ABUNDANCE INSTITUTE

Comment on Request for Information to Explore Data Privacy and Security Framework

→ Neil Chilson* → Taylor Barkley†

April 7, 2025

* Head of AI Policy, Abundance Institute

† Director of Policy, Abundance Institute

Thank you for the opportunity to provide feedback in response to the Privacy Working Group's request for information, particularly questions (III)(B), (III)(C), and (V) concerning federal preemption and artificial intelligence (AI). The Abundance Institute is a nonprofit organization dedicated to creating a policy environment that supports emerging technologies.

As the Committee well knows, the existing patchwork of privacy laws in the states is costly to new and established innovators. The growing patchwork of state AI laws will further undermine AI advances that increase our economic competitiveness, secure our nation, and drive life-changing advances for American consumers.

The House Energy and Commerce Committee has a unique opportunity to set a clear, nationwide course for data privacy and AI governance. Doing so will protect Americans' personal data while ensuring that U.S. innovators can focus on building the next generation of advanced technologies.

Congress Should Preempt State Privacy Laws (Questions III(B) and III(C))[1]

The Working Group has recognized that the U.S. currently has a "complex web of state and federal data privacy and security laws, which in some cases create conflicting legal requirements."[2] Since 2018, a total of 19 comprehensive data privacy laws have

1 House Committee on Energy and Commerce, Privacy Working Group Request for Information (February 12, 2025), III. Existing Privacy Frameworks & Protections (B) ("Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.") (C) ("Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?"), https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework.

2 House Committee on Energy and Commerce, *Privacy Working Group Request for Information* (February 12, 2025), Page 1 ("However, the challenge of providing clear digital protections for Americans is compounded by the fast pace of technological advancement and the complex web of state and federal data privacy and security laws, which in some cases create conflicting legal requirements."), https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework.

been enacted in the states, with overlapping and sometimes contradictory rules.[3] This "patchwork" imposes especially high costs on small and medium-sized innovators that lack robust legal teams, while simultaneously giving large incumbents a regulatory advantage. For example, California's own analysis estimated that its California Consumer Privacy Act (CCPA) adds approximately $55 billion in compliance costs affecting between 15,643 and 570,066 businesses.[4] California's rules may be uniquely burdensome, but every state privacy law imposes some costs. Even for well-resourced organizations, a thicket of varied rules across multiple states drains compliance resources that could otherwise be invested in developing or improving products.[5] Moreover, certain state laws risk restricting beneficial data flows that support services consumers have come to expect—like recommendations, fraud detection, or advanced analytics.

The best solution is a federal privacy and data security framework that preempts state laws. The internet and digital communications are inherently cross-border and the Constitution grants the federal government the power to regulate interstate commerce.[6] A federal law would minimize compliance burdens and create a uniform standard for consumer protection and beneficial data use. An expressly preemptive federal law would avoid subjecting developers to a patchwork system that creates confusion and potentially stifles emerging technologies.

3 Benjamin W. Perry, Lauren N. Watson, Zachary V. Zagger, *U.S. Continues Patchwork of Comprehensive Data Privacy Requirements: New Laws Set to Take Effect Over Next 2 Year* (August 6, 2024), Ogletree Deakins, https://ogletree.com/insights-resources/blog-posts/u-s-continues-patchwork-of-comprehensive-data-privacy-requirements-new-laws-set-to-take-effect-over-next-2-years/.

4 Berkeley Economic Advising and Research, LLC, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (2019), Prepared for the California Department of Justice, Office of the Attorney General, https://web.archive.org/web/20190830173026/http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

5 Jennifer Huddleston and Gent Salihu, *The Patchwork Strikes Back: State Data Privacy Laws after the 2022–2023 Legislative Session* (July 6, 2023), Cato Institute, https://www.cato.org/blog/patchwork-strikes-back-state-data-privacy-laws-after-2022-2023-legislative-session-0.

6 Ash Johnson, *How Congress Can Foster a Digital Single Market in America* (February 20, 2024), Information Technology and Innovation Foundation, https://itif.org/publications/2024/02/20/how-congress-can-foster-a-digital-single-market-in-america/

Congress Should Preempt State AI Laws (Question V)[7]

A surge of state-level AI legislation threatens to further complicate this existing patchwork. Since January 2025, state lawmakers have introduced more than nine hundred AI-related bills with a range of requirements, including regulations concerning automated decision-making and algorithmic fairness.[8] A recent study analyzing algorithmic fairness bills in the states shows there is a growing patchwork of variable regulatory requirements.[9]

It is common sense to observe that a patchwork of 50 different state AI regulations will increase costs and reduce innovation. But recent activities in California and Colorado provide real examples and data that serve as an early indication of just how costly a state patchwork could become.

California: A Case Study in the Cost of Broad AI Regulation

Because California's market is so large, its regulations can become *de facto* national regulations.[10] A recent rule proposed by California's privacy agency is a good case study for the Working Group's consideration, because it is a state privacy regulation with a direct effect on AI and advanced computing systems.

7 House Committee on Energy and Commerce, *Privacy Working Group Request for Information* (February 12, 2025), V. Artificial Intelligence (A) ("How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?"), https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework.

8 MultiState.ai, *Artificial Intelligence (AI) Legislation,* https://www.multistate.ai/artificial-intelligence-ai-legislation (as of April 2025).

9 Logan Kolas and Nate Karren, *Irresponsible Collaboration: Evidence of a Growing AI Fairness Patchwork* (February 2025), American Consumer Institute, https://www.theamericanconsumer.org/2025/02/report-irresponsible-collaboration-evidence-of-a-growing-ai-fairness-patchwork/.

10 Jennifer Huddleston, *AI Could Become the Next Victim of the "Sacramento Effect"* (June 7, 2024), Reason Magazine, https://reason.com/2024/06/07/ai-could-become-the-next-victim-of-the-sacramento-effect/.

The California Privacy Protection Agency (CPPA) has proposed regulations governing Automated Decision-Making Technology (ADMT) under the California Consumer Privacy Act (CCPA).[11] The CCPA directs the Agency "...to adopt regulations to implement and clarify requirements related to cybersecurity audits, risk assessments, and ADMT [automated decision-making technology]."[12]

To implement this one provision of the CCPA, the Agency has proposed an entire AI regulatory regime with minimal demonstrated consumer benefit. The proposal would transform the CPAA from a privacy regulator into a *de facto* AI regulator.[13] As we've noted separately,

> *"If [the proposal is] enacted, companies may be compelled to scale back on the personalized, innovative services that have defined today's technology landscape. This shift would disproportionately burden small businesses, potentially undermining California's vibrant startup ecosystem. Ultimately, consumer choice could diminish, and the dynamic, user-focused nature of the digital economy may be compromised."*[14]

By the California agency's own estimates, the proposed regulation will impose $3.5 billion of compliance costs in the first year, with average annual costs around $1 billion; will trigger job losses peaking at roughly 126,000 positions by 2030; and will reduce annual state tax revenue by approximately $6.17 billion by 2030.[15] Yet this analysis dramatically underestimates the costs. For example, California's estimates didn't include the increased cost of labor and indirect expenses for non-regulated businesses

11 Id.

12 California Privacy Protection Agency, Notice of Proposed Rulemaking (Nov. 22, 2024), Page 4 ("Finally, the Agency is statutorily mandated to adopt regulations to implement and clarify requirements related to cybersecurity audits, risk assessments, and ADMT."), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_notice.pdf ("NPRM").

13 Neil Chilson, *Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations* (February 2025), https://abundance.institute/articles/ccpa-cyber-risk-admt ("Chilson CCPA Comments").

14 Logan Whitehair and Ahmad Nazeri, *California's High-Stakes Privacy Gamble* (March 21, 2025), https://nowandnext.substack.com/p/californias-high-stakes-privacy-gamble

15 California Privacy Protection Agency, *Standardized Regulatory Impact Assessment* at 9, 11, 63, 103 (October 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf ("SRIA").

that depend on targeted advertising platforms.[16] The estimate also underestimates the affected number of businesses, given that the proposed regulation defines automated decision-making "so broadly that it sweeps in nearly any software or process that uses personal information to aid or replace human decision-making."[17] The consequence is a regulatory regime that would significantly increase the cost and risk of operating a business in California. Companies will face the choice of complying with California law in order to reach its large population or not complying and excluding that market.

Colorado: A Case Study in the Uncertainty and Difficulty of Implementing Broad AI Regulation

These comprehensive-style bills also pose practical issues. Colorado is the only state that has passed this kind of broad regulatory framework for AI, and it already is proving problematic.[18] The new law is intended to reduce algorithmic discrimination in high-risk settings. But it also creates a broad new compliance burden for developers and deployers who must interpret confusing statutory language, uncertain enforcement triggers, and complex disclosure requirements.[19]

Governor Jared Polis expressed deep concerns about the legislation in his signing statement, but hoped that the bill would "further the conversation, especially at the national level."[20] He established a task force to fix the law's problems before its effective date. Yet the task force's recent report failed to offer solutions. The report notes that due to "a number of issues for which stakeholder groups have firm disagreements" the task force was "unable to make substantive recommendations with respect to

16 Chilson CCPA Comments at 3-6.

17 *Id.* at 7-8.

18 Colorado Senate Bill 24-205, *Consumer Protections in Interactions with Artificial Intelligence Systems* (2024), 74th Gen. Assemb., Reg. Sess. codified at Colo. Rev. Stat. § 6-1-1701 et seq. (effective Feb. 1, 2026).

19 Colorado General Assembly, *Senate Bill 24-205: Consumer Protections in Interactions with Artificial Intelligence Systems* (2024), 74th Gen. Assemb., Reg. Sess., https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_205_signed.pdf; Matthew G. White, Alexander F. Koskey, *The Colorado AI Act Shuffle: One Step Forward, Two Steps Back* (February 11, 2025), Baker Donelson, https://www.bakerdonelson.com/the-colorado-ai-act-shuffle-one-step-forward-two-steps-back.

20 Governor Jared Polis, *Colorado Senate Bill 24-205 Signing Statement* (May 17, 2024), available at https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2024/05/sb24205-signing-statement.pdf?rev=a902184eafe046cfb615bb047484e11c&hash=213F4C6CDFF52A876011290C24406E7F

these issues" but hoped for "creative solutions for building consensus as stakeholders continue to engage."[21]

The Privacy Working Group should learn from Colorado's experience that passing broad legislation on a general purpose technology like AI will face significant implementation challenges and create uncertainty.

Avoiding an AI Regulatory Patchwork

Imagine multiplying California's compliance costs and Colorado's implementation difficulties by fifty. Some states have passed narrowly focused AI bills with compliance costs that presumably are less than the estimates of costs for California's regulation. However, other states, such as Nebraska, Connecticut, and Texas, are considering similar "comprehensive" AI legislation.[22] Not all of these efforts have been successful – Virginia's Governor Youngkin vetoed a sweeping AI bill.[23] However, a large multistate policymaker working group continues to push these types of bills.[24] We expect that the activity and uncertainty will persist. The patchwork will grow unless Congress acts.

To stem this flood of expensive, conflicting legislation, Congress should federally preempt restrictive state AI regulations. A consistent national regulatory landscape would eliminate barriers to entry for innovators and entrepreneurs, stimulating competition and fostering market dynamism. Congress should do this soon, because as more state laws are passed and signed into law, preemption becomes less politically feasible.

---

21 *Report and Recommendations: Artificial Intelligence Impact Task Force* (February 2025), Colorado Legislative Council, https://leg.colorado.gov/sites/default/files/images/report_and_recommendations_5.pdf.

22 Nebraska Legislative Bill 642, *Artificial Intelligence Consumer Protection Act* (2025), 109th Leg., 1st Sess; Connecticut Senate Bill No. 2, *An Act Concerning Artificial Intelligence* (2024), Gen. Assemb., Feb. Sess; Texas House Bill 1709, *Texas Responsible Artificial Intelligence Governance Act* (2025), 89th Leg., Reg. Sess.

23 Benjamin W. Perry and Lauren N. Watson, *Virginia Governor Vetoes Artificial Intelligence Bill HB 2094: What the Veto Means for Businesses* (March 28, 2025), Ogletree Deakins, https://ogletree.com/insights-resources/blog-posts/virginia-governor-vetoes-artificial-intelligence-bill-hb-2094-what-the-veto-means-for-businesses/.

24 Adam Thierer, *Updated Compendium of Bills Pushed by the Multistate AI Policymaker Working Group* (Jan. 23, 2025), https://medium.com/@AdamThierer/updated-compendium-of-bills-pushed-by-the-future-of-privacy-forum-fpf-multistate-ai-policymaker-40cb0566cb2f.

Other Recommendations for Congressional Action on AI

To enhance the innovation environment for AI and maintain U.S. global leadership, Congress should act decisively. The following recommendations focus specifically on creating a vibrant environment that attracts investment, stimulates innovation, and encourages new market entrants:[25]

1. **Establish Negative Liability Protections:** Congress should establish negative liability laws that limit the exposure of general-purpose AI model developers to legal risks stemming from third-party misuse. Reducing disproportionate litigation risks will encourage more companies, including startups, to enter the AI market and innovate without fear of prohibitive legal consequences.
2. **Create Safe Harbor Provisions:** Safe harbor laws clearly defining minimal, innovation-friendly compliance practices will significantly lower the barriers for new and smaller players in the AI space. Clear standards enable emerging competitors to innovate confidently, leveling the playing field with established companies.
3. **Codify the Right to Compute:** By establishing a robust right to compute, Congress can prevent overly restrictive governmental actions against computational resources. Protecting this right ensures that new competitors and smaller businesses can access essential technological resources without burdensome regulatory barriers, fostering greater competition. For example, Montana recently passed SB 212, its Right to Compute Act.[26]
4. **Clarify Liability Frameworks:** Congress should clearly differentiate liability between foundational AI model developers and specific deployers of AI applications. A clear

25 These recommendations are based on our response to the Office of Science and Technology Policy's Request for Comment on the Development of an Artificial Intelligence Action Plan. That document offers more detail about some of these recommendations. See Neil Chilson and Josh Smith, *Comment on Request for Information on the Development of an Artificial Intelligence Action Plan* (March 2025), https://abundance.institute/articles/development-of-an-AI-action-plan.

26 Montana Legislature, 69th Legislature, Senate Bill 212 – *The Right to Compute Act* (2025), https://bills.legmt.gov/#/laws/bill/2/LC0292?open_tab=bill.

liability framework reduces uncertainty, encouraging new entrants by ensuring that liability risks are predictable and manageable, thereby invigorating competition.

5. **Accelerate Data Availability for AI Training:** Mandating the release and digitization of unstructured federal datasets will democratize access to valuable training data. Improved access to data reduces the advantage of large incumbents, enabling smaller firms and startups to innovate more effectively and compete more vigorously in the AI market.

General Principles for Federal Data Privacy Legislation

The Working Group, of course, is focused on privacy more broadly. While our focus is on AI, we believe that a robust federal privacy framework can lay the groundwork for AI governance by enabling consistent data flows under well-understood principles of consumer protection. However, a miscalibrated federal privacy law could inadvertently choke American AI innovation.

When considering federal data privacy legislation, Congress should adopt the following principles.[27]

→ **Maximize Permissionless Innovation.** Avoid designating broad "high-risk" categories that automatically restrict data usage or require advanced approval. Instead, allow developers to iterate and only intervene with enforcement if concrete consumer harm arises.

→ **Avoid Data Ownership Metaphors.** Personal data is not solely "owned" by an individual because it often relates to interactions among multiple parties. Treating data as "owned" by a single party can create confusion.

27 *See generally,* Neil Chilson, *When Considering Federal Privacy Legislation* (2020), 7 Pepp. L. Rev. 917, https://digitalcommons.pepperdine.edu/plr/vol47/iss4/2/.

- → **Distinguish Privacy from Data Security.** While overlapping, these concepts deserve different considerations: security focuses on preventing unauthorized access, whereas privacy can concern authorized but undesired uses.
- → **Clarify FTC Authority.** The FTC needs clarity to address harmful data practices, especially at a national scale. Carefully ensuring the FTC can address novel privacy abuses can increase predictability for businesses and better protect consumers.
- → **Focus Enforcement on Outright Consumer Harm.** Overly rigid rules can impose large costs with few commensurate benefits. Instead, consistent with the Federal Trade Commission's historical approach, focus on "unfair or deceptive" practices that result in tangible harm.
- → **Avoid Overly Broad Rulemaking Authority.** Detailed or prescriptive "command-and-control" rules can quickly become outdated, especially in the fast-moving AI ecosystem. Instead, flexible, outcome-focused enforcement fosters accountability and innovation.

A federal privacy law consistent with these principles that preempts state laws would clear the way for American AI innovation and its many benefits.

Conclusion

We are pleased that the Privacy Working Group is "explor[ing] the parameters of a federal comprehensive data privacy and security framework." Such a framework can and should protect consumers while strengthening American leadership in AI and other advanced data-driven technologies. To do so, Congress should:

- → Include an express federal preemption provision to ensure a consistent national standard.
- → Incorporate a flexible approach to AI and automated decision-making, recognizing the risks of stifling beneficial uses and encouraging best practices while limiting duplicative or contradictory state mandates.

→ Adhere to legislative principles favoring a case-by-case, outcome-oriented enforcement model, building upon the FTC's proven consumer protection framework.

We appreciate your consideration and opportunity to assist in developing a federal approach that protects consumers, prevents a stultifying patchwork of state laws, and promotes rapid innovation in a data-driven world.