



Comments of

TechFreedom

Andy Jungⁱ

In the Matter of

House Committee on Energy and Commerce Privacy Working Group Request for Information

April 7, 2025

ⁱ Andy Jung is Associate Counsel at TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at ajung@techfreedom.org.

TABLE OF CONTENTS

Introduction	1
I. Federal privacy law should preempt state-level AI frameworks, including requirements related to automated decision-making.....	2
A. A federal privacy law that preempts state-level AI frameworks would create uniform rules for AI nationwide and ensure that domestic AI policy is driven by experts.	4
Conclusion.....	6

INTRODUCTION

TechFreedom is a nonprofit, nonpartisan think tank based in Washington, D.C. It is dedicated to promoting technological progress that improves the human condition. It seeks to advance public policy that makes experimentation, entrepreneurship, and investment possible and thus unleashes the ultimate resource: human ingenuity.

TechFreedom regularly engages on privacy issues ranging from data collection and security¹ to the Fourth Amendment² to children's online privacy.³ It has long called for federal preemption of state privacy laws.⁴ TechFreedom champions a light-touch approach to AI regulation⁵ led by the federal government.⁶

The Request for Information correctly recognizes that a “growing number of states” are enacting laws regulating AI.⁷ Additionally, “[m]ost state comprehensive data privacy and security laws regulate AI through ‘automated decision-making’ requirements.”⁸ The result is

¹ *TechFreedom Delivers Remarks at FTC's Commercial Surveillance and Data Security Public Forum*, TECHFREEDOM (Sept. 8, 2022), <https://techfreedom.org/techfreedom-delivers-remarks-at-ftcs-commercial-surveillance-and-data-security-public-forum/>; TechFreedom, Comment on Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 21, 2022), <https://techfreedom.org/wp-content/uploads/2022/11/TechFreedom-Comments-Trade-Regulation-Rule-on-Commercial-Surveillance-and-Data-Security.pdf>.

² Tech Policy Podcast, 395: *The Digital Fourth Amendment — With Orin Kerr*, TECHFREEDOM (Jan. 23, 2025), <https://podcast.techfreedom.org/episodes/395-the-digital-fourth-amendment-with-orin-kerr>.

³ TechFreedom, Comment on Children's Online Privacy Protection Rule (Mar. 11, 2024), <https://techfreedom.org/wp-content/uploads/2024/03/TechFreedom-COPPA-Rule-Comments-3.11.2024.pdf>.

⁴ See TechFreedom, Comment on Developing the Administration's Approach to Consumer Privacy, at 35-36 (Sept. 26, 2018), https://www.ntia.gov/sites/default/files/publications/techfreedom_ntia_comments_on_privacy_framework_-_11.18.0.pdf#page=41 (arguing that any federal privacy legislation should explicitly preempt state consumer privacy regulations).

⁵ See, e.g., Tech Policy Podcast, 397: *AI Policy Potpourri (Part One)*, TECHFREEDOM, at 38:24 (Feb. 17, 2025), <https://podcast.techfreedom.org/episodes/397-ai-policy-potpourri-part-one> (discussing how a “caution-first” approach to AI regulation might be futile); Andy Jung, *Don't California My Texas: Stargate Edition*, TECHFREEDOM (Jan. 24, 2025), <https://techfreedom.substack.com/p/dont-california-my-texas-stargate> (writing that the Texas Responsible AI Governance Act could burden Stargate's AI development and infrastructure); Andy Jung, *'Unregulated AI' is a Myth*, THE ORANGE CNTY. REG. (Apr. 1, 2024), <https://www.ocregister.com/2024/04/01/unregulated-ai-is-a-myth/> (describing how AI is already regulated, especially in California).

⁶ TechFreedom, Comment on the Development of an AI Action Plan, at 5 (Mar. 15, 2015), <https://techfreedom.org/wp-content/uploads/2025/03/TF-Public-Comment-on-AI-Action-Plan.pdf#page=7>.

⁷ Privacy Working Grp., *Request for Information*, HOUSE COMM. ON ENERGY & COM., at 3 (Feb. 21, 2025) https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf#page=3.

⁸ *Id.* See, e.g., CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT) and Insurance Companies, 47-Z Cal. Regulatory Notice Reg. 1494 (proposed Nov. 22, 2024) (proposing a rule to advance regulations concerning AMDT technologies).

a “complex web of state and federal data privacy and security laws, which in some cases create conflicting legal requirements.”⁹ This web of state laws “raise[s] questions about the role of privacy and consumer protection standards in AI regulation and the impact on U.S. AI leadership.”¹⁰ Overall, a state-based approach creates regulatory uncertainty that hampers domestic AI development.

To untangle the web of state privacy laws, “[m]embers of Congress have spent many years working toward federal comprehensive data privacy and security standards to bring consumer protections into the digital age while ensuring that the U.S. continues to lead in a globally competitive environment.”¹¹ To that end, the Request for Information “explore[s] the parameters of a federal comprehensive data privacy and security framework”¹² — a federal privacy law. If Congress passes a federal privacy law, it should preempt state-level privacy frameworks for AI.¹³

I. Federal privacy law should preempt state-level AI frameworks, including requirements related to automated decision-making.

Across the country, states are considering hundreds of potential bills related to AI, and states like California and Colorado have already passed AI legislation.¹⁴ While federalism sometimes benefits innovation, AI services are offered nationwide, so one state’s regulation will inevitably demand compliance by all American companies. The result is a web of inconsistent legislation, with each state’s laws layering on multiple sets of conflicting obligations.¹⁵

The United States needs a national approach to AI policy “to sustain and enhance America’s AI dominance, and to ensure that unnecessarily burdensome requirements do not hamper private sector AI innovation.”¹⁶ Europe and China, our principal rivals in the AI race, have

⁹ Privacy Working Grp., *supra* note 7, at 3.

¹⁰ *Id.*

¹¹ *Id.* at 1.

¹² *Id.*

¹³ Specifically, these comments address question V.A. in the Request for Information: “How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?” *Id.* at 3.

¹⁴ Devin McCormick, *State AI Policy in 2024: What Happened, What Didn’t, and Where do we go From Here?*, LIBERTAS INST. (Jan. 7, 2025), <https://libertas.institute/tech-innovation/state-ai-policy-in-2024-what-happened-what-didnt-and-where-do-we-go-from-here/>.

¹⁵ Privacy Working Grp., *supra* note 7, at 1 (“[T]he 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.”). *See also* Alan Untereiner, *The Defense of Preemption: A View from the Trenches*, 84 TUL. L. REV. 1257, 1262 (2010).

¹⁶ TechFreedom, *supra* note 6, at 5 (quoting Request for Information on the Development of an Artificial Intelligence (AI) Action Plan, 90 Fed. Reg. 9088-89 (Feb. 6, 2025)).

internally harmonized their approaches, offering their companies the clarity of a single model.

In contrast, AI firms in the U.S. must comply with a wide variety of regulations and answer to multiple regulators across various states. In California, for example, eighteen new AI laws went into effect in January 2025 *alone*.¹⁷ The California Attorney General and state agencies share enforcement authority, and some of the laws include a private right of action, allowing victims to sue violators directly.¹⁸

On top of the AI laws passed by the California legislature, the California Consumer Privacy Agency recently released proposed regulations on Automated Decision-Making Technology (ADMT), which would shoehorn AI regulations into the state's privacy law and grant the agency broad authority over automated technologies.¹⁹ Taken together, AI firms doing business in California must comply with a web of regulations enforced by the state attorney general, various state agencies, and even suits by private citizens. And that's *just* the Golden State. AI firms operate nationwide and are therefore subject to hundreds of state laws across the country.

While states rush ahead with disjointed AI laws, Congress is taking a more focused and measured approach. Representative Nancy Pelosi (D-CA) emphasized the federal government's intention to regulate AI:

AI has been a central policy focus of the President and the Congress for the past few years In the House of Representatives and the U.S. Senate, we early on brought in academics, entrepreneurs and leaders from the public, private and non-profit sectors to express AI's opportunities and challenges.

The review is coming down to if and what standards and guardrails should Congress legislate. In addition to focusing on protections, we wanted to pursue

¹⁷ See Jeewon K. Serrato et al., *California's AI Laws are Here — Is Your Business Ready?*, PILLSBURY (Feb. 7, 2025), <https://www.pillsburylaw.com/en/news-and-insights/california-ai-laws.html> (describing California's eighteen new AI laws).

¹⁸ *Id.* See, e.g. S.B. 942, 2023-24 Regular Session (Cal. 2024) (requiring "covered providers" to provide free AI detection tools and providing enforcement by the California Attorney General). See also A.B. 1008, 2023-24 Regular Session (Cal. 2024) (updating the CCPA to mandate that AI-generated data be treated as personal information and dictating that both the California Attorney General and the California Privacy Protection Agency enforce the law); S.B. 926, 2023-24 Regular Session (Cal. 2024) (criminalizing the creation and distribution of non-consensual deepfake pornography and providing enforcement by the California Attorney General and a private right of action).

¹⁹ See TechFreedom, Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations (Feb. 19, 2025), <https://techfreedom.org/wp-content/uploads/2025/02/TF-Public-Comment-on-CCPA-Updates-Cyber-Risk-ADMT-and-Insurance.pdf> (describing how the proposed ADMT regulations are outside of the CCPA's scope).

improving AI. This work continues under the Bipartisan Task Force on Artificial Intelligence under the leadership of co-chairs Congressman Ted Lieu and Congressman Jay Obernolte.²⁰

Federal Trade Commission Chair Andrew Ferguson stated the risk of overregulating AI more bluntly: “Such regulation could strangle this nascent technology in its cradle, or move the development of the technology to foreign states hostile to our national interests.”²¹

A state-based approach to AI policy is fundamentally flawed: states lack the institutional capacity to regulate the rapidly developing technology; conflicting state laws create a patchwork of rules which reduce regulatory clarity; and states disagree on the relative risk of AI and the appropriate approach to oversight.²² To reinvigorate domestic AI policy and unleash the full potential of this transformative technology, federal privacy law should preempt state-level AI frameworks, including requirements related to automated decision-making.

A. A federal privacy law that preempts state-level AI frameworks would create uniform rules for AI nationwide and ensure that domestic AI policy is driven by experts.

Federal preemption is ubiquitous in modern regulation: “it is almost certainly the most frequently used doctrine of constitutional law in practice.”²³ Federal statutes preempt state law to shape the regulatory environment for most major industries, including pharmaceuticals, medical devices, banking, air transportation, securities, automobile safety, and tobacco.²⁴

Federal preemption of state-level AI frameworks would reinvigorate domestic AI policy:

²⁰ Press Release, Nancy Pelosi, Pelosi Statement in Opposition to California Senate Bill 1047 (Aug. 16, 2024), <https://pelosi.house.gov/news/press-releases/pelosi-statement-opposition-california-senate-bill-1047>.

²¹ Andrew N. Ferguson, Comm’r, Fed. Trade Comm’n, Concurring and Dissenting Statement of Commissioner Andrew N. Ferguson Joined by Commissioner Melissa Holyoak Regarding the FTC Staff Report on AI Partnerships & Investments 6(b) Study Matter P246201 (Jan. 17, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/ferguson-ai-6b-statement.pdf.

²² Dean W. Ball & Alan Z. Rozenshtein, *Congress Should Preempt State AI Safety Legislation*, LAWFARE (June 17, 2024, 2:00 PM), <https://www.lawfaremedia.org/article/congress-should-preempt-state-ai-safety-legislation>.

²³ Stephen A. Gardbaum, *The Nature of Preemption*, 79 CORNELL L. REV. 767, 768 (1994). *See also* Garrick B. Pursley, *Preemption in Congress*, 71 OHIO ST. L. J. 511, 514 (2010) (describing preemption as “the issue of constitutional law that most directly impacts everyday life”); Thomas W. Merrill, *Preemption and Institutional Choice*, 102 NW. U. L. REV. 727, 730 (2008) (noting that “[p]reemption is one of the most widely applied doctrines in public law”).

²⁴ Bryan L. Adkins et al., *Federal Preemption: A Legal Primer*, CRS Report No. R45825, at 1 (citing Pursley, *supra* note 23, at 513-514).

The broadly applicable preemption doctrine can and does bring with it very substantial public benefits. We live in a large and sprawling country that is rich in many things, including government and regulation. In addition to the fifty state governments, each with its own legislature, executive branch and administrative agencies, and court system, there were by last count more than 87,500 local governmental units in the United States, including counties, cities, and other municipalities. This multiplicity of government actors below the federal level virtually ensures that, in the absence of federal preemption, businesses with national operations that serve national markets will be subject to complicated, overlapping, and sometimes even conflicting legal regimes.²⁵

A federal privacy law that preempts state-level AI frameworks is superior to a patchwork approach in several ways. A preemptive federal privacy law would “prescribe[] a single set of uniform rules for the entire country...streamlin[ing] the legal system, reduc[ing] the regulatory burdens on business, and help[ing] to create a unified national marketplace” for AI.²⁶ In doing so, a federal privacy law would “reduce[] the barriers to new entry by small businesses and lower[] the cost of doing business,” reducing AI prices for consumers.²⁷ Most importantly, preempting state-level AI frameworks would ensure that AI policy is “formulated by expert regulators with a broad national perspective and needed scientific or technical expertise, rather than by decision makers — such as municipal officials, elected state judges, and lay juries — who may have a far more parochial perspective and limited set of information.”²⁸

In response to the recent Request for Information on the Development of an Artificial Intelligence (AI) Action Plan, both public and private sector stakeholders submitted comments calling for federal preemption of state-level AI frameworks.²⁹ The Privacy

²⁵ Untereiner, *supra* note 15, at 1261-62.

²⁶ *See id.* at 1262.

²⁷ *See id.*

²⁸ *See id.*

²⁹ OpenAI called for preemption to “[e]nsur[e] the Freedom to Innovate” and to “[h]elp keep the US public and private sectors competitive by allowing AI companies of all sizes to pursue bleeding-edge AI technology free from the regulatory uncertainty created by some state-based liability regimes.” OpenAI, Comment on the Development of an AI Action Plan, at 6-7 (Mar. 13, 2025), <https://cdn.openai.com/global-affairs/ostp-rfi/ec680b75-d539-4653-b297-8bcf6e5f7686/openai-response-ostp-nsf-rfi-notice-request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan.pdf>. *See also* Andreessen Horowitz, Comment on the Development of an AI Action Plan, at 5 (Mar. 14, 2025), <https://d1lamhf6l6yk6d.cloudfront.net/uploads/2025/03/a16z-National-AI-Action-Plan-OSTP-Submission.pdf#page=5>. (“Because the AI development market is inherently a national one with potential significant impacts in commerce, national security, and foreign relations, the federal government is best-

Working Group and the executive branch should collaborate and share information as they craft their respective policy frameworks. A unified federal approach to regulation centered around a preemptive federal privacy bill would upgrade domestic AI policy, making it more efficient, uniform, and expert-driven.

CONCLUSION

States have hijacked domestic AI policy and threatened to derail the nascent industry by creating a web of conflicting local laws. Any comprehensive federal privacy bill passed by Congress should preempt state-level AI frameworks, including requirements related to automated decision-making. Congress, however, should only regulate the data collection and usage practices of AI firms insofar as they cause concrete harms to consumer privacy: balancing individuals' privacy interests against U.S. interests like innovation, national security, and AI competitiveness.

Respectfully submitted,

_____/s/____

Andy Jung
Association Counsel
TechFreedom
ajung@techfreedom.org
1500 K Street NW
Floor 2
Washington, D.C. 20005

Date: April 7, 2025

positioned to regulate this market. The Administration, therefore, should work with Congress to pass legislation that creates a national AI model market and preempts state-specific restrictions on model development and legislation that promotes access to AI infrastructure, data, and talent.”); Int’l Ctr. for L. & Econ., Comment on the Development of an AI Action Plan, at 12 (Mar. 14, 2025), <https://laweconcenter.org/wp-content/uploads/2025/03/OSTP-AI-2025-comments-v-1.pdf> (stating that the AI Action Plan should “[e]nsure that federal standards provide transparency and clarity, preempting conflicting state and local regulations.”); R Street, Comment on the Development of an AI Action Plan (Mar. 15, 2025), <https://www.rstreet.org/outreach/comments-of-the-r-street-institute-in-request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan/> (arguing that the AI Action Plan should “[h]elp Congress craft a framework for preemption of state AI regulatory patchwork”).