law, its General Data Protection Regulation (GDPR). Throughout the years, both the EU and the state-based approaches have shown significant drawbacks that should be a warning call for policymakers. Analysis of the GDPR has found that the law "induced the exit of about a third of available apps [from the Google Play Store]; and in the quarters following implementation, entry

of new apps fell by half."[4] This is not the way to benefit consumers nor maintain the dominance of the American tech sector.

The U.S. should reject this approach. If platforms choose a revenue model that relies on data-driven personalized ads, and informed consumers assent, regulators should have nothing to say about it. Likewise, if platforms offer paid subscriptions without personalized advertising, that choice should not be interfered with. Market forces and informed consumer choice should be left to decide these questions and strike the right balance.

The SECURE Data Act contains some prescriptive requirements to force platforms, even after users give informed consent, to adhere to certain requests from users. These provisions could introduce compliance costs and deviate from TPA's preferred model of informed consent. However, these provisions are relatively modest when compared to previous privacy proposals in Congress, and they should not serve as an opening in future negotiations to radically expand the compliance costs of the bill. To know the effects of truly heavy-handed privacy regulation, members of the Committee need only look to the disastrous results produced by European regulation.

Conclusion

The issues of privacy and the data economy are critical to the strength of the American technology sector and, consequently, to the entire American economy. They are also critical to consumer choice and welfare. TPA appreciates the opportunity to provide input and applauds the committee for carefully considering these important matters. TPA would welcome the opportunity for further conversations with yourselves and your offices.

Sincerely,

David Williams
President
Taxpayers Protection Alliance

[4] https://www.nber.org/papers/w30028#fromrss

June 2, 2026

The Honorable Gus Bilirakis
Chair
Commerce, Manufacturing, and Trade Subcommittee
United States House of Representatives
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Commerce, Manufacturing, and Trade Subcommittee
United States House of Representatives
Washington, D.C. 20515

The Honorable Brett Guthrie
Chair
Energy & Commerce Committee
United States House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Ranking Member
Energy & Commerce Committee
United States House of Representatives
Washington, D.C. 20515

Re: Statement for the Record in Support of the SECURE Data Act (H.R. 8413)

Dear Chairs Guthrie and Bilirakis, and Ranking Members Pallone and Schakowsky,

The National Business Coalition on Artificial Intelligence and Privacy (the "Coalition") is a Section 501(c)(6) nonprofit organization dedicated for almost three decades to the enactment and adoption of rational and balanced federal privacy policies. The Coalition applauds the efforts of the House Committee on Energy and Commerce (the "Committee") to develop a practical national privacy framework that protects every hardworking individual, and we thank the Subcommittee on Commerce, Manufacturing, and Trade (the "Subcommittee") for convening a hearing on H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act ("SECURE Data Act"). The SECURE Data Act reflects broad consensus that individuals deserve strong privacy rights and that Congress should enact a commonsense federal privacy law that extends those rights to every consumer in America.

It is essential that the SECURE Data Act is enacted this year. Currently, millions are without privacy rights due to a patchwork of state consumer privacy laws. Privacy protections should be extended to everyone in the country and individuals should not receive different privacy rights based solely on the state in which they reside. By creating a uniform federal privacy framework, the bill would ensure that privacy protections are applied consistently across the country, while providing certainty for individuals, businesses, and regulators alike. We commend the Committee for recognizing that a durable national privacy law must include meaningful federal preemption in order to achieve these goals.

The bill strikes the right balance between protecting individuals and enabling responsible data use. For financial services companies, data is essential to providing products and services that consumers rely on every day, including fraud prevention, account servicing, identity verification, risk management, and customer support. The SECURE Data Act builds on the consensus framework adopted by many states and proposes to establish clear consumer rights, transparency obligations, and reasonable data governance requirements. In doing so, it provides strong privacy protections while preserving the ability of financial institutions to meet customer expectations, safeguard accounts, and deliver innovative services.

Finally, the SECURE Data Act adopts an effective enforcement framework that ensures accountability. The bill preserves an important role for state attorneys general while layering on federal enforcement by the Federal Trade Commission. By avoiding a broad private right of action, the bill reflects the state consensus and supports small businesses, among others, through strong and effective enforcement without creating the risk of costly litigation that does little to advance individuals' privacy.

For these reasons, we support the SECURE Data Act and applaud the Subcommittee's efforts to advance comprehensive federal privacy legislation. The bill reflects years of thoughtful work by states around the country and builds on the broad consensus that has emerged among policymakers, regulators, consumers, and industry stakeholders. We are proud to support the SECURE Data Act and encourage the Subcommittee to move forward with this historic legislation.

Sincerely,

Thomas M. Boyd
Co-Counsel
National Business Coalition on Artificial Intelligence and Privacy

Tara Potashnik
Co-Counsel
National Business Coalition on Artificial Intelligence and Privacy

CC: Representative John Joyce (R-PA)
Members of the Subcommittee on Commerce, Manufacturing, and Trade, House Committee on Energy and Commerce

DAVE YOST
OHIO ATTORNEY GENERAL

Administration
Office 800-282-0515

June 2, 2026

The Honorable Brett Guthrie
Chairman, House Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Guthrie:

We, the undersigned Attorneys General, write in support of H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act). This legislation offers a necessary and overdue step toward establishing a coherent national framework for consumer data privacy, and we urge its passage.

The digital economy does not stop at state lines, but privacy regulation increasingly does. Businesses operating across the country today face a growing and often inconsistent patchwork of state-level requirements, each with its own definitions, obligations, and enforcement mechanisms. Compliance within this fragmented landscape is costly and complex, particularly for small and mid-sized businesses that lack the legal resources of large technology companies. These costs are ultimately borne by consumers in the forms of reduced innovation, higher prices, and barriers to market entry.

A uniform national standard will provide the clarity, consistency, and enforceable protections that consumers lack currently. The SECURE Data Act establishes clear rules of the road that promote confidence in the digital marketplace, reduce unnecessary compliance burdens, and allow businesses to focus their resources on serving consumers rather than navigating an ever-shifting regulatory maze.

There is a broader structural concern that this legislation helps address.

For years, the de facto national standard for consumer data privacy has been shaped not through federal legislation, but through the market power of a single state: California. Because of California's economic size, businesses operating nationally have little practical choice but to conform to California's regulatory requirements. The result is that California's policy judgments — made by California's legislature and enforced by California's regulators with accountability only to California's voters — have effectively governed the data privacy landscape for consumers and businesses in all fifty states.

Yes, states play an important role as laboratories of democracy and should remain free to address emerging concerns. However, any regulations influencing interstate commerce and the national marketplace should be established through Congress, where every state has a voice, rather than through the policy preferences of a single state. The SECURE Data Act restores that balance, ensuring that American data privacy policy is set through deliberation and democratic accountability at the national level, not imposed through one state's market leverage.

For these reasons, we support the SECURE Data Act and encourage the Committee to advance this legislation.

Respectfully,

Dave Yost
Attorney General
State of Ohio

Steve Marshall
Attorney General
State of Alabama

Christopher M. Carr
Attorney General
State of Georgia

Statement for the Record

On Behalf of the

American Bankers Association

before the

House Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing, and Trade

June 3, 2026

Statement for the Record

On Behalf of the

American Bankers Association

before the

House Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing, and Trade

June 3, 2026

The American Bankers Association (ABA) appreciates the opportunity to provide a Statement for the Record for this hearing, *Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law*. ABA is the voice of the nation's $26.1 trillion banking industry, which is composed of small, regional and large banks that together employ over 2 million people, safeguard $20.5 trillion in deposits, and extend $13.7 trillion in loans.

Banks are a unique sector already subject to an extensive national compliance regime for data privacy and security. As we have previously shared with the Committee, the financial services industry was among the first sectors subject to a federal framework governing the collection, use, and sharing of consumer personal information pursuant to the Gramm-Leach-Bliley Act of 1999 (GLBA).

Given the existing legal requirements, ABA has consistently highlighted the need for legislation created for other industrial sectors to avoid inconsistent or duplicative requirements for banks. This would be achieved by way of an entity-level and data-level exemption for financial institutions.

SECURE Data Act

ABA commends the Energy and Commerce Committee for its efforts to produce H.R. 8413[1] ("SECURE Data Act"), which contains many of the policy priorities for which ABA has advocated over many years. We and our members appreciate the Committee's efforts to create a uniform standard that protects all Americans while minimizing the burden on businesses operating in interstate commerce.

[1] https://www.congress.gov/bill/119th-congress/house-bill/8413

House Committee on Financial Services—Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act

Importantly, under the proposed SECURE Data Act, banks would fall under the GLBA framework and all its attendant obligations. As the Energy and Commerce Committee works on its legislation, the House Financial Services Committee is endeavoring to modernize GLBA through H.R.8398[2] ("Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act"). The Energy and Commerce Committee's and the House Financial Service Committee's bills are complementary and reflect a commitment to renewed Congressional leadership in the privacy space, which has been left to the states for far too long.

Moreover, ABA greatly appreciates the Committees working in tandem on this salient issue. There were many areas of potential overlap and conflict, and the products reflect a mature and highly serious attempt to collaborate in a way that enhances consumer protections, expands the reach of data security safeguards, and ensures regulatory oversight by agencies with the necessary levels of subject matter expertise.

Conclusion

Banks' most important currency is trust. Financial information is among the most sensitive types of data, and consumers need to feel comfortable with what banks collect, how they use it, with whom it is shared, and why.

It is vital that new laws enhance, rather than jeopardize, that trust. This can be achieved by the passage of thoughtful and balanced legislation, such as those found in H.R. 8413 ("SECURE Data Act") and H.R.8398 ("Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act").

Thank you for allowing us to provide our views on this very important topic.

[2] https://www.congress.gov/bill/119th-congress/house-bill/8398

June 2, 2026

The Honorable Brett Guthrie, Chairman
The Honorable John Joyce, Vice Chairman
House Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Re: Support for H.R. 8413, the SECURE Data Act

Dear Chairman Guthrie and Vice Chairman Joyce,

On behalf of the NAI (Network Advertising Initiative), I write to express our support for H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act).

The NAI is not a typical industry trade association. Founded in 2000, the NAI has nearly 75 member companies and is the leading non-profit, self-regulatory trade association for advertising technology companies. Our mission is to promote strong consumer privacy protections and a free and open Internet, and enable small businesses to thrive by promoting the highest voluntary industry standards for the responsible collection and use of consumer data. Through our industry-leading privacy review program, we are committed to providing our members with independent privacy reviews and promoting their compliance with enforceable laws and regulations. In short, we are a tool to help federal and state U.S. enforcement agencies ensure that digital advertising businesses are responsible stewards of consumer data.

The NAI's top public policy objective is to achieve a workable, uniform national privacy framework — the very goal H.R. 8413 advances. For more than a decade, the absence of comprehensive federal privacy legislation has given rise to an ever-expanding patchwork of state laws — each with its own definitions, consumer rights, and compliance timelines. This fragmentation fails to establish a clear, consistent set of rights that can be relied upon by all consumers regardless of the state they live in, while imposing enormous compliance costs, particularly on small and mid-size companies.

The SECURE Data Act was crafted to address this problem by incorporating consensus provisions from state laws enacted with strong bipartisan support in more than 20 states. This legislation strives to create a single, enforceable national standard, uniform consumer rights — including the rights to access, correct, delete personal data — and a set of clear obligations for controllers and processors of consumer data modeled off prevailing approaches across U.S. states.

The bill's enforcement structure—empowering the Federal Trade Commission and state attorneys general, while declining to create a private right of action—focuses accountability and compliance mechanisms where they belong without exposing businesses to unlimited litigation risk. The NAI strongly supports this enforcement approach.

We also applaud the SECURE Data Act's recognition that self-regulatory programs can play a complementary role alongside federal law. A federal framework that works in concert with industry self-regulation—rather than displacing it—will achieve better consumer outcomes while reducing the costs and delays of government-only enforcement.

The NAI commends Chairman Guthrie, Vice Chairman Joyce, and the members of the Energy and Commerce Privacy Working Group for developing a bill that balances consumer protection, regulatory clarity, and innovation. We look forward to working with the Committee as H.R. 8413 moves forward and stand ready to provide technical expertise, stakeholder engagement, and any other assistance that may be helpful. The NAI is also committed to supporting efforts to build bipartisan support for this legislation.

Thank you for your leadership on this critical issue.

Sincerely,

Leigh Freund
President & CEO
The NAI

cc: Members of the Subcommittee on Commerce, Manufacturing, and Trade

June 2, 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

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

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

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

Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

NATSO, Representing America's Travel Centers and Truck Stops, and SIGMA: America's Leading Fuel Marketers,[1] welcome the introduction of comprehensive privacy legislation, the SECURE Data Act, and commend the House Committee on Energy and Commerce's ongoing efforts on these policies.

In particular, NATSO and SIGMA appreciate that the legislation would replace the current patchwork of state privacy laws with a consistent national framework under which our members can better operate. A clear nationwide standard would strengthen consumer trust, provide individuals with meaningful control over their personal information, and give businesses the certainty needed to innovate, protect data, and drive economic growth.

As the legislation advances, NATSO and SIGMA encourage the Committee to carefully consider how data minimization requirements under the bill are applied in practice. Travel centers, truck stops, and fuel marketers rely on customer loyalty and rewards programs to provide customers with personalized offers, benefits, and discounts. Overly restrictive limitations on the collection and use of data that consumers provide could inadvertently reduce the effectiveness of these programs and diminish the value they deliver to consumers.

[1] NATSO currently represents approximately 5,000 travel plazas and truck stops nationwide, comprising both national chains and small, independent locations. SIGMA represents a diverse membership of approximately 260 independent chain retailers and marketers of motor fuel. The retail fuels and convenience industry provide 2.38 million jobs at approximately 120,000 retail establishments across the country.

NATSO and SIGMA look forward to working with the Committee on the SECURE Data Act. Please do not hesitate to contact us with questions regarding our members' perspectives on the provisions discussed above or any other aspects of the legislation.

Sincerely,

NATSO, Representing America's Travel Centers and Truck Stops
SIGMA: America's Leading Fuel Marketers

cc: Members of the Subcommittee on Commerce, Manufacturing, and Trade

BR Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

June 3, 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

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

Dear Chairman Guthrie and Chairman Bilirakis:

On behalf of Business Roundtable, thank you for the opportunity to submit this statement for the record for the Subcommittee on Commerce, Manufacturing, and Trade's hearing titled "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law." Business Roundtable is an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. BRT CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. gross domestic product (GDP).

Business Roundtable strongly supports enactment of a clear national data privacy standard that gives all Americans the same rights and protections, no matter where they live or travel. A single national privacy standard ensures that privacy protections are consistent across state lines, while making data practices easier to understand and more transparent. It also reduces the uncertainty and compliance burden that employers, innovators, and businesses face when trying to navigate multiple, sometimes conflicting, state requirements.

The SECURE Data Act (H.R. 8413) strikes the right balance. It provides consumers with meaningful control over their information, draws on proven, bipartisan state privacy frameworks and allows innovative and beneficial uses of data while protecting consumers. It also empowers the Federal Trade Commission to enforce consumer privacy law while preserving an enforcement role for state attorneys general. Most importantly, it fully preempts state laws and ends the confusing and harmful patchwork approach that currently undermines clarity and predictability.

The need for a national privacy law is widely recognized by the public on a bipartisan basis. Recent surveys show that 86% of Americans believe data privacy should be governed by federal law and 73% support federal preemption, including large majorities across party lines. By contrast, only 14% of Americans believe data privacy should be regulated solely by the states. These figures underscore the breadth of support for a comprehensive federal framework that delivers consistent protections for consumers nationwide.

The SECURE Data Act is also built on effective and proven state privacy laws already enacted in Colorado, Connecticut, Florida, Iowa, Kentucky, Texas, Utah, and Virginia, to name a few. Across the country, lawmakers from both parties have repeatedly demonstrated that meaningful privacy legislation can pass with broad bipartisan support. In total, 1,119 Democrats and 1,449 Republicans across 20 state legislatures have voted for data privacy laws used to develop the SECURE Data Act.

The SECURE Data Act offers a practical path forward and is good for American businesses and consumers. By creating clear, consistent rules, Congress can protect privacy rights, support innovation and eliminate the compliance challenges caused by an increasingly fragmented regulatory landscape.

Business Roundtable thanks the Committee for holding this important hearing and asks the Committee to act quickly to advance the SECURE Data Act.

Sincerely,

Amy Shuart
Vice President, Technology & Innovation
Business Roundtable

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.

---

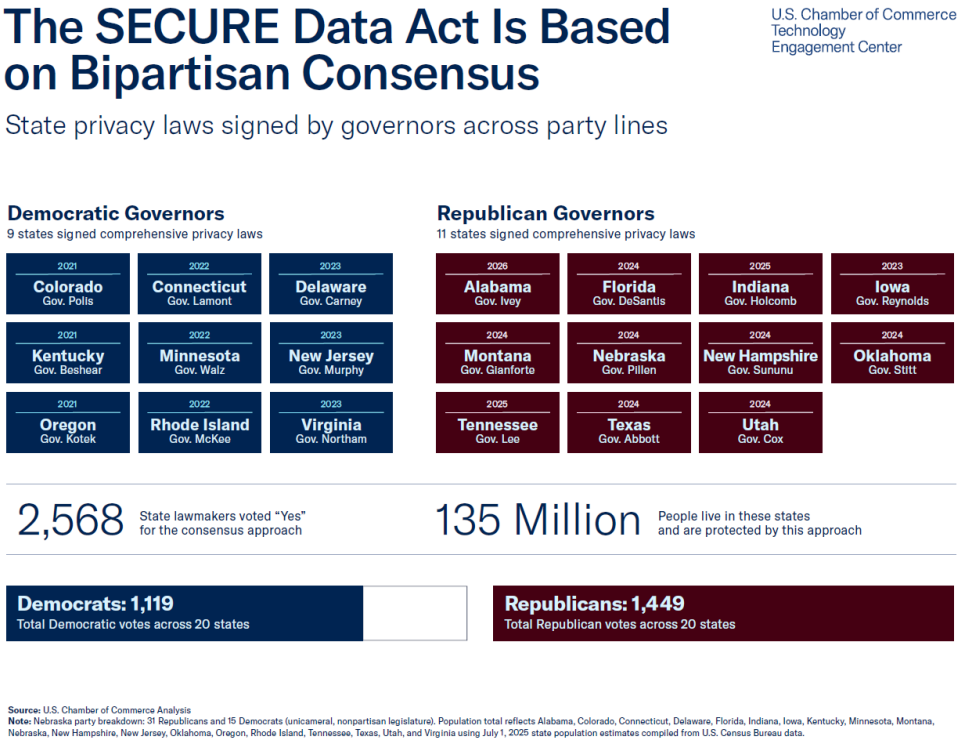
[6] See Amicus of U.S. Chamber of Commerce, Guiterez v. Converse (C.D. Cal January 22, 2025) *available at* https://www.uschamber.com/assets/documents/U.S.-Chamber-Coalition-Amicus-Brief-Gutierrez-v.- Converse-Inc.-Ninth-Circuit.pdf.

[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.

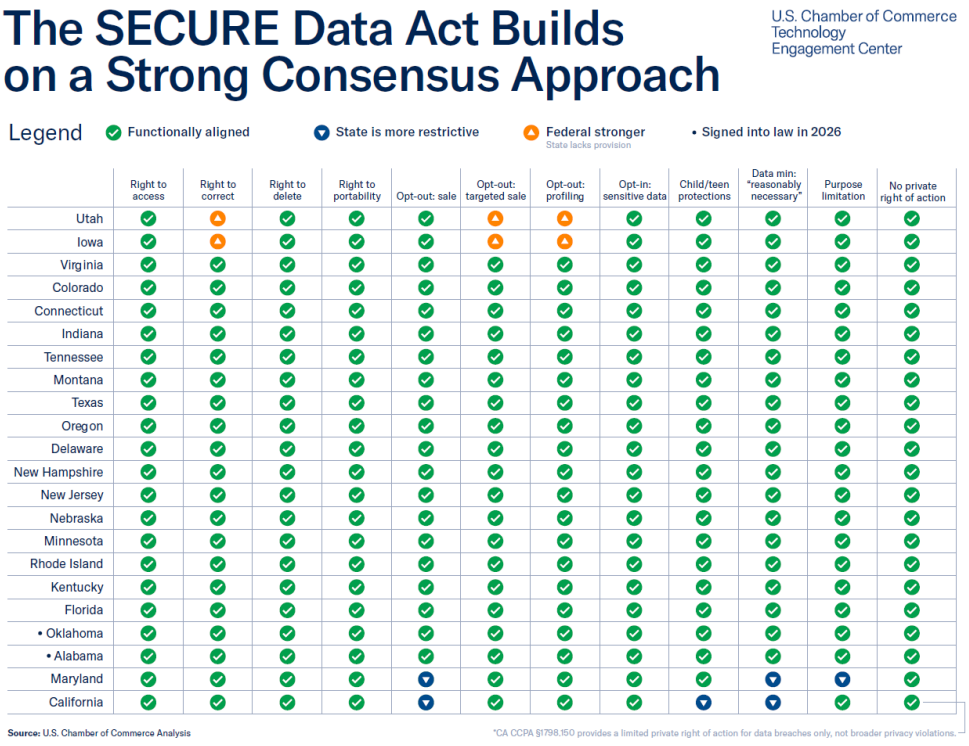
The SECURE Data Act mirrors the state Consensus Privacy Approach in that it provides consumers robust privacy protections including the right to:

- 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.

U.S. Chamber of Commerce

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

June 2, 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

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Bilirakis, and Ranking Member Schakowsky:

The undersigned state and local chambers of commerce write to express support for H.R. 8413, the "SECURE Data Act," and urge the House Committee on Energy and Commerce to advance this legislation.

The SECURE Data Act would establish a single national privacy standard with robust consumer protections that builds upon a strong framework already adopted in 20 states. Those protections include data minimization and sensitive data requirements, as well as access deletion, correction, and opt-out rights. Importantly, this legislation will also help small businesses who are disproportionately impacted by the regulatory confusion caused by a patchwork of state privacy laws.

For these reasons, the undersigned organizations support enactment of a single national privacy standard that protects consumers and provides a workable compliance framework for businesses of all sizes. We respectfully urge you to advance the SECURE Data Act.

Sincerely,

U.S. Chamber of Commerce

Alabama
Prattville Area Chamber of Commerce
Selma and Dallas County Chamber of Commerce and Tourism Information

Alaska
Alaska Chamber of Commerce

Arizona
Apache Junction Area Chamber of Commerce
Arizona Chamber of Commerce & Industry
Chandler Chamber of Commerce
Gilbert Chamber of Commerce
Greater Flagstaff Chamber of Commerce
Nogales Santa Cruz County Chamber of Commerce & Tourism Center
Northwest Valley Chamber of Commerce
Queen Creek Chamber of Commerce

Arkansas
Little Rock Regional Chamber
Rogers Lowell Chamber

California
Brea Chamber of Commerce
Carlsbad Chamber of Commerce
Greater Bakersfield Chamber of Commerce
Greater High Desert Chamber of Commerce
Greater Modesto Chamber of Commerce
La Canada Flintridge Chamber of Commerce
Long Beach Area Chamber of Commerce
North San Diego Business Chamber
Rancho Cordova Area Chamber
San Juan Capistrano Chamber of Commerce
Santa Barbara South Coast Chamber of Commerce
Temecula Valley Chamber of Commerce

Colorado
Vail Valley Partnership

Connecticut
Connecticut Business & Industry Association
Greater New Haven Chamber of Commerce

Delaware
Delaware State Chamber of Commerce

Florida
Lakeland Chamber of Commerce
Venice Area Chamber of Commerce

Georgia
Barrow County Chamber of Commerce
Columbia County Chamber of Commerce
Georgia Chamber of Commerce
Gwinnett Chamber of Commerce
Moultrie-Colquitt County Chamber of Commerce
Murray County Chamber of Commerce

Idaho
Pocatello-Chubbuck Chamber of Commerce

Illinois
Edwardsville/Glen Carbon Chamber of Commerce
Illinois Chamber of Commerce
The Greater Springfield Chamber of Commerce
Western DuPage Chamber of Commerce

Indiana
Angola Area Chamber of Commerce
Indiana Chamber of Commerce

Iowa
Iowa Association of Business and Industry

Kansas
Coffeyville Area Chamber of Commerce
Overland Park Chamber of Commerce
Parsons Chamber of Commerce

Kentucky
Kentucky Chamber of Commerce
Northern Kentucky Chamber of Commerce
One Louisville

Louisiana
Bossier Chamber of Commerce
Central Louisiana Regional Chamber of Commerce
River Region Chamber of Commerce
St. Tammany Chamber of Commerce

Maine
Maine State Chamber of Commerce

Maryland
Harford County Chamber of Commerce

Massachusetts
Greater Boston Chamber of Commerce

Michigan
Blue Water Area Chamber of Commerce
Detroit Regional Chamber
Michigan Chamber

Minnesota
FORWARD Worthington
Shakopee Area Chamber of Commerce
The Chamber Grand Forks / East Grand Forks

Mississippi
Covington County Chamber of Commerce
Mississippi Business Alliance

Missouri
Greater Kansas City Chamber of Commerce

Montana
Glasgow Area Chamber of Commerce & Agriculture
Montana Chamber of Commerce

Nebraska
Nebraska Chamber of Commerce and Industry

Nevada
Mesquite Chamber of Commerce
Vegas Chamber of Commerce

New Jersey
New Jersey State Chamber of Commerce

New York
Capital Region Chamber
Tompkins Chamber

North Carolina
Black Mountain Swannanoa Chamber of Commerce
Lillington Area Chamber of Commerce
McDowell Chamber of Commerce

North Dakota
Greater North Dakota Chamber

The Chamber Grand Forks / East Grand Forks

Ohio
Ohio Chamber of Commerce
Toledo Regional Chamber of Commerce
Troy Area Chamber of Commerce

Oklahoma
Oklahoma Technology Alliance
The State Chamber of Oklahoma

Oregon
Gresham Area Chamber of Commerce
Oregon Business & Industry

Pennsylvania
Cambria Regional Chamber of Commerce
Pennsylvania Chamber of Business and Industry
Schuylkill Chamber of Commerce

South Carolina
Fountain Inn Chamber of Commerce
Greater Easley Chamber of Commerce
Hilton Head Island - Bluffton Chamber of Commerce
Myrtle Beach Area Chamber of Commerce

Tennessee
Kingsport Chamber
Tennessee Chamber of Commerce & Industry

Texas
Dallas Regional Chamber
Longview TX Chamber of Commerce

Virginia
Central Fairfax Chamber of Commerce
ChamberRVA
Colonial Beach Chamber of Commerce
Fredericksburg Regional Chamber of Commerce
Hampton Roads Chamber
Loudoun County Chamber of Commerce
Lynchburg Regional Business Alliance
Top of Virginia Regional Chamber
Virginia Chamber of Commerce
Virginia Peninsula Chamber

Washington
Covington Chamber of Commerce
Lakewood Chamber of Commerce
Sedro-Woolley Chamber of Commerce
SnoValley Regional Chamber
Tacoma-Pierce County Chamber

Wisconsin

Rice Lake Chamber of Commerce
Wisconsin Manufacturers & Commerce

Wyoming
Greater Cheyenne Chamber of Commerce
Jackson Hole Chamber of Commerce
Riverton Chamber and Visitors Center
Rock Springs Chamber of Commerce

cc: The Honorable John Joyce and Members of the House Committee on Energy and Commerce

Anthony Qaiyum
Merz Apothecary
4716 N Lincoln Ave, Chicago, IL 60625

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on H.R. 8413, the SECURE Data Act

June 3, 2026

Chairmen Guthrie and Bilirakis, and Members of the Committee and Subcommittee:

My name is Anthony Qaiyum. I own Merz Apothecary, a 151-year-old Chicago pharmacy offering a large selection of natural and hard-to-find health, beauty, and personal care products. I support the SECURE Data Act because it provides small businesses like mine with clear, consistent data privacy rules that will allow us to continue responsibly using data-powered tools to grow, thrive, and serve our customers and communities.

My family has owned Merz Apothecary for more than 50 years. We have succeeded by evolving to meet the needs of today's online shoppers, while consistently offering exceptional health and beauty products and providing outstanding customer service. We've been selling our goods online since 1997, long before most small businesses were doing so. Today, we operate a thriving brick-and-mortar store on Chicago's North Side, as well as a sizable online retail business serving customers nationwide.

Data-powered tools are essential to our business. We use data-powered digital ads, for instance, to reach people who are likely to be interested in our specialty and natural products. Data-powered analytic tools, in turn, help us understand which ads are most effective — allowing us to adjust accordingly and make the most of our marketing budget. We also use past-purchase data to follow up with existing customers about deals, products they might have run out of, and new products they might be interested in.

Currently, however, 20 states have passed data privacy laws, each with its own definitions, restrictions, and compliance requirements — creating a complex legal patchwork that's expensive and difficult to navigate. Some state laws, like Maryland's, tightly restrict basic data

uses, like those described above, that are vital to our business, making it harder for us to find customers and grow. I am worried more states will follow suit.

Small businesses need a clear, balanced federal privacy framework that provides legal clarity and preserves access to the tools that help us grow and succeed. The SECURE Data Act would establish such a standard while offering critical data security to all Americans. I respectfully urge the Committee and Subcommittee to advance the SECURE Data Act.

Sincerely,

Anthony Qaiyum
Owner
Merz Apothecary

Neil Abramson
ECi Stores
1021 Central St Leominster, MA 01453

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on H.R. 8413, the SECURE Data Act

June 3, 2026

Chairmen Guthrie and Bilirakis, and Members of the Committee and Subcommittee:

My name is Neil Abramson. In 1998, my wife and I launched ECi Stores, a small chain of consignment shops in Leominster, MA. I'm writing to express my support for the SECURE Data Act, which would ensure small businesses like mine can continue using data-powered tools to grow, compete, and succeed in the digital economy. In addition, I respectfully offer one request for minor changes to the bill.

In many ways, ECi Stores is a classic Main Street business. Our inventory comes exclusively from residents of central Massachusetts, and our three stores employ 30 people in the local community. But today, thanks to digital tools, we're also able to sell and compete nationally. At any given time, we have roughly 60,000 unique items in our stores, around 20,000 of which are also listed online.

Data-powered tools help drive our success online. We use data-powered digital ads, for instance, to reach new customers. These ads are delivered to people whose basic data suggests they're likely to be interested in our products, such as shoppers who have searched online for unique or vintage clothes. The ad platforms we work with also collect data that helps us see which ads are working best, so we can adjust accordingly and make the most of our limited ad dollars. Similarly, basic purchase-history data lets us follow up in ways that customers appreciate and that help us drive sales.

A growing patchwork of state data privacy laws, however, threatens to make it harder and more expensive for small businesses like mine to use these basic tools. Today, we face 20 different state privacy laws, each with different definitions, thresholds, and compliance requirements —

adding confusion and costs to our operations. Additional states consider new privacy laws every year, and some laws go so far that they seriously restrict small businesses' ability to use data-powered tools. Massachusetts lawmakers, for example, are considering legislation that would so severely restrict data use that it could prevent me from using past-purchase information to follow up with customers about other products they are likely to be interested in.

As the Committee and Subcommittee continue their work, I respectfully urge members to refine one provision to better advance the SECURE Data Act's goals. The bill's teen age-verification and parental-consent requirements, while well-intentioned, could create unnecessary barriers for young people trying to shop from age-appropriate online businesses — including teens shopping for vintage clothing from resale businesses like mine. Congress should avoid overly broad requirements that make it harder for teens to access appropriate online products and that require businesses to collect personal information from young users.

By creating a single national privacy standard, the SECURE Data Act would replace the growing state-by-state patchwork with clear, consistent rules that protect consumers and work for businesses of all sizes. Importantly, it would give small businesses like mine the certainty we need to continue responsibly using data-driven tools to reach customers, compete online, and grow.

I thank Committee and Subcommittee members for their work on the critically important issue of data privacy, and urge them to refine and advance the SECURE Data Act.

Sincerely,
Neil Abramson
Co-Founder
ECi Stores

Written Testimony of Jason Stock
Founder, Firecracker Software (Spokane, Washington)

To the Members of the Committee on Energy and Commerce, and the Subcommittee on Commerce, Manufacturing, and Trade:

My name is Jason Stock, and I am the founder of Firecracker Software, a small app development company based in Spokane, Washington. For over ten years, I have built mobile games and applications and proudly participated in the American app ecosystem.

Thank you for the opportunity to submit this testimony. As an independent developer and small business owner, I strongly endorse the Securing and Establishing Consumer Uniform Rights and Enforcement (SECURE) Data Act, with minor adjustments to its teen mandates.

My apps are downloaded by users across the country, and as a small business, I am constantly striving to scale and reach new users. However, the current framework of data privacy laws makes this incredibly difficult. Complying with a 50-state patchwork of different regulations—where some states pass overly restrictive laws while others conflict—drives up compliance costs and creates massive hurdles for small developers trying to grow.

Furthermore, my business relies on utilizing basic data to generate revenue. Like most developers, we use basic information to identify and fix software crashes, understand which game features our players enjoy most, and provide a seamless user experience. We also use this data to show relevant advertisements, which helps us keep our games free to download. If overly restrictive laws prevent us from collecting or utilizing this basic data, we lose both the ability to improve our products and the revenue needed to keep our small business afloat.

The SECURE Data Act solves this by providing a unified national standard. Establishing a clear and unified set of rules protects consumers nationwide while avoiding unnecessary, burdensome hurdles that stifle innovation and harm app-based businesses.

Also, user trust is incredibly important to us at Firecracker Software, which is why I appreciate that the SECURE Data Act focuses on consumer choice and transparency. This bill requires companies to tell people exactly what data is collected and how it is used, gives users the right to opt out, and limits data collection to only what was disclosed. By establishing these clear rules, the SECURE Data Act strikes the right balance. It delivers the transparency and data control that consumers deserve while providing the app ecosystem with the regulatory certainty it needs to continue driving innovation and economic growth.

Though I fully support the SECURE Data Act and its vision for a unified national privacy standard, serious concerns remain around its age-verification requirements. Requiring verifiable parental consent for teens aged 13–15 is operationally unworkable. Because there is no simple way to verify a parental relationship without demanding sensitive documents like government IDs or birth certificates, or complex digital signals, developers would be forced to implement invasive checks for all users. I do not want to collect or handle this highly sensitive documentation, and safely storing these extra data signals is extremely expensive.

Furthermore, forcing users to submit personal documentation just to access online apps and information creates an unnecessary liability and directly interferes with the First Amendment. This approach places a heavy burden on citizens seeking to access protected online speech and

restricts developers' rights to distribute it, failing the constitutional requirement of the least restrictive means. I commend the Subcommittee for tackling this critical issue and strongly urge you to advance the SECURE Data Act while addressing these unworkable age-verification mandates so that small businesses are not crushed by the resulting data liabilities.

Sincerely,

Jason Stock
Founder, Firecracker Software
Spokane, Washington

To the Members of the Committee on Energy and Commerce, and the Subcommittee on Commerce, Manufacturing, and Trade

The Developers Alliance, a leading advocate for developers, the companies they build, and the industries that rely on them, strongly endorses the Securing and Establishing Consumer Uniform Rights and Enforcement (SECURE) Data Act.

First and foremost, developers need a clear, single national framework. Every app developer has customers across states, and the current patchwork of laws drives up the compliance costs and creates massive backlogs for developers trying to grow and succeed.

Uncertainty around the patchwork of 50+ state laws on data privacy burdens developers with massive liabilities. While large tech companies can easily manage and absorb these expenses, small developers and businesses are most affected. According to RaftLabs[1], building new apps that comply with privacy laws costs between $30,000 and $80,000, but updating existing apps to comply can cost $90,000–$250,000+ and waste weeks of development time and resources.

Beyond the financial burden of navigating conflicting rules, states are increasingly imposing stringent data restrictions. For example, Maryland recently passed privacy legislation that is significantly more restrictive than frameworks in California or even Europe. As several other states consider similarly extreme measures, developers are stripped of the ability to utilize the data necessary to build, maintain, and improve their products.

The SECURE Data Act solves this by providing a unified national standard. Establishing a clear and unified set of rules protects consumers nationwide while avoiding unnecessary, burdensome hurdles that stifle innovation and harm app-based businesses.

Secondly, the SECURE Data Act gets it right by focusing on consumer choice and transparency. Data is at the center of all applications; it allows developers to run analytics, understand their customers, and monetize their apps quickly and easily through ads. Ads account for some two-thirds of app revenue[2], and effective advertising requires good data that developers can collect from their users and that their ad partners can collect to ensure the right ads are being served to the right audience. When apps have a strong understanding of their users' behavior and preferences, they can generate up to twice the ad revenue as those that rely solely on third-party data[3]. Broadly restricting data collection and use, rather than empowering consumers to opt out of specific use cases, severely undermines the economics of the developer ecosystem.

This bill follows the gold-standard framework of privacy laws: it requires companies to tell people exactly what data is collected and how it is used, gives users the right to opt out, and limits data collection and use to only what was disclosed.

---

[1] Raftlabs, US state privacy laws: A state-by-state guide for app builders, May 2026. https://www.raftlabs.com/blog/us-state-privacy-laws-guide
[2] App Developer Magazine, Mobile app ad revenue continues to soar, September 2024. https://appdevelopermagazine.com/mobile-app-ad-revenue-continues-to-soar/?utm_source=chatgpt.com
[3] App Verticals, Mobile App Monetization Statistics in 2026: Revenue Benchmarks, Models & Trends, February, 2206. https://www.appverticals.com/blog/mobile-app-monetization-statistics/?utm_source=chatgpt.com

By establishing these clear rules, the SECURE Data Act strikes the right balance. It delivers the transparency and data control that consumers deserve while providing the app ecosystem with the regulatory certainty it needs to continue driving innovation and economic growth.

However, developers do have some concerns over requiring verifiable parental consent for teens aged 13-15. First, there is no standard, sure-fire way to verify that an adult is a parent or guardian for a minor, short of producing sensitive documents such as a birth certificate. This creates an incredibly high bar for young teens and their parents to clear to access online content.

These burdens directly connect to the second concern: the First Amendment. Such a requirement likely infringes not only on citizens aged 13-15 right to access protected speech online, but also on the First Amendment right of developers to distribute protected speech, because it likely fails the least restrictive means test. A similar approach to app store age verification was passed in Texas, and is currently being challenged in court on constitutional grounds[4], and a U.S. District Court struck down an Ohio law that required age verification for social media use[5]. Efforts to protect minors online should focus on the apps, websites, and other avenues that are geared toward adults or offer users different experiences based on their age. We don't require malls to age verify every shopper because there is a wine store in the mall, which is the wine store's job before providing an adult experience, selling alcohol. We also don't require toy stores to receive parental consent before kids purchase Monopoly.

Lastly, this raises serious privacy concerns. To comply, platforms would have to implement invasive age checks for everyone, forcing developers to handle sensitive personal information that they do not want or need. Receiving and safely storing this sensitive age data is extremely expensive, with most developers estimating annual compliance costs of $10,000 or more.

The Developers Alliance commends the Subcommittee for tackling this issue and strongly urges you to advance the SECURE Data Act while addressing the concerns raised above.

Sincerely,

Jake Ward
Board Chair

---

[4] Troutman, Pepper, Locke. Federal District Court Grants Preliminary Injunction of Texas App Store Accountability Act, December 2025
https://www.troutmanprivacy.com/2025/12/federal-district-court-grants-preliminary-injunction-of-texas-app-store-accountability-act/

[5] Ohio Capital Journal, Ohio judge permanently blocks social media age verification law, April, 2025.
https://ohiocapitaljournal.com/2025/04/18/ohio-judge-permanently-blocks-social-media-age-verification-law/

Written Testimony of Kerry Gallivan
Founder & CEO, Chimani (Portland, Maine)

To the Members of the Committee on Energy and Commerce, and the Subcommittee on Commerce, Manufacturing, and Trade:

My name is Kerry Gallivan, and I am the founder and CEO of Chimani, a mobile technology company based in Maine. For over sixteen years, my team and I have built mobile app guides and tools that help millions of travelers discover, navigate, and explore America's national parks.

Thank you for the opportunity to submit this testimony. As an independent developer who recently walked the halls of Capitol Hill advocating for a federal privacy framework for the mobile app ecosystem, I strongly endorse the Securing and Establishing Consumer Uniform Rights and Enforcement (SECURE) Data Act.

By the very nature of tourism and travel, Chimani's users come from every single state across the country. Trying to scale a small business while navigating a conflicting patchwork of data privacy laws has become incredibly difficult. Complying with multiple, fragmented state regulations—where some states implement overly restrictive rules while others directly conflict—drives up compliance overhead and creates massive barriers to entry for small developers trying to innovate

Furthermore, my business relies on utilizing basic data to function and provide value to travelers. When users open the Chimani app, we rely on basic usage data to run essential analytics, monitor crash reports, and map out multi-park itineraries. We also utilize GPS location data, allowing users to see exactly where they are on our offline park maps and check in at locations throughout their journey, creating a personalized travelogue of their experiences. We rely on these data signals to build next-generation tools, like our AI-powered travel assistant, and to keep our core park guides free for everyone to access. If extreme and fragmented state laws prevent us from collecting or utilizing these basic signals, independent developers lose the ability to improve their features, deploy new AI solutions, and keep their businesses viable.

The SECURE Data Act solves this problem by providing a single, straightforward national standard. Establishing one clear set of rules protects consumers across the country while eliminating the expensive and confusing compliance hurdles that make it so hard for small app-based businesses to survive and innovate.

We deeply value user trust, and the SECURE Data Act does the same. It requires companies to clearly explain what data they collect and how they use it, and it gives users the right to opt out. This way, consumers stay in control of their information, which encourages more app downloads and helps the entire app economy thrive.

Though I fully support the SECURE Data Act and its vision for a unified national privacy standard, serious concerns remain around its age-verification requirements. Because there is no simple way to verify a parental relationship, it demands government IDs and sensitive data. Receiving and safely storing this sensitive data is extremely expensive, with most developers estimating $10,000 or more annually in compliance costs.

Furthermore, forcing users to submit personal documentation just to access online content raises serious First Amendment issues. Courts have struck down similar regulations because they violate constitutional free speech protections by creating unnecessary barriers to access safe,

age-appropriate content and burden safe, age-appropriate apps with unnecessary data receipt and storing requirements. A federal judge already blocked a similar Texas law in December 2025, ruling that its sweeping mandates likely violate free speech protections.

I commend the Subcommittee for tackling this critical issue. I strongly urge you to advance the unified framework of the SECURE Data Act while removing these unworkable age-verification mandates.

Sincerely,

Kerry Gallivan
Founder & CEO, Chimani
Portland, Maine

Connected Commerce Council (3C)
1701 Rhode Island Avenue NW
Washington, DC 20036

House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade

Hearing on H.R. 8413, the SECURE Data Act

June 3, 2026

Chairmen Guthrie and Bilirakis, and Members of the Committee on Energy and Commerce, and the Subcommittee on Commerce, Manufacturing, and Trade:

As Executive Director of the Connected Commerce Council (3C), I appreciate the opportunity to express 3C's support for the "Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act" (the "SECURE Data Act") and its goal of creating a unified national data privacy framework. I also respectfully offer one recommendation to further strengthen the bill.

3C works to promote small businesses' access to digital tools and technologies, and to cultivate a policy environment that supports their digital empowerment. Accordingly, we have long called for a single, balanced federal data privacy standard that — as the SECURE Data Act does — supersedes state laws; ensures small businesses can continue leveraging data-powered tools to grow, compete, and succeed; and meaningfully addresses the data-security risks facing Americans.

Digital platforms and data-powered tools have revolutionized commerce for America's 34 million small businesses — enabling even small, highly specialized shops like Prados Beauty, an Indigenous makeup provider, and EaZyHold, a toolmaker for the physically challenged, to grow with unprecedented efficiency. Data-powered tools allow such businesses to affordably market their products to the right customers, advertise to interested audiences, and quickly ship their products to buyers nationwide.

The current absence of a national data-privacy standard, however, threatens digital tools' affordability and effectiveness, jeopardizing small businesses' growth. Unfortunately, many states have passed laws that make it harder and more expensive for small businesses to engage in critical data-driven activities, including advertising and marketing. To date, 20 states have enacted 20 different state-level data privacy laws, each with different definitions, thresholds, and

compliance requirements. Additional states consider new data-privacy laws every year, creating a growing patchwork that is increasingly unmanageable for small businesses.

Worse, states with the most stringent data-privacy laws put their own states' small businesses at a significant disadvantage to other states'. The Maryland Online Data Privacy Act (MODPA), for instance, is far more restrictive than any other state's data privacy legislation — including California's and even the EU's. That means Maryland small businesses can no longer use many cost-effective data-powered tools that are vital to success in the digital economy, while their competitors in other states can.

The growing patchwork of state laws also makes it more difficult for small businesses to compete with larger rivals. Big companies can call on teams of legal, marketing, and technical experts to help navigate the complexities of interstate data-privacy compliance, but most small businesses cannot afford to do so. Compliance and legal costs are major expenses[1] for small-businesses; unsurprisingly, 71%[2] of small business owners say they would prefer a national data privacy law over the current patchwork of state laws.

3C welcomes the SECURE Act's balanced, comprehensive approach to these challenges. We note with particular appreciation the bill's strong federal preemption clause, adoption of key elements of successful state data-privacy frameworks, and avoidance of potentially devastating private rights of action and overly restrictive limits on responsible data use.

As the committee and subcommittee continue their work, we respectfully urge members to consider a key provision that could be refined to ensure the SECURE Act's progress and better advance its goals. The bill's teen age-verification and parental-consent mandates — though well-intentioned — may make it harder for teens to patronize age-appropriate online businesses like popular online resale site Depop, or family table-games maker ASM Games. In addition, the mandates are likely to create serious new privacy and security concerns and run afoul of First Amendment speech protections, potentially hampering the SECURE Data Act's passage.

3C thanks the committee members for their work on the critical issue of data privacy and for the opportunity to comment on the SECURE Data Act. We support efforts to create a national data privacy framework that acknowledges the critical role data plays for digitally empowered small businesses, and applaud the sponsors for introducing the bill. We request that the committee

---

[1] Connected Commerce Council, Privacy Patchwork, https://connectedcouncil.org/privacy-patchwork/.
[2] Connected Commerce Council, The Digital Advantage for Small Businesses: How Digital Ads and AI Drive Growth (2026), https://connectedcouncil.org/the-digital-advantage-for-small-businesses-how-digital-ads-and-ai-drive-growth/.

address the issue of burdensome age verification requirements and consider the appropriate, kid-friendly purchases these requirements would impede.

Sincerely,
Rob Retzlaff
Executive Director
Connected Commerce Council

Biotechnology Innovation Organization
1201 New York Ave., NW
Suite 1300
Washington, DC 20005
202-962-9200

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

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

June 3, 2026

Dear Chairman Guthrie, Ranking Member Pallone:

On behalf of the Biotechnology Innovation Organization (BIO), I am writing to share our support for a federal comprehensive data privacy and security framework, as outlined in the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, or SECURE Data Act (H.R. 8413).

BIO is the premier biotechnology advocacy organization representing biotech companies, industry leaders, and state biotech associations in the United States and more than 35 countries around the world. Our members research and develop breakthrough biotechnology products that save and change people's lives. More than 90 percent are small and medium-sized companies, many of which are pre-commercial, and represent the true drivers of biotechnological innovation in our nation. In fact, statistics show that more than half of all innovative medicines originate with them.

As health care transforms from traditional one-size-fits-all medical care to personalized medicine tailored to the genomic, molecular, and lifestyle characteristics of individual patients, BIO and our members stand ready to deliver further breakthrough innovations. Yet companies' ability to efficiently access and leverage health data to drive biomedical research – while appropriately protecting patient privacy – is critical to their efforts to progress commercial research and development, both domestically and globally.

The existing patchwork of various data privacy laws – across states, federal regulations, and privacy rules around the world, have created confusion and regulatory burdens that hinder coordination and collaboration amongst companies and research partners. BIO supports the SECURE Data Act's strong federal preemption provisions to ensure one uniform federal privacy standard that provides innovators with the regulatory certainty and consistency needed to advance biotechnology for the benefit of American patients.

Further, we believe that harnessing health data for biomedical R&D can continue without impinging on the protection of patients' privacy rights. H.R. 8413 strikes the appropriate balance by recognizing existing federal frameworks governing clinical trial data, as well as de-identified health data standards under HIPAA, without unduly burdening innovators with dual regulatory regimes in legitimate clinical research settings.

We look forward to continuing to work with the Committee to clarify these needs for the research community while enhancing the privacy and security of sensitive health data.

Sincerely,

John F. Crowley
President and CEO, Biotechnology Innovation Organization (BIO)

June 3, 2026

The Honorable Brett Guthrie
Chair
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus Bilirakis
Chair
House Energy and Commerce, Commerce, Manufacturing and Trade Subcommittee
2306 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member House Energy and Commerce, Commerce, Manufacturing and Trade Subcommittee
2408 Rayburn House Office Building

Re: Letter of Support of H.R. 8413, the SECURE Data Act

Dear Representative Guthrie, Pallone, Bilirakis, and Schakowsky:

On behalf of the undersigned organizations representing America's telecommunications and technology ecosystem, we write to commend you, Vice Chairman Joyce, and the members of the House Energy and Commerce Committee's Data Privacy Working Group for your leadership in introducing the SECURE Data Act. We are pleased to see a common sense, balanced approach to such a critical issue and we urge the Committee to move expeditiously to schedule a markup of this important legislation.

The SECURE Data Act represents a critical step toward establishing the unified national privacy framework that American consumers, businesses, and innovators urgently need. In the absence of a federal standard, Americans are left navigating an increasingly inconsistent patchwork of state privacy laws that creates confusion for consumers and significant compliance challenges for businesses operating across state lines. A single national framework will provide consumers with consistent and meaningful protections

regardless of where they live, while also delivering the regulatory certainty necessary for companies to continue investing, innovating, and competing globally.

Importantly, the SECURE Data Act strikes the right balance between strong consumer protections and a workable compliance structure that supports innovation and economic growth. The legislation preserves key consumer rights, including the ability to access, correct, and delete personal data, while avoiding overly burdensome or conflicting requirements that could hinder investment in next-generation communications infrastructure and digital services.

As providers and innovators serving millions of American consumers and businesses every day, we believe a clear and consistent national privacy standard is essential to maintaining trust in the digital economy and ensuring continued U.S. leadership in communications and technology innovation. The current fragmented approach creates uncertainty for consumers, increases operational complexity, and diverts resources away from innovation and deployment.

We appreciate your leadership on this issue and respectfully encourage the Committee to quickly advance the SECURE Data Act through markup and consideration by the full House. Establishing a durable national privacy framework is long overdue, and we stand ready to work with you and the Committee to advance this important legislation.

Sincerely,

Computer & Communications Industry Association (CCIA)

Consumer Technology Association (CTA)

CTIA

INCOMPAS

NCTA—The Internet & Television Association

NetChoice

Software & Information Industry Association

TechNet

USTelecom—The Broadband Association

CC: Representative John Joyce, M.D., Vice Chair of the Energy and Commerce Committee Members, House Commerce, Manufacturing and Trade Subcommittee

June 3, 2024

The Honorable Brett Guthrie
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Richard Hudson
Chairman
Subcommittee on Communications & Technology
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Doris Matsui
Ranking Member
Subcommittee on Communications & Technology
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Guthrie, Ranking Member Pallone, Chairman Hudson, and Ranking Member Matsui:

The Security Industry Association (SIA) applauds the Communications & Technology Subcommittee for conducting a hearing on Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law. We write to you today to express our support for H.R. 8413, the SECURE Data Act. The SECURE Data Act is the product of more than a year of work by the House Privacy Working Group. SIA had a chance to participate in the process of sharing industry insights with the working group, and we are encouraged to see further efforts to continue the many years of work that has been done to bring consumer protections into the digital age while ensuring that U.S. businesses continue to lead in a globally competitive environment.

SIA is a nonprofit trade association representing more than 1,700 companies that provide safety and security products essential to protecting lives, property, businesses, schools, and critical infrastructure throughout the U.S. and employ thousands of technology leaders. Many of these companies are small businesses committed to the mission of protecting our country, our citizens and our economy. The security industry as a whole contributes over $430 billion to the economy and supports more than 2.1 million jobs in the United States.

Our industry welcomes the introduction of comprehensive legislation that would establish a single national privacy standard, building upon a consensus model of state privacy frameworks with proven, strong consumer protections. A clear nationwide standard, like the one set by the SECURE Data Act, would strengthen trust, help individuals exercise meaningful control over their information, and give businesses the certainty needed to innovate, protect data, and drive growth. Like most state privacy framworks, it would also ensure data can be used effectively for security, anti-fraud and public safety purposes. Most importantly, the bill would preclude a confusing patchwork that harms consumers and small businesses.

While many states have adopted comprehensive privacy laws that generally fit the consensus framework, a few state laws like the Illinois Biometric Information Protection Act (BIPA) still differ in a number of ways, and states have other privacy laws (like biometrics laws) that impose additional obligations. Companies and consumers alike already have to navigate the complex patchwork of state

laws, and the situation will grow worse as more laws become effective and states continue to issue state-specific regulations under their laws. This patchwork approach has numerous detrimental effects. The current fragmented landscape generates consumer confusion as to what rights they have; creates inconsistencies and gaps in coverage from state-to-state; and drives up inefficient compliance costs with no benefit.

Additionally, we are encouraged to see that the SECURE act relies on State Attorneys General and the Federal Trade Commission for enforcement of the law, rather than a private right of action. Where state laws establish private rights of action (e.g., BIPA), they lead to litigation abuse that benefits plaintiffs' attorneys regardless of any tangible benefit for consumers. We have seen the impact firsthand under the deeply flawed BIPA where "sue-and-settle" lawsuits have been filed against many of our members and their customers in Illinois, even though no actual consumer harm is alleged. As a result, today there are many innovative industry products that suppliers refuse to provide to Illinois businesses and consumers due to the litigation risk, despite wide availability elsewhere, cutting off access to effective technologies for home and building security, workplace safety, security investigations and emergency response.

SIA is committed to engaging with our industry and working with leaders in Congress in support of a workable and effective national data privacy standard. We encourage you to advance H.R. 8413, and are happy to continue working with your offices and the committee to support the legislation.

Respectfully Submitted,

Don Erickson
Chief Executive Officer
Security Industry Association
Silver Spring, MD
www.securityindustry.org

Staff Contact: Lauren Bresette, lbresette@securityindustry.org

Center for AI and Digital Policy

June 3, 2026

Chairman Brett Guthrie and Ranking Member Frank Pallone Jr.
Chairman Gus Bilirakis and Ranking Member Jan Schakowsky
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building, Washington, DC 20515

Re: CAIDP Statement for the Record — Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law

Dear Chair Guthrie, Ranking Member Pallone, Chair Bilirakis, Ranking Member Schakowsky, and Members of the Committee,

We write regarding the Energy Subcommittee's hearing on "**Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law.**"[1] We support a comprehensive, baseline federal data privacy law. This work is made even more pressing in the face of risks to public safety, civil liberties, and national security posed by advanced AI systems. Many machine learning systems rely on the collection of detailed, personal data, which violate privacy and is now being used for mass surveillance.[2] This problem is compounded by the lack of accountability and oversight of unscrupulous business practices that treat American's sensitive personal information as a mere commodity.

[1] U.S. House Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, *Hearing: Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law*, (Jun. 3, 2026), https://energycommerce.house.gov/posts/chairmen-guthrie-and-bilirakis-announce-hearing-on-establishing-a-federal-data-privacy-law; Committee Majority Staff, *Subcommittee on Commerce, Manufacturing, and Trade Hearing on June 3, 2026* Jun. 1, 2026, https://d1dth6e84htgma.cloudfront.net/06_03_2026_Data_Privacy_Legisative_Hearing_Memo_0e5c64d462.pdf

[2] The Conversation, *US government ramps up mass surveillance with help of AI tech, data brokers – and your apps and devices*, (Apr. 21, 2026), https://theconversation.com/us-government-ramps-up-mass-surveillance-with-help-of-ai-tech-data-brokers-and-your-apps-and-devices-277440; CAIDP, *Comments to the Privacy and Civil Liberties Oversight Board regarding the Role of Artificial Intelligence in Counterterrorism*, (Jul. 1, 2024), https://documents.pclob.gov/prod/DynamicImages/Generic/cb8294a3-c924-44c8-9f55-4e61aa81dd4a/CAIDP-Comment-PCLOB-NRPC-07012024_CR.pdf

However, the Secure Data Act (SDA) does not offer meaningful privacy protections for Americans. It falls below the thresholds of previous legislative proposals (most recently the APRA[3]) and should not proceed. Enactment of the SDA would be a significant setback for the privacy rights of Americans. We recommend the following:

1. **A federal privacy law should establish meaningful privacy protections. This Committee should build on the discussion draft of the Americans' Privacy Rights Act**
2. **Congress should enact a comprehensive, baseline federal privacy law, not preempt stronger state privacy laws that safeguard American consumers**

ABOUT CAIDP

The Center for AI and Digital Policy (CAIDP) is an independent research and education organization based in Washington, D.C.[4] CAIDP's mission is to ensure that artificial intelligence (AI) serves the public interest based on fundamental rights, democratic institutions, and the rule of law. CAIDP advises governments and international organizations on AI and digital policy.[5] CAIDP routinely provides nonpartisan advice to Congressional committees on matters involving AI.[6] We also publish the annual *Artificial Intelligence and Democratic Values* report – the "***CAIDP AI Index"*** –, rating and ranking national AI policies and practices across 90 countries.[7]

AMERICANS ARE DEEPLY CONCERNED ABOUT DATA PRIVACY

Across party lines, Americans are concerned about their privacy, and young Americans are overwhelmingly concerned about the privacy of their financial data.[8] A recent poll found that **61% of Americans** say limiting access to their personal data is very important.[9] Pew found that

[3] 118th Congress, 2nd Session, H.R. 8818, American Privacy Rights Act of 2024, https://d1dth6e84htgma.cloudfront.net/H_R_8818_American_Privacy_Rights_Act_of_2024_a265f50b54.pdf ; See also, H.R. 8818 – American Privacy Rights Act of 2024, https://www.congress.gov/bill/118th-congress/house bill/8818/text

[4] CAIDP, https://www.caidp.org/

[5] CAIDP, Statements, https://www.caidp.org/statements/

[6] CAIDP, Statements, https://www.caidp.org/statements/

[7] CAIDP, Artificial Intelligence and Democratic Values 2025, https://www.caidp.org/reports/aidv-2025/

[8] Ipsos, *Privacy is important to Americans. Here's the data they're worried about*, Ipsos Consumer Tracker, (May 12, 2025), https://www.ipsos.com/en-us/privacy-important-americans-heres-data-theyre-worried-about

[9] YouGov, *Data privacy day US 2026: How concerned are Americans about data security?*, (Jan. 13, 2026),

81% of Americans are very or somewhat concerned with how companies use the data they collect about them.[10] Pew also found that **72% Americans want more government regulation** of what companies can do with their customers' personal information.[11] Consumer Reports survey found that **78% of Americans, would support a law regulating how companies can collect, store, use, and disclose our personal data**. A recent Gallup poll found that **80% of U.S. adults believe the government should maintain rules for AI safety and data security**, even if it means developing AI capabilities more slowly.[12]

CAIDP RECOMMENDATIONS

Data-driven business practices are impacting Americans' affordability through discriminatory and extractive pricing practices, including daily essentials and groceries.[13] Americans' opportunities and benefits are moderated through opaque automated decision-making systems that determine employment, credit, and housing.[14] The unregulated processing of personal data threatens Americans' rights and democratic foundations through profiling and mass surveillance.[15] Alarmingly, Americans' genetic data is also being commoditized with serious national security risks of such data being for sale to foreign

https://yougov.com/en-us/articles/53862-data-privacy-day-us-2026-how-concerned-are-americans-about-data-security

[10] Pew Research Center, *How Americans View Data Privacy,* Report, (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[11] *Id*.

[12] Gallup, *Americans Prioritize AI Safety and Data Security,* (Sept. 17, 2025), https://news.gallup.com/poll/694685/americans-prioritize-safety-data-security.aspx

[13] CAIDP, *Comments to the Federal Trade Commission in response to the ANPRM on Proposed Rule on Unfair or Deceptive Fees in Online Food Delivery Services*, (May 18, 2026), https://www.linkedin.com/posts/caidp-ftc-price-discrimination-may-18-ugcPost-7462577150311825408-aBn1/; FTC, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer

[14] Testimony and statement for the record of CAIDP President Merve Hickok, *Advances in AI: Are We Ready For a Tech Revolution?, House Committee on Oversight and Accountability: Subcommittee on Cybersecurity, Information Technology, and Government Innovation*, (Mar. 8, 2023), pg. 4, https://oversight.house.gov/wp-content/uploads/2023/03/Merve-Hickok_testimony_March-8th-2023.pdf; CAIDP, *Statement to House Energy and Commerce Committee on Safeguarding Data and Innovation: Building the Foundation for the Use of Artificial Intelligence* (Oct.18, 2023), https://www.caidp.org/app/download/8482422563/CAIDP-HECC-AI-10182023%20.pdf?;

[15] CAIDP, *Comments to the Privacy and Civil Liberties Oversight Board regarding the Role of Artificial Intelligence in Counterterrorism*, (Jul. 1, 2024), https://documents.pclob.gov/prod/DynamicImages/Generic/cb8294a3-c924-44c8-9f55-4e61aa81dd4a/CAIDP-Comment-PCLOB-NRPC-07012024_CR.pdf

adversaries. None of these egregious privacy risks is lost on this committee. Yet, **after several discussions and multiple rounds of feedback, it is now a test of public trust whether Congress can pass meaningful[16] privacy legislation to protect Americans.**

To be clear, the Secure Data Act ("SDA"), as it currently stands,[17] will not solve these problems. The SDA lacks a private right of action and preempts current state protections and diminishes the ability of states to respond to new privacy challenges. The SDA misses many essential elements of modern privacy laws, including privacy assessments, risk mitigation, privacy enhancing technologies (PETs), and algorithmic transparency. While the SDA seeks to limit the collection to what is "adequate, relevant, and reasonably necessary" and requires consent for incompatible secondary uses, it is more procedural rather than substantive. Robust data minimization requires default restrictions placed on the purpose for which data is collected and used.[18] **The SDA legitimizes the warning label approach to automated decision-making, even for sensitive personal data. It offers little more than "notice and consent" which treats Americans' privacy as a tick-mark exercise rather than a fundamental right.[19]**

The rapid advancements in AI systems demand a more effective requirement for "human review and oversight" because self-learning machine-learning systems modify the assessment process without human intervention or review.[20] The 2024 House AI Taskforce Report found that "Improper use of AI can violate laws and deprive Americans of our most important rights."[21] The federal privacy law should establish baseline protections for privacy

---

[16] Forbes, *How DNA Companies Like Ancestry And 23andMe Are Using Your Genetic Data*, (Dec. 5, 2018), https://www.forbes.com/sites/nicolemartin1/2018/12/05/how-dna-companies-like-ancestry-and-23andme-are-using your-genetic-data

[17] Text - H.R.8413 - 119th Congress (2025-2026): SECURE Data Act. (Apr.21,2026). https://www.congress.gov/bill/119th-congress/house-bill/8413/text

[18] Jordan Francis, *Data Minimization's Substantive Turn: Key Questions and Operational Challenges Posed by New State Privacy Legislation,* (Jun. 5, 2025), https://dx.doi.org/10.2139/ssrn.5309096

[19] CAIDP, *Comment to FTC on COPPA* (Mar. 11, 2024), https://downloads.regulations.gov/FTC-2024-0003-0262/attachment_1.pdf; Marc Rotenberg, *Artificial Intelligence and Democratic Values: The Role of Data Protection*, European Data Protection Law Review, Issue. 4, pg. 496, 2021, https://doi.org/10.21552/edpl/2021/4/6

[20] Marc Rotenberg, *CJEU PNR Decision Unplugs the "Black Box"* ,(2022) 8(3) European Data Protection Law Review 431; CAIDP, *Comments to the Dutch Data Protection Authority on Automated Decision-Making*, (May 26, 2026), https://media.licdn.com/dms/document/media/v2/D4E1FAQHv7e76ytC-lg/feedshare-document-sanitized-pdf/B4EZ5fzDkHHEA8-/0/1779723681060?

[21] Bipartisan House Task Force Report on Artificial Intelligence, 118th Congress, pg. xii, (December 2024), https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf

and principles for AI governance, while allowing states to enact stronger protections where necessary.[22]

1. A federal privacy law should establish meaningful privacy protections

A federal privacy law should set minimum standards for data privacy and security, including requirements for automated decision making, Privacy Enhancing Technology, transparency, contestability, and impact assessments.[23] It should **enumerate rights and protections for individuals**, including the right to know when automated decision-making is used, the right to access the basis of automated decision-making, and the right to opt-in in high-risk AI uses (e.g., profiling for employment or lending).

A federal privacy law should also **establish obligations for businesses who choose to collect and use personal data**. Requirements such as privacy and impact assessments for individuals affected by automated decision making, and regular auditing should be included in the federal law to ensure compliance and reduce friction. Impact assessments for high-risk applications (e.g., healthcare, credit scoring) and auditing mechanisms for reliability and accuracy.[24]

(a) Data Minimization Mechanisms: Personal data collection must be "necessary, proportionate, and limited" to the specified purpose.[25] Crucially, a federal privacy law must discard the "opt-out" model of data collection that unduly burdens consumers. The opt-out

[22] CAIDP, *Comments to the House Energy and Commerce Privacy Working Group regarding the federal data privacy and security framework* (Apr. 11, 2025); CAIDP, *Statement to House Energy and Commerce Committee on Mark-Up Hearing on H.R. 8188*, (Jun. 27, 2024); Marc Rotenberg, *The Need for a Strong Privacy Law,* New York Times, Op-Ed, Mar. 15, 2021, https://www.nytimes.com/2021/03/15/opinion/letters/privacy-data.html

[23] Marc Rotenberg, *Fair AI Practices*, Communications ACM, (Oct. 12, 2022), https://cacm.acm.org/blogcacm/fair-ai-practices/

[24] CAIDP, *Statement to Senate Commerce Committee on The Need to Protect American's Privacy and the AI Accelerant,* (Jul. 10, 2024); Marc Rotenberg, *Artificial Intelligence and the Right to Algorithmic Transparency*, The Cambridge Handbook of Information Technology, Life Sciences and Human Rights. Ed. Marcello Ienca, et al. Cambridge: Cambridge University Press, 2022. 153–165. Print. Cambridge Law Handbooks, https://doi.org/10.1017/9781108775038.015 ; Marc Rotenberg*, Fair AI Practices, Communications* ACM, Oct. 12, 2022, https://cacm.acm.org/blogcacm/fair-ai-practices/; ACM Technology Policy Council, *STATEMENT ON PRINCIPLES FOR RESPONSIBLE ALGORITHMIC SYSTEMS*, (Oct. 26, 2022), https://www.acm.org/binaries/content/assets/public-policy/final-joint-ai-statement-update.pdf

[25] CAIDP, *Statement to House Energy and Commerce Committee on Mark-Up Hearing on H.R. 8188*, (Jun. 27, 2024)

approach is administered through blanket and unintelligible privacy practices that are woefully inadequate and meaningless, causing "consent fatigue" rather than informed consent.[26]

Regarding existing protections in state laws, the One-Stop Opt-Out Platform System (OOPS),[27] currently used by over 100 million Americans is now required by at least 12 state laws. OOPS allows consumers to practice their privacy rights across all affiliated businesses in a single step. The company-by-company opt-out model of the SDA puts an unreasonable burden on consumers and benefit businesses at the expense of consumers.

A new federal data privacy law should also incorporate a deletion mechanism parallel to California's Data Removal and Opt-Out Platform (DROP),[28] which is currently used by over 40 million Americans. DROP is an accessible deletion mechanism that allows people to request data brokers delete their personal information in one step, rather than forcing them to individually contact hundreds of brokers.

(b) Privacy Enhancing Technologies: A federal law would be inadequate without **requiring "implementation of PETs"** defined precisely as techniques that **"minimize or eliminate the collection of personal data."**[29] "The aim of PETs is not to enable further transfers of personal

[26] CAIDP, *Comment to FTC on COPPA,* (Mar. 11, 2024), https://downloads.regulations.gov/FTC-2024-0003-0262/attachment_1.pdf ; Marc Rotenberg, *Artificial Intelligence and Democratic Values: The Role of Data Protection,* European Data Protection Law Review, Issue. 4, pg. 496, 2021, https://doi.org/10.21552/edpl/2021/4/6

[27] Competition Policy International, *States Step Up Scrutiny of Businesses' Compliance With Data Opt-Out Signal*s, (May 14, 2026), https://www.pymnts.com/cpi-posts/states-step-up-scrutiny-of-businesses-compliance-with-data-opt-out-signals/; CalMatters, *Why a new California law could change the way all Americans browse the internet*, (Nov. 2, 2025), https://calmatters.org/economy/technology/2025/11/california-browser-settings-benefit-nation/

[28] CalPrivacy, https://privacy.ca.gov/drop/

[29] Marc Rotenberg, *Eurocrats Do Good Privacy: The contrast between a decorated cryptographer in Europe and one trying to avoid prosecution in the United States is more than curious*, Wired, May 1, 1996, (describing early government efforts to promote "Privacy Enhancing Technologies"), https://www.wired.com/1996/05/eurocrats/. See also, Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in Technology and Privacy: The New Landscape 143–67 (eds., Philip E. Agre & Marc Rotenberg 1997)

data but rather to limit the collection of personal data in the first instance."[30] The implementation of PETs should follow these principles:

i. Genuine PETs reduce privacy and security risks as data that is not collected cannot be misused by the data collector or be subject to data breach.
ii. Genuine PETs protect vulnerable groups, particularly children, e.g. from targeted behavioral advertising
iii. Genuine PETs are aligned with well-established privacy norms, e.g. privacy by design and default
iv. PETs typically seek to implement Fair Information Practices, and where possible, to minimize or eliminate the collection of personally identifiable information.
v. Genuine PETs encourage the development of innovative techniques that are less dependent on the collection of personal data.
vi. Genuine PETs minimize processing and are therefore aligned with emerging norms for AI policy that consider the environmental impact of big data models.
vii. Genuine PETs are aligned with democratic values as they reduce the risk of mass surveillance.

(c) Purpose Limitations: The purpose limitation principle ensures that data is collected for a **specific, explicit, and legitimate purpose** and is not further processed in ways incompatible with that purpose.[31] A federal privacy law should **limit data collection** strictly to what is necessary for the stated purpose.[32] For instance, personal health records or social media activity should not be collected or used in employment decisions unless legally permissible. Additionally, businesses must not use data collected for one purpose (e.g., loan decisions) and repurpose for another (e.g., employment) without obtaining explicit consumer consent.[33] This is even more urgent because of the rapid embedding of AI-driven business practices. For example, general-purpose AI models are not built for a specific context or

[30] CAIDP, *Statement to OSTP on a US AI Action Plan,* (Mar. 14, 2025), CAIDP, *Statement to OSTP on Privacy Enhancing Technologies*, (Jul. 8, 2022), https://www.caidp.org/app/download/8402029763/CAIDP-PETS-OSTP-07082022.pdf
[31] The Irish Data Protection Commission, *Principles of Data Protection*, https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection
[32]CAIDP, *Comment to the UK Information Commissioners Office (ICO) Consultation on Purpose limitation in the generative AI lifecycle*, (Apr. 12, 2024)
[33] CAIDP, *Comments to the California Privacy Protection Agency (CalPrivacy) on ADMT Regulations* (Jan. 2025)

condition of use, allowing for a scale and variety of applications that create new privacy vulnerabilities.[34]

(d) Transparency and Contestability: One of the most significant AI policy issues today is algorithmic transparency.[35] Many state laws now afford a level of transparency and contestability for automated decision making.[36] Credit determinations, employment assessments, educational tracking, as well as decisions about government benefits, border crossings, communications surveillance and even inspections in sports stadiums rely on black box techniques that produce results that are unaccountable, opaque, and often unfair.[37] Federal privacy law should require meaningful algorithmic transparency – the data, logic, and factors underlying an AI or automated decision, and provide for "contestability" – the right to contest automated decisions.[38]

(e) Prohibition on profiling: Real-world deployments of AI for user profiling, behavioral modification, and online advertising are taking place without consideration of the potential harms. Attempts to profile people based on behavior or personal characteristics may escalate misuse, biased and discriminatory decision-making, false identification, and mass surveillance in public spaces.[39] In worst cases, AI systems without scientific validity (such as biometric categorization, predictive policing, and emotion analysis) may be used for profiling.[40] A federal data privacy law should prohibit profiling based on personal data.

---

[34] OECD, *The AI Data Challenge: How do we protect privacy and other fundamental rights in an AI driven world?* (Oct. 19, 2023), https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-aidriven-world

[35] CAIDP, *AI and Democratic Values* (2026), https://www.caidp.org/reports/caidp-index-2026/

[36] IAPP, *Notable AI, privacy bills hit finish line in Illinois, Connecticut and New York,* (May 28, 2026) https://iapp.org/news/a/notable-ai-privacy-bills-hit-finish-line-in-illinois-connecticut-and-new-york

[37] Marc Rotenberg, *Artificial Intelligence and the Right to Algorithmic Transparency*, The Cambridge Handbook of Information Technology, Life Sciences and Human Rights. Ed. Marcello Ienca, et al. Cambridge: Cambridge University Press, 2022. 153–165. Print. Cambridge Law Handbooks, https://doi.org/10.1017/9781108775038.015

[38] CAIDP, *Statement to House Financial Services Committee Hearing on Updating America's Financial Privacy Framework for the 21St Century,* (Mar. 17, 2026); *See,* Consumer Financial Protection Bureau, *Consumer Financial Protection Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms,* (May 26, 2022) ,https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/

[39] CAIDP, *Statement to the UK Home Office on New Legal Framework for Law Enforcement Use of Biometrics, Facial Recognition and Similar Technologies* (Feb. 11, 2026), https://www.linkedin.com/posts/caidp-uk-biometrics-11-feb-2026-ugc

[40] CAIDP, *Comments to the UK Information Commissioners Office (ICO) on the Draft Guidance about*

(f) Private Right of Action: A federal privacy law should also afford a private right of action. We recognize that class actions that provide fees to attorneys but little benefit to class members or meaningful changes in business practices are not useful. We favor a private right of action only when the outcomes are aligned with the interests of class members and the intent of the legislation enacted by Congress.[41]

(g) Creation of a Privacy Agency: The creation of a federal **privacy agency –** a privacy protection commission was a key component of the original privacy protection scheme developed by the Congress in the early 1970s but was never enacted.[42] With the ever-expanding uses of personal data it becomes increasingly difficult to identify problems and resolve complaints. A privacy agency could prove invaluable.[43] The United States is one of the few countries in the world without a federal agency with the competence and resources to assess emerging privacy challenges.

2. A federal privacy law should not preempt state legislation

Many U.S. states have already enacted data privacy and AI regulations.[44] A federal law should not preempt state laws that already provide important safeguards for American consumers. Preemption of state legislation will also hinder regulatory innovation to meet the rapidly emerging risks of advanced AI systems.[45] States must retain the ability to respond to new challenges as they emerge. CAIDP has consistently urged policymakers to reject proposals that restrict the authority of state lawmakers to address privacy, data protection, and AI governance challenges.[46]

Automated Decision Making, including Profiling, (May 29, 2026)

[41] Marc Rotenberg, *A Federal Privacy Law is Desperately Needed*, Letter to Editor, Washington Post, (Apr. 4, 2022), https://www.washingtonpost.com/opinions/2022/04/04/federal-privacy-law-is-desperately-needed/

[42] Marc Rotenberg, *In Support of a Data Protection Board in the United States,* Government Information Quarterly*,* Vol. 8, No. 1, pgs, 79-93, https://archive.epic.org/dpa/Rotenberg-DPA-1991-GIQ.pdf

[43] *Id.*

[44] National Conference of State Legislatures (NCSL), *Consumer Privacy 2025 Legislation, https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy*; NCSL, *3 Trends Emerge as AI Legislation Gains Momentum*, (Jan. 23, 2025), https://www.ncsl.org/state-legislatures-news/details/3-trends-emerge-as-ai-legislation-gains-momentum

[45] CAIDP, *Comments to the House Energy and Commerce Privacy Working Group regarding the federal data privacy and security framework*, (Apr. 11, 2025)

[46] CAIDP, *Statement to Senate Commerce Committee on The Need to Protect American's Privacy and the AI Accelerant,* Jul. 10, 2024

State consumer protection laws, currently in force, prohibit companies from acting deceptively or unfairly in their collection and use of consumers' data. State attorneys general enforce data breach notification requirements, enforce privacy and consumer protection laws to address deceptive and/or unfair business practices, and enforce federal privacy law.[47] There has been bipartisan consensus as attorneys general enforce privacy and online safety across the country.[48] Enactment of SDA would be a significant step backward and undermine these safeguards.

States are passing new laws to protect consumer data, such as one in Oregon regarding data collected by motor vehicles and the collection of biometric data through neurotechnology.[49] The National Conference of State Legislatures (NCSL) has also urged congress to reject any preemption provisions in updating consumer privacy and financial privacy laws.[50] The SDA would displace state laws while providing weaker protections in key areas. The SDA would eliminate existing state safeguards and prevent states from addressing future privacy and AI risks.

The American Privacy Rights Act (APRA discussion draft introduced by Chair Cantwell and Chair Rodgers) is a better starting point. The APRA contained strong provisions that would address the pressing challenges of AI systems relating to privacy, data security, algorithmic

[47] National Association of Attorneys General, *Privacy, Consumer Protection Issues*, https://www.naag.org/issues/consumer-protection/consumer-protection-101/privacy/

[48] Ken Paxton, Office of the Attorney General of Texas, *Attorney General Ken Paxton Launches Investigations into Character.AI, Reddit, Instagram, Discord, and Other Companies over Children's Privacy and Safety Practices as Texas Leads the Nation in Data Privacy Enforcement*, News Releases, Dec. 12, 2024, https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-investigations-characterai-reddit-instagram-discord-and-other; Office of the Attorney General for the District of Columbia, *AG Racine Announces Google Must Pay $9.5 Million for Using "Dark Patterns" and Deceptive Location Tracking Practices that Invade Users' Privacy*, Newsroom, Dec. 30, 2022, https://oag.dc.gov/release/ag-racine-announces-google-must-pay-95-million

[49] NCSL, *As AI Tools Become Commonplace, so Do Concerns*, (Nov. 11, 2025), https://www.ncsl.org/state-legislatures-news/details/as-ai-tools-become-commonplace-so-do-concerns

[50] NCSL, *NCSL Concerns with Preemption in GLBA Modernization Discussion*, (Mar. 26, 2026), https://www.ncsl.org/resources/details/ncsl-concerns-with-preemption-in-glba-modernization-discussion

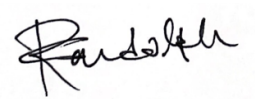
transparency, and accountability.[51] We support that initiative with the strong recommendation to remove efforts to tie the hands of state lawmakers that are addressing similar challenges.[52]

We thank you for the consideration of our views and we request that this statement be entered into the hearing record.

Sincerely,

Marc Rotenberg
CAIDP Executive Director

Merve Hickok
CAIDP President



Christabel Randolph
Associate Director

Taja Nadeau
Law Clerk

Nienyin (Nasrin) Lin
Law Clerk

Elizabeth Barwick
Research Assistant

Lillian Smith
Research Assistant

Grace Van Benschoten
Research Assistant

[51] U.S. Senate Committee on Commerce, Science and Transportation, *Committee Chairs Cantwell, McMorris Rodgers Unveil Historic Draft Comprehensive Data Privacy Legislation,* Press Release, (Apr.7, 2024), https://www.commerce.senate.gov/2024/4/committee-chairs-cantwell-mcmorris-rodgers-unveil-historic-draft comprehensive-data-privacy-legislation;

[52] CAIDP, *Statement to Senate Commerce Committee on The Need to Protect American's Privacy and the AI Accelerant*, Jul. 10, 2024; Congressional Research Service, *Preemption and Privacy Law,* R48667, (Aug. 29, 2025), https://www.congress.gov/crs-product/R48667

The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org

The Leadership Conference

June 3, 2026

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

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

Dear Chair Bilirakis and Ranking Member Schakowsky,

On behalf of The Leadership Conference on Civil and Human Rights' Center for Civil Rights and Technology (Center), we thank you for the opportunity to submit our views regarding the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, or SECURE Data Act. The Leadership Conference is a coalition charged by its diverse membership of more than 240 national organizations to promote and protect the rights of all persons in the United States. We ask for this letter to be entered into the record of the Subcommittee on Commerce, Manufacturing, and Trade hearing titled *Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law* on June 3, 2026. We have supported comprehensive federal privacy legislation in the past and as a coalition have called for laws that meaningfully regulate data collection and use, limit harmful data practices, and prevent discrimination.

Public opinion is clear: people have become increasingly aware of how their data is being collected and used and, unsurprisingly, they are fearful. People want their privacy protected.

- In a Pew Research survey, 81% of respondents said they are concerned about how companies use the data they collect about them, with 61% having little to no understanding of what is being done with their data.

The Leadership Conference

- The results also show that most (73%) believe they have little or no control over what companies do with their data.
- When it comes to AI, 81% of people surveyed said they fear their personal information will be used in ways they won't be comfortable with or that weren't originally intended. [1]
- Consumer Reports found that 78% of people across party lines would support a law regulating how companies can collect, store, share, and use their personal data.[2]

The Leadership Conference has weighed in with the full Energy & Commerce Committee and its subcommittees many times over the past five years regarding a comprehensive federal privacy and data security law.[3] Our position has remained consistent over this time: we strongly support the need for federal legislation, but any law passed by Congress must be protective of civil rights. We stand behind the following language, first shared with the full committee following the removal of civil rights protections from the American Privacy Rights Act (APRA) and shared again with the House Republican Privacy Working Group:

> *"Privacy rights and civil rights are no longer separate concepts — they are inextricably bound together and must be protected. Abuse of our data is no longer limited to targeted advertising or data breaches. Instead, our data are used in decisions about who gets a mortgage, who gets into which schools, and who gets hired — and who does not. All too often, those data-driven decisions come with discriminatory outcomes, which have been compounded as algorithmic technologies and AI have advanced at an unprecedented pace. Individuals who face discrimination on the basis of their race, ethnicity, sex, disability, national origin, sexual orientation, gender identity, immigration status, or religion already contend with rampant harms as a result of invasive and predatory data practices. For example, companies have used AI to discriminate based on these characteristics against job applicants, deny equal access to credit, impair access to healthcare, and unfairly prejudge students' academic prospects. A privacy bill that does not include civil rights protections will not meaningfully protect us from the most serious abuses of our data.*"

Unfortunately, the SECURE Data Act fails to deliver those necessary safeguards at a time of pervasive data collection, algorithmic decision making, and AI-driven profiling. Even worse, the SECURE Data Act

---

[1] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park, "How Americans View Data Privacy," *Pew Research Center,* (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[2] Scott Medintz, "Americans Want Much More Online Privacy Protection Than They're Getting," *Consumer Reports* (Nov. 20, 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/.

[3] Letter from the ACLU, Lawyers' Committee for Civil Rights Under Law, and The Leadership Conference on Civil and Human Rights to The Honorable Cathy McMorris Rodgers, (June 25, 2024), https://civilrights.org/resource/civil-society-letter-house-energy-commerce-committee-privacy-legislation/.

will impede states' efforts to protect their residents' personal data by preempting any privacy laws they may pass.

Relying on an outdated "notice and consent" model does not work today.

The current "notice and consent" model, in which companies provide notice of data collection and implore users to consent to their data being used, is ineffective in both protecting users' privacy and in empowering people to control how their data is used. Unfortunately, instead of meaningfully addressing this issue, the SECURE Data Act fails to include restrictions on data collection and use and instead simply repackages the status quo.

Privacy protections should not depend on individuals' ability or willingness to navigate complex disclosures written in dense legalese. In maintaining the status quo, the SECURE Data Act recklessly puts the burden of protecting their data on individuals, leaving them at the mercy of Big Tech and the companies that use their technologies.

Another issue is the lack of strictures on companies' ability to coerce consent for data collection and use. The SECURE Data Act has no prohibition on coercive practices like dark patterns, to obtain consent, and despite language that *appears* to prohibit a company from limiting a user's access to their services because that person declined to provide their data, the SECURE Data Act allows companies to provide different tiers of services based on a person's willingness to turn over their data. Such a framework is ripe for abuse and could result in coerced consent.

The public wants strong limits, not just more disclosures. According to Consumer Reports, 86% of Americans support federal privacy legislation that truly limits data collection and use, going beyond the simple and past-its-prime notice and consent framework embodied in the SECURE Data Act.[4]

Data and AI are inexorability linked; any data protection bill must include civil rights protections and algorithmic accountability.

As we wrote in the Civil Rights Principles in the Era of Big Data,[5] privacy laws must *"*ensure that data is not used in ways that reinforce existing inequities or create new forms of discrimination*."* The SECURE Data Act, unlike prior bipartisan comprehensive federal privacy legislation considered and passed by the Committee, will allow algorithmic discrimination, digital redlining, biased automated decision making, continued use of opaque AI systems trained on people's personal data, and algorithmic profiling based on AI inferences about individuals.

---

[4] Scott Medintz, "Americans Want Much More Online Privacy Protection Than They're Getting," Co*nsumer Reports,* (Nov. 20 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/.

[5] The Leadership Conference on Civil and Human Rights, "Civil Rights Principles for the Era of Big Data," (Feb. 2024), https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/.

The Leadership Conference

The "protections" in the SECURE Data Act are narrow, incomplete, and riddled with loopholes and exceptions.

In addition to expecting a systemic problem to be addressed by individuals' actions, the SECURE Data Act is riddled with loopholes and exceptions that renders individual choice effectively meaningless.; it will do little to nothing to actually restrict what data companies can collect or how they will use it[6].

While the SECURE Data Act includes provisions addressing sensitive data, the definition is narrow and excludes the processes of making inferences and predictions based on the data collected — both of which may include what should be protected traits, such as gender, religion, political affiliation, disability, and sexual orientation. And despite providing for an "opt-in" for sensitive data, it is undermined by broad exceptions, like for "operational purposes," "product development," "service improvement," and "internal research." The outcome is that companies will continue to collect whatever data they wish and use it in whatever way they wish. The "protections" in the SECURE Data Act are anything but.

Congress should not weaken stronger state protections. Instead we must pass meaningful federal privacy protections.

Simply put, the SECURE Data Act will leave people worse off.

The public deserves a privacy law that limits data collection, includes enforceable civil rights protections, regulates automated AI decision making, and ensures accountability. The SECURE Data Act does not achieve these goals. If Congress wants to help bolster the public's trust in technology — including AI, thereby helping to ensure its sustained use and acceptance — it must address the mounting public skepticism about technology. Congress can do so by pursuing a comprehensive privacy bill that actually protects people and their data.

We stand ready to work with Congress on policies that will protect civil rights, prevent unlawful discrimination, and advance equal opportunity. Should you require further information or have any questions regarding this issue, please feel free to contact Jonathan Walter, senior policy counsel, at walter@civilrights.org

Sincerely,

Alejandra Montoya-Boyer
VP, Center for Civil Rights and Technology

---

[6] Mario Trujillo, "The SECURE Data Act is Not a Serious Piece of Privacy Legislation," *Electronic Frontier Foundation.* (May 6, 2026), https://www.eff.org/deeplinks/2026/05/secure-data-act-not-serious-piece-privacy-legislation.

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

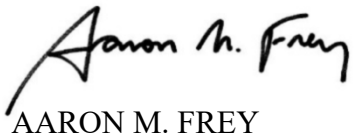
WILLIAM TONG
Connecticut Attorney General

KATHLEEN JENNINGS
Delaware Attorney General

MANA MORIARTY
Executive Director
State of Hawaii
Office of Consumer Protection

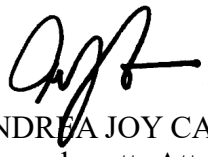
KWAME RAOUL
Illinois Attorney General

[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

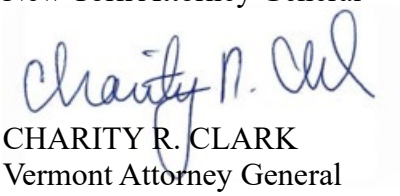
AARON D. FORD
Nevada Attorney General

JOHN M. FORMELLA
New Hampshire Attorney General

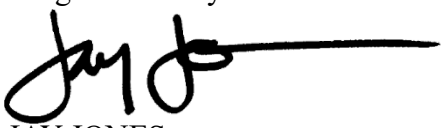
JENNIFER DAVENPORT
New Jersey Attorney General

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

CALIFORNIA PRIVACY PROTECTION AGENCY
400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov

April 27, 2026

The Honorable Brett Guthrie, Chair
The Honorable Frank Pallone, Ranking Member
House Committee on Energy and Commerce
2125 Rayburn House Building
Washington, DC 20515

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

Dear Chair Guthrie and Ranking Member Pallone,

The California Privacy Protection Agency (Privacy Agency)[1] writes in respectful opposition to H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act).[2] All Americans deserve strong, meaningful protections over their personal information. The SECURE Data Act includes preemption language that seeks to strip away a substantial amount of important privacy protections that individuals have today under state privacy laws — including rights that are available to over 100 million Americans. The bill could remove important guardrails on businesses, make exercising privacy rights harder for consumers, and weaken available remedies, leaving Americans less protected. We urge you to consider federal privacy legislation that truly protects Americans by setting a floor, not a ceiling on those rights.

Background

For years, California has played a leading role in developing strong privacy protections. In 1972, California voters established the right of privacy in the California Constitution, amending it to include privacy as one of Californians' "inalienable" rights.[3] California passed the first data breach notification law in 2002 and was the first state to require businesses to post privacy policies outlining their data use practices.[4] In 2018, it became the first state in the nation to adopt a comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA),[5] and

[1] Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians' consumer privacy. The Privacy Agency implements and enforces the California Consumer Privacy Act and the Delete Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.
[2] 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.
[3] Cal. Cons. Art. 1 § 1.
[4] Cal. Civ. Code § 1798.82; National Council of State Legislators, *Summary of Security Breach Notification Laws* (last updated January 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.
[5] Cal. Civ. Code § 1798.100 et seq.

since then over 20 states across the country have enacted similar comprehensive privacy laws.[6]

Furthermore, enhancements to California's privacy law were put to the voters and resoundingly approved. Specifically, in November 2020, over 9.3 million California voters[7] — roughly equivalent to the total combined population of the 10 smallest states by population[8] — ratified Proposition 24, the California Privacy Rights Act, which amended the CCPA by adding new substantive provisions to the law and creating the Privacy Agency, the first authority with full administrative powers focused on privacy and data protection. The CCPA also instructs the Privacy Agency to develop regulations requiring businesses whose collection and use of personal information presents significant privacy and security risks to perform cybersecurity audits and risk assessments on a regular basis.

In recent years, California has continued to adopt legislation to further strengthen privacy protections, including the California Delete Act which strengthens consumer privacy protections with respect to data brokers.[9] The law transferred the administration and enforcement of the state's Data Broker Registry to the Privacy Agency and increased the disclosure requirements for data brokers so that consumers can learn whether a data broker maintains certain types of sensitive data such as children's data or location data and whether they sell or share data with certain third parties. Additionally, the law established a first-in-the-nation global data broker deletion requirement. The mandated deletion tool launched in January 2026 and over 280,000 Californians have already submitted deletion requests. Additionally, the Privacy Agency has enforcement powers under the law that it has already used effectively to bring actions against nearly a dozen data brokers.

The SECURE Data Act Seeks to Remove Existing Rights Leaving Americans Less Protected

The preemption language in the SECURE Data Act is broad and seeks to preempt any state law that "relates to the provision of the Act." Removing the important rights and obligations provided under the CCPA and the Delete Act without providing equivalent protections, as this bill seeks to do, would be a significant step backwards for privacy.

The SECURE Data Act Makes Privacy Harder for Consumers

Many of the state protections that the SECURE Data Act seeks to preempt are tools and requirements that make privacy rights more accessible to consumers. Removing consumer-oriented protections will make it materially harder for consumers to take control of their personal information and exercise their privacy rights, establishing new roadblocks that disadvantage

---

[6] Alabama, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oklahoma, Oregon, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, Utah, and Virginia. *See*, IAPP, US State Comprehensive Privacy Laws Report: 2025 Legislative Session (October 2025), https://prod.iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2025_session.pdf; *See, also,* AL HB 351 (2025), https://alison.legislature.state.al.us/files/pdf/SearchableInstruments/2026RS/HB351-eng.pdf; OK SB 546 (2026), https://www.oklegislature.gov/cf_pdf/2025-26%20ENR/SB/SB546%20ENR.PDF.

[7] California Secretary of State, *Statement of the Vote: General Election November 3, 2020* at 67, https://elections.cdn.sos.ca.gov/sov/2020-general/sov/complete-sov.pdf.

[8] WY – 588,753; VT – 644,663; AK – 737,270; ND – 799,358; SD – 935,094; DE – 1,059,952; RI – 1,114,521; 1,144,694; ME – 1.414.874; NH – 1,415,342; *See*, United States Census Bureau, *Annual Estimates of Resident Population of the United States, Regions, States, District of Columbia, and Puerto Rico: April 1, 2020 – July 1, 2025*, available at https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html.

[9] Cal. Civ. Code § 1798.99.80 et seq.

consumers in favor of business. The SECURE Data Act is substantially weaker for consumers in the following ways, among others:

- **The SECURE Data Act does not require businesses to honor opt-out preference signals, removing an important consumer privacy tool in use today.** Opt-out preference signals (OOPS) are simple tools that allow consumers to easily communicate their privacy preferences to the businesses they interact with, making privacy rights easier and possible to exercise at scale. Without OOPS, consumers face the daunting task of submitting individual opt-out requests to hundreds, if not thousands, of businesses. Under the CCPA and implementing regulations, businesses are required to process OOPS as a valid request to opt out of sale or sharing — allowing consumers to stop the sale and sharing of their personal information with all businesses they interact with online in a single step.[10] Additionally, beginning January 1, 2027, browsers will be required to offer these signals to California consumers.[11] A dozen states, including California, currently require that businesses honor OOPS.[12]

  The SECURE Data Act does not provide a similar requirement — nor does it require browsers to offer OOPS — but instead tasks the Secretary of Commerce with performing a three-year study on this consumer-friendly tool that is already widely used and recognized in states around the country. This would have the effect of stripping over 100 million Americans from an important privacy right that they enjoy today.

- **The SECURE Data Act seeks to eliminate a valuable first-of-its-kind data broker deletion tool.** On January 1, the Privacy Agency launched the Delete Request and Opt-out Platform (DROP), an accessible deletion mechanism that allows consumers to request that all data brokers delete their personal information in one step.[13] DROP, established pursuant to the Delete Act, makes it easy for consumers to take control of their personal information with respect to hundreds of data brokers that are processing and selling their data but with whom they do not have existing relationships. As a testament to the pent-up demand for such a tool, over 280,000 Californians signed up for DROP in the first few months of its availability, and eight other states have considered similar legislation this year.[14] The SECURE Data Act eviscerates this global deletion mechanism and seeks to strip from over 40 million Americans the ability to take advantage of this important privacy tool.

- **The SECURE Data Act significantly reduces important data broker disclosure requirements.** The Delete Act requires data brokers to provide detailed disclosures that provide consumers with important information about how their data is collected and used so that they can make informed decisions regarding their privacy. This includes: (1) disclosures about whether they collect certain types of sensitive personal information, such as a consumer's citizenship data, sexual orientation, precise geolocation, or social

[10] Cal. Civ. Code § 1798.135; 11 CCR § 7025.
[11] Cal. Civ. Code § 1798.136.
[12] California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas.
[13] Cal. Civ. Code § 1798.99.86.
[14] SB 4, February Session 2026 (CT 2026); HB2463, 2026 Regular Session (HI 2026); HB 2913, 104th General Assembly (IL 2026); S2619, 194th General Court (MA 2026); LB 602, 109th Legislature (NE 2026); SB192, 2026 Regular Session (NM 2026); S9088, 2025-2026 Legislative Session (NY 2026); H211, Regular Session 2025-2026 (VT 2026).

security number; and (2) whether they sell or share consumer data with certain types of third parties, including law enforcement, GenAI developers, or foreign actors.[15] For example, a review of data broker disclosures to the Privacy Agency revealed that over two dozen California-registered data brokers had reported selling and sharing data with non-US actors in North Korea, China, Russia, and Iran.[16]

The SECURE Data Act establishes a registry for data brokers but requires minimal disclosures, such as categories of personal information collected and links to privacy policies, which do not provide consumers with sufficient information to evaluate risk.

- **The SECURE Data Act does not prohibit businesses from nudging consumers into sharing their data.** The CCPA prohibits businesses from using dark patterns — deceptive interfaces that impede consumers from making their intended choices — or acceptance of general broad terms of use to obtain consent from a consumer.[17] Additionally, the implementing regulations provide guidance about how businesses can fairly obtain consumer consent, including requirements that the language used is easy to understand and not confusing to the consumer, that there is symmetry in the choices provided, that the choice architecture does not interfere with a consumer's ability to make a choice, and that the choices are easy to execute without unnecessary burden or friction.[18]

  The SECURE Data Act merely requires that consent be "freely given, specific, informed, and unambiguous." Without a prohibition similar to the CCPA, businesses could design confusing consent mechanisms that prevent consumers from making their intended choices.

- **The SECURE Data Act caps requests to exercise privacy rights.** The CCPA does not put a cap on the number of free requests to opt-out, correct, and delete that a consumer can submit per year. In contrast, the SECURE Data Act allows businesses to charge or simply disregard privacy requests in excess of two per year. This could particularly hurt the most vulnerable consumers like domestic violence victims subject to tech stalking, or consumers whose data has been breached, who may need to exercise their rights multiple times per year.

The SECURE Data Act Significantly Weakens Existing Guardrails

Existing state laws, like the CCPA, establish important baseline obligations on businesses' collection and processing of personal information that the SECURE Data Act seeks to undo. Obligations on businesses ensure that consumers receive foundational privacy protections without having to act. These popular standards and requirements, incorporated in many state privacy laws, are significantly weakened or absent in the federal bill. The SECURE Data Act weakens existing guardrails on businesses' collection, use, and sharing of data in the following ways, among others:

---

[15] Cal. Civ. Code § 1798.99.82.
[16] Electronic Privacy Information Center, *The Data Brokers Selling US Data to Foreign Actors, According to California* (March 25, 2026), https://epic.org/the-33-data-brokers-selling-us-data-to-foreign-actors-according-to-california/.
[17] Cal. Civ. Code § 1798.140(h).
[18] 11 CCR § 7004.

- **The SECURE Data Act does not limit how much data businesses can use, retain, and share about consumers.** Consumer privacy laws typically include data minimization obligations on businesses — important baseline standards that limit how much data businesses can collect, process, and share — that apply even if the consumer takes no action. These standards ensure that businesses are collecting and using only the minimum amount of data needed so that consumers' personal information has a default level of protection.

  The data minimization standard included in the SECURE Data Act is weaker than what is included in many state privacy laws. The SECURE Data Act only provides a data minimization standard for data collection. The CCPA, in contrast, requires businesses to apply data minimization principles to their collection, use, retention, and sharing of consumers data. This ongoing requirement is crucial because it ensures that once data is collected, it is only used as necessary to meet the consumer's expectations. However, guardrails directing businesses to minimize their data use and sharing are entirely absent from the bill.

- **The SECURE Data Act does not adequately restrict the purposes for using consumers' data.** Consumer privacy laws typically establish default purpose limitation rules that businesses must meet — guidelines that specify what purposes a business may use consumer data for. These standards are intended to ensure that a business only uses consumer data in ways they would reasonably anticipate or expect, protecting consumers from unfettered use of their data.

  The CCPA has a strong purpose limitation standard that explicitly requires that the purposes for which data are used are "consistent with the reasonable expectations of the consumer."[19] Additionally, the implementing regulations provide guidance on what considerations indicate a consumer's reasonable expectation, including, among other things: the relationship between the consumer and the business; the type, nature, and amount of personal information collected; and the specificity of the disclosures to consumers.[20] This level of detailed guidance leads to predictability in the marketplace, ensuring that businesses are acting in good faith and using consumer data in a way that would be anticipated or expected.

  The SECURE Data Act, however, provides only that a business may not process personal data for a purpose that is not "reasonably necessary or compatible" with a disclosed purpose. This limited standard does not require a business to consider the expectations or understanding of consumers.

- **The SECURE Data Act does not establish any limits on data retention.** Data retention limits are important to ensure that consumers' personal data is not stored indefinitely and thereby vulnerable to misuse, breach, or theft. Under the CCPA, data retention is governed by the data minimization standard and therefore must be "reasonably necessary and proportionate" to achieve the purposes disclosed to the consumer.[21] Additionally, the CCPA requires businesses to disclose their data retention practices to consumers and

[19] 11 CCR § 7002(b).
[20] 11 CCR § 7002(b).
[21] Cal. Civ. Code § 1798.100(c).

expressly states that businesses shall not retain personal information "for longer than is reasonably necessary" for the disclosed purpose.[22] The SECURE Data Act provides no limits on how long a business may retain consumer data, thus paving the way for data breaches and other harms that come from indefinite data retention.

- **The SECURE Data Act does not offer heightened protection for many types of sensitive personal information that are protected today.** Many state privacy laws provide heightened protections to numerous types of sensitive personal information because misuse or theft of this data can lead to discrimination, harassment, identity theft, and fraud. Yet, the SECURE Data Act's definition of sensitive personal data is much narrower that many existing state privacy laws, and does not include: Social Security numbers and other government identification numbers; financial account information in combination with credentials for access; union membership; the contents of consumers' communications; neural data; and genetic data — all of which are covered under the CCPA's definition of sensitive personal information.[23]

- **The SECURE Data Act does not require risk assessments.** The goal of a risk assessment is to assess whether the risks of processing the personal information outweigh the benefits, to ensure businesses are engaged in responsible processing of consumer data. Under the CCPA and implementing regulations, businesses whose processing of personal information presents a significant risk to consumers' privacy are required to conduct a risk assessment before processing personal information and review the assessment for accuracy at least once every three years thereafter.[24] Most other states with privacy laws require similar data impact assessments. The SECURE Data Act does not mandate assessments, thereby weakening accountability and seeking to eliminate key guardrails over businesses' use of personal information. In addition, because of the preemption provision, the bill would not only throw these existing protections out the window — it would prevent states from requiring them.

The SECURE Data Act Weakens Privacy Enforcement and Compliance

With passage of the California Privacy Rights Act in 2020, millions of Californians voted to create the Privacy Agency and grant it the power to audit and bring administrative actions against businesses under its jurisdiction, creating a dedicated law enforcement entity to protect consumer privacy.[25] California's unique audit authority, in particular, will allow for thorough and transparent compliance oversight, affording insight into industry practices, and evolving norms for how privacy is implemented in practice. The broad preemption in the SECURE Data Act, however, seeks to remove many enforcement options available to protect Americans today, weakening both remedies and compliance. The bill will impede successful enforcement of privacy rights in the following ways, among others:

- **The SECURE Data Act seeks to eliminate a robust multi-layered enforcement system for Americans' privacy rights.** The Privacy Agency was created by the voters of California with the passage of Proposition 24 in part because the voters wanted a dedicated agency to focus on privacy as a complement to the state Attorney General.

[22] Cal. Civ. Code § 1798.100(a)(3).
[23] Cal. Civ. Code § 1798.140(ae).
[24] Cal. Civ. Code § 1798.185(a)(14)(B); 11 CCR § 7150.
[25] Cal. Civ. Code § 1798.199.

In the short time that the Privacy Agency has had enforcement authority with respect to the CCPA, it has already demonstrated its effectiveness in protecting consumer privacy. For example, in the fall of 2024 the Privacy Agency's enforcement division began an investigative sweep of data broker registration compliance with the Delete Act[26] that has resulted in nearly a dozen enforcement actions[27] and led to the development of a special strike force within the division.[28] The federal bill only allows for enforcement of the law by the Federal Trade Commission (FTC) or state Attorneys General. Constraining effective existing privacy enforcers when Americans need greater privacy enforcement disadvantages consumers.

The following enforcement actions by the Privacy Agency are just a few examples of what the federal bill seeks to scale back:

- ***Protecting patients with Alzheimer's disease***. The Privacy Agency brought an action to stop a data broker from selling lists of people with Alzheimer's disease, leaving them vulnerable to targeting by malicious actors.[29]

- ***Fallout from massive data breaches***. The Privacy Agency took action against National Public Data for failing to register after a data breach exposed 2.9 billion records, including the names of Social Security numbers of nearly every American.[30]

- ***Collecting "Scary" Amounts of Information About Americans***. The Privacy Agency took action to stop a data broker from collecting "scary" amounts of information that it could "dig up on someone" and generate profiles about them.[31]

- ***Tracking Americans' Behaviors***. The Privacy Agency took action against an unregistered data broker that profiled Americans based on their behavioral data.[32]

- **The SECURE Data Act incentivizes non-compliance.** The bill hampers strong enforcement by providing businesses with an ongoing 45-day cure period for all violations of the law. Such a window for correction — that, unlike many state privacy laws, never sunsets — encourages businesses to take a wait and see approach to compliance that harms consumers.

---

[26] *CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act* (October 30, 2024), https://cppa.ca.gov/announcements/2024/20241030.html

[27] See, e.g., *CPPA Brings Enforcement Action Against Florida Data Broker* (February 20, 2025), https://cppa.ca.gov/announcements/2025/20250220.html; *Data Broker Promoting Ability to Dig Up 'Scary' Amounts of Information Agrees to Shut Down* (February 27, 2025), https://cppa.ca.gov/announcements/2025/20250227.html

[28] *CalPrivacy Launches Data Broker Enforcement Strike Force* (November 19, 2025), https://privacy.ca.gov/2025/11/calprivacy-launches-data-broker-enforcement-strike-force/

[29] *CalPrivacy Brings New Round of Enforcement Actions Against Data Brokers* (January 8, 2026), https://privacy.ca.gov/2026/01/calprivacy-brings-new-round-of-enforcement-actions-against-data-brokers/

[30] *CPPA Orders Florida Data Broker to Pay Fine* (May 8, 2025), https://cppa.ca.gov/announcements/2025/20250508.html

[31] *Data Broker Promoting Ability to Dig Up "Scary" Amounts of Information Agrees to Shut Down* (February 27, 2025), https://cppa.ca.gov/announcements/2025/20250227.html

[32] *CalPrivacy Fines Marketing Firm for Selling Custom Audiences Without Data Broker Registration* (Dec. 3, 2005), https://cppa.ca.gov/announcements/2025/20251203.html

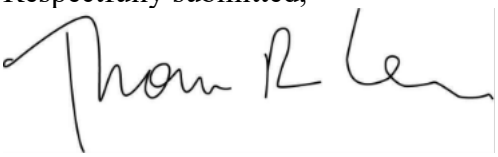
Federal Privacy Laws Traditionally Support States' Ability to Legislate

Traditionally, federal privacy laws have established a baseline of protections and preserved states' abilities to adopt stronger protections for their residents. This is critical for emerging privacy harms that states are well equipped to address. This multi-level governance has proven successful — California laws operate successfully alongside federal counterparts, providing additional protection as California has deemed necessary. Indeed, at least ten federal privacy statutes do not preempt states from enacting additional protections, including the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), Title I of the Electronic Communications Privacy Act (ECPA), the Video Privacy Protection Act, and the Driver's Privacy Protection Act, among others.[33] California's increased protections in these areas have not prevented it from becoming one of the largest economies in the world.[34]

Conclusion

Preemption would strip away important existing state privacy provisions that protect tens of millions of Americans now. That would be a significant step backward in privacy protection at a time when individuals are increasingly concerned about their privacy and security online, and when challenges from data-intensive new technologies such as AI are developing quickly. Furthermore, federal privacy legislation should make privacy easier for Americans, not harder. For these reasons, we respectfully request that the Committee reject this bill and uphold the longstanding approach to federal privacy legislation: establish a baseline for protections while preserving states' authority to adopt stronger laws.

Respectfully submitted,



Tom Kemp
Executive Director
California Privacy Protection Agency

cc: Members, House Committee on Energy & Commerce

[33] 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 1681, et seq.; 18 U.S.C § 2501-2523; 18 U.S.C. § 2710 et seq.; 18 U.S.C. § 2712. *See also*, Employee Polygraph Protection Act, 29 U.S.C § 2009 et seq.; Telephone Consumer Protection Act, 47 U.S.C. § 227; Family Educational Rights and Privacy Act, 20 U.S.C. §1232(g); Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq.

[34] Office of Governor Gavin Newsom, *California is Now the Fourth Largest Economy in the World* (April 23, 2025), https://www.gov.ca.gov/2025/04/23/california-is-now-the-4th-largest-economy-in-the-world/