STATE OF CALIFORNIA

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

June 23, 2025

The Honorable John Thune, Majority Leader
The Honorable Charles E. Schumer, Minority Leader
United States Senate
Washington, DC 20510

Re: Proposed Budget Reconciliation Bill – AI Enforcement Moratorium

Dear Majority Leader Thune and Minority Leader Schumer,

We, the undersigned state privacy enforcement authorities, write in respectful opposition to S. Comm. on Com., Sci. & Transp., 119th Congress, Reconciliation Text, Sec. 0012(p)-(q) (Comm. Print 2025), that would prohibit all states from enforcing AI or automated decisionmaking technology laws for 10 years (Enforcement Moratorium). We object to any proposal that would unduly constrain states' authority to regulate AI, whether it's a straightforward preemption of state law, or conditioning federal funds on compliance with federal policy. The Enforcement Moratorium's sweeping provisions could rob millions of Americans of rights they already enjoy. We urge the Senate to reject the Enforcement Moratorium that would strip states of their ability to safeguard their residents' privacy rights from AI-related harms.

States have played a leading role in developing 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.[1] Then, in 2018 it 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.[2] Similarly, Vermont enacted the first data broker registration law in 2018, and several states have followed suit since.[3] Finally, just last year, Colorado passed the first comprehensive legislation regulating discriminatory processing of personal information by high-risk AI systems.[4]

States have consistently led on privacy and technology because they have the proximity and agility to identify emerging threats and implement innovative solutions. State privacy authorities are often the first to receive consumer complaints and identify problematic practices. States also possess the nimbleness to respond quickly to privacy threats, as demonstrated by recent action in

[1] 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.
[2] Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, 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.
[3] California, Oregon, and Texas, *See* 9 V.S.A. § 2446 et seq.
[4] Colo. Rev. Stat § 6-1-1701 et seq.

Colorado to extend privacy protections to neural data and other novel categories of personal information in response to new technologies, which has since been mirrored by other states.[5]

In fact, existing state privacy laws already address substantial privacy harms posed by AI. For example, the California Privacy Protection Agency is charged, by voter mandate, to develop regulations under the CCPA that grant consumers the right to opt-out of or access the information processed by automated decisionmaking technology (ADMT).[6] Similarly, more than a dozen state privacy laws grant individuals the right to opt out of the automated processing of personal information in furtherance of decisions that produce legally significant effects.[7] These are crucial rights that provide consumers with transparency about how their information is used and offer them greater control over how their personal information is processed. The Enforcement Moratorium threatens these important protections, creating legal uncertainty and undermining years of regulatory development.

Artificial intelligence systems pose immediate and tangible privacy risks that cannot wait a decade for federal action. AI applications currently collect, process, and make decisions based on vast amounts of personal data, often without meaningful consent or transparency. For example, the use of ADMT in employment can lead to inadvertent disclosures of sensitive information, such as whether an employee is pregnant, or surveillance of union activity.[8] This moratorium would silence vital state-level experimentation precisely when we need diverse regulatory approaches to understand and address AI's complex privacy challenges.

The often-cited concerns about a patchwork of state laws are overstated, as states regularly work together and build upon one another's legislative frameworks, creating coherent approaches that respect both innovation and consumer protection. The state privacy laws, for example, are remarkably consistent with one another because of intentional collaboration among the states. In fact, recently, privacy regulators from seven states came together to form a bipartisan Consortium of Privacy Regulators to facilitate discussions about privacy law developments and shared priorities.[9] The state privacy laws they oversee are working as intended — protecting consumer privacy while allowing businesses to thrive and innovate. Indeed, the tech sector's ability to adapt and thrive among these state privacy regimes demonstrates that regional protections do not impede business operations or technological advancement.

Restricting state action is also not consistent with established federal privacy law frameworks. Many existing federal privacy laws recognize the importance of state-level innovation in privacy protection and explicitly preserve states' abilities to adopt stronger protections for their residents. For example, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act operate alongside California's Confidentiality of Medical Information Act and Financial Information Privacy Act which build upon the protections offered by the federal statutes.[10] California's increased protections in these areas have not prevented it from becoming

[5] *See* H.B. 24-1058, 74th Gen. Assemb., Reg, Sess. (Co. 2024); S.B. 1223, 2023-2024 Leg. (Ca. 2024).
[6] Cal. Civ. Code § 1798.185(a)(15).
[7] Colorado, Connecticut, Delaware, Indiana, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, New Hampshire, New Jersey, Rhode Island, Tennessee, Texas, Utah, and Virginia. *See* Colo. Rev. Stat § 6-1-1306(1)(a)(I)(c).
[8] Peterson, Hayley, Whole Foods Tracks Unionization Risk with Heat Map, Business Insider, April 20, 2020, https://www.businessinsider.com/whole-foods-tracks-unionization-risk-with-heat-map-2020-1
[9] California Privacy Protection Agency, State Regulators Form Bipartisan Consortium to Collaborate on Privacy Issues, April 16, 2025, https://cppa.ca.gov/announcements/2025/20250416.html
[10] 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807; Cal. Civ. Code § 56.10 et seq.; Cal. Fin. Code § 4051(b).

one of the largest economies in the world.[11]

Furthermore, the moratorium would create a regulatory vacuum that benefits AI developers at the expense of privacy rights. It is highly unusual for Congress to preempt state action in an area without any corresponding federal law because while Congress deliberates on AI regulation, Americans are left unprotected from current harms. The moratorium would compound this problem by stripping away existing state protections that residents currently enjoy under state laws related to the privacy risks associated with the automated processing of personal information. The provision is not germane to the budget and would be a significant step backward in privacy protection at a time when Americans are increasingly concerned about their privacy and data security, and when challenges from new technology are developing quickly.

The rapidly evolving nature of this technology demands the flexibility and responsiveness that only multi-level governance can provide. We respectfully urge you to remove the Enforcement Moratorium from any final reconciliation bill and to ensure that states retain their essential role in protecting their residents from privacy harms.

Respectfully,

Tom Kemp, Executive Director
California Privacy Protection Agency

Rob Bonta
California Attorney General

William Tong
Connecticut Attorney General

Kathleen Jennings
Delaware Attorney General

Matthew J. Platkin
New Jersey Attorney General

Dan Rayfield
Oregon Attorney General

[11] 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/

Charity R. Clark
Vermont Attorney General

cc: Members, United States Senate