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

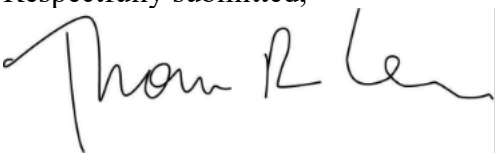
Federal Privacy Laws Traditionally Support States' Ability to Legislate

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/