STATE OF CALIFORNIA

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

April 7, 2025

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

Re: Privacy Working Group – Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce,

We, the undersigned state privacy enforcement authorities, thank the House Committee on Energy and Commerce's Privacy Working Group (Working Group) for soliciting public comments to inform its consideration of a comprehensive data privacy and security law.[1] The undersigned appreciate that the Working Group is considering a federal privacy law. All Americans deserve strong, meaningful protections over the collection, use, and disclosure of their personal information. However, these protections should not come at the expense of protections that consumers already enjoy. States play a crucial ongoing role in addressing emerging privacy challenges. To ensure adequate safeguards, federal privacy laws should establish a floor of protections while allowing states the ability to adopt stronger protections.

States have played a leading role in the development of strong privacy and technology protections. For example, California passed the first data breach notification law in 2002 and today all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have similar laws in place.[2] Similarly, in 2018 California became the first state in the nation to adopt a comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA), and since then nearly 20 states across the country have enacted their own comprehensive privacy laws.[3] Just last year, Colorado became the first state to enact a comprehensive law regulating high risk artificial intelligence systems.[4]

The comprehensive state privacy laws in effect today build upon one another, establishing consistencies among the laws and promoting interoperability. Nearly all of the laws provide consumers with rights of access, deletion and correction and the right to opt out of the sale of personal information. They also establish similar

[1] *Chairman Guthrie and Vice Chairman Joyce Issue Request for Information to Explore Data Privacy and Security Framework*, U.S. House Committee on Energy & Commerce (February 21, 2025), https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework.
[2] 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.
[3] Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, Texas, New Hampshire, New Jersey, Rhode Island, Tennessee, Utah, and Virginia. *See*, IAPP, US State Comprehensive Privacy Laws Report: 2024 Legislative Session (October 2024), https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session.pdf.
[4] Colo. Rev. Stat § 6-1-1701 et seq.

obligations for businesses regarding data minimization, purpose limitations, transparency and risk assessment for certain types of data processing.[5] Differences among the laws are typically minor, such as the processing and revenue thresholds that require compliance with the law.

To the extent that there are differences among state privacy laws, they often reflect the important role that states play in establishing and testing innovative solutions to new privacy problems. For example, the Colorado and Virginia privacy laws, enacted after the CCPA, built on the opt-out rights provided in the CCPA and established a new right to opt-out of data processing for profiling.[6] That consumer right, proven valuable, has been adopted by most states that followed.

These laws are remarkably consistent with one another because of intentional collaboration among the states. The California Privacy Protection Agency (CPPA), for example, is required under the CCPA to "cooperate with other agencies with jurisdiction over privacy laws…to ensure consistent application of privacy protections" and many other state legislatures voluntarily engage with one another when crafting and considering new legislation.[7]

States have also proven capable of amending their existing privacy laws in a timely manner to address evolving privacy challenges. For example, in recent years Colorado amended its privacy law to address privacy concerns posed by new neural data technologies, a trend that has been followed in bills introduced by other states like California and Montana.[8] Similarly, California has amended its law a few times in response to local needs, including to ensure that consumers maintain their privacy protections when interacting with artificial intelligence systems.[9] In contrast to the federal lawmaking process that moves more deliberately to consider amendments, states have demonstrated flexibility and nimbleness to adapt quickly to novel technologies and data practices by changing their laws.

Federal preemption of these established state privacy laws risks removing privacy protections from large numbers of Americans. Residents of the approximately 20 states with comprehensive privacy laws have come to rely upon their current protections. For example, in 2020, millions of Californians voted to establish a floor of privacy protections in California that the legislature cannot amend to "compromise or weaken consumer privacy."[10]

Preemption is also not necessary. Existing federal privacy laws explicitly preserve states' abilities to adopt stronger protections for their residents. For example, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Telephone Consumer Protection Act do not preempt states from enacting additional protections.[11] In fact, interpretive rules have been issued to clarify that FCRA does not prevent states from regulating consumer reporting and, in November 2024, the Consumer Financial Protection Bureau released a report that called on states to consider regulating consumer financial data where the GLBA protections end.[12]

---

[5] IAPP, US State Privacy Legislation Tracker 2025, https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.
[6] C.R.S. § 6-1-1306(1)(a); Va. Code § 59.1-577(A)(5).
[7] Cal. Civ. Code § 1798.199.40(i).
[8] CO HB 1058 (2024); MT SB 163 (2025); CA SB 1223, (2024).
[9] CA AB 1008, (2024).
[10] Proposition 24, Section 3(C)(6), 2020.
[11] 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807; 15 U.S.C. § 1581; 47 U.S.C § 227(f).
[12] 12 C.F.R. Part 1022; Consumer Financial Protection Bureau, *State Consumer Privacy Laws and the Monetization of Consumer Financial Data*, November 2024, https://files.consumerfinance.gov/f/documents/cfpb_state-privacy-laws-report_2024-11.pdf

States have often built upon this symbiotic relationship, enacting laws that augment the protections offered by the federal statutes. For example, California's Confidentiality of Medical Information Act and Financial Information Privacy Act build on protections offered by the federal laws.[13] California's increased protections in these areas have not prevented it from becoming one of the largest economies in the world.[14]

Because of the critical role states play in developing privacy regulation, a federal privacy law should establish a meaningful floor of protections for all Americans while allowing states to adopt stronger protections and address new challenges. States are powerful laboratories for successful privacy protections and should remain empowered to address emerging privacy concerns. State level innovation has contributed greatly to the development of baseline US privacy standards, and states must be able to continue to react and respond to new issues in real time so that regulatory development is not frozen as new technologies advance.

States also provide localized enforcement capabilities that would strengthen a federal privacy law. By incorporating state enforcement powers into federal privacy legislation, Congress can create a more robust, multi-layered protection system for Americans' privacy rights.

The undersigned have established enforcement powers and have demonstrated effectiveness in protecting consumer privacy. States authorities regularly audit businesses to ensure compliance with privacy laws. For example, Connecticut performed a compliance review of business privacy policies within the first six months that its privacy law was in effect.[15] States have also brought critical privacy enforcement actions. In California, for example, both the Attorney General and the California Privacy Protection Agency have brought enforcement actions under the CCPA.[16] In fact, a recent enforcement sweep by the CPPA of data broker compliance with California's Delete Act resulted in more than a half dozen enforcement actions, including one against National Public Data whose data breach last year exposed 2.9 billion records that included names and social security numbers.[17] Additionally, in January the Texas Attorney General took action against Allstate and Arity under their comprehensive privacy law, for unlawfully processing data about the location and movement of Texans' cell phones.[18]

States with privacy laws often have specialized staff uniquely positioned to address the complicated and novel privacy concerns that arise from rapidly evolving technologies such as artificial intelligence, social media, and new data processing methods. The CPPA, for example, has fully staffed legal and enforcement divisions with in-house technical experts to effectively address evolving privacy challenges. Similarly, last year a specialized

---

[13] Cal. Civ. Code § 56.10 et seq.; Cal. Fin. Code § 4051(b).
[14] Office of Governor Gavin Newsom, *California Remains the World's 5th Biggest* Economy (Apr. 16, 2024), https://www.gov.ca.gov/2024/04/16/california-remains-the-worlds-5th-largest-economy/.
[15] Connecticut Attorney General, *Report to the General Assembly's General Laws Committee*, February 1, 2024, https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.
[16] *See Attorney General Bonta Announces Settlement with Sephora* (August 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement; *Honda Settles with CPPA Over Privacy Violations,* (March 12, 2025), https://cppa.ca.gov/announcements/2025/20250312.html.
[17] *CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act* (October 30, 2024), https://cppa.ca.gov/announcements/2024/20241030.html; *CPPA Brings Enforcement Action Against Florida Data Broker* (February 20, 2025), https://cppa.ca.gov/announcements/2025/20250220.html;.
[18] *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies* (January 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

team of privacy experts was established within the Texas Attorney General's Consumer Protection Division.[19] These teams of localized experts provide states with meaningful resources to protect Americans' privacy.

All Americans deserve meaningful privacy protections and states should remain vital testing grounds for creative approaches to emerging privacy concerns. The undersigned states are proud to be leaders in privacy and consumer protection and we encourage the Working Group to establish a strong floor of protections while allowing states to continue to build on top of them. States have played a key role in the development of strong privacy standards, and they have an important ongoing role to play addressing new technologies and challenges.

Sincerely,

TOM KEMP
Executive Director, California Privacy Protection Agency

MATTHEW J. PLATKIN
Attorney General of New Jersey

cc: Members, House Energy & Commerce Committee

[19] *Attorney General Paxton Launches Data Privacy and Security Initiative to Protect Texans' Sensitive Data,* (June 4, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-launches-data-privacy-and-security-initiative-protect-texans-sensitive.