

Comments of the International Center for Law & Economics

*U.S. House Energy and Commerce Committee Privacy Working Group
Request for Information*

April 7, 2025

Authored by:

Kristian Stout (Director of Innovation Policy, International Center for Law & Economics)

I. Introduction

The International Center for Law & Economics (ICLE) appreciates the Privacy Working Group's efforts to develop a comprehensive federal data-privacy and security framework. Our comments specifically address the request for information's (RFI) Section V on artificial intelligence (AI), although they are also relevant to such related issues as market effects and regulatory fragmentation.

In particular, we highlight two vital lessons for crafting effective federal privacy and AI legislation. First, fragmented state regulations that create diverse and conflicting standards for automated decision-making technologies (ADMT) and AI significantly undermine U.S. competitiveness in the global AI landscape, making clear federal preemption essential. Second, precise and informed definitions of ADMT and AI are fundamental to effective legislation, as these would help to ensure that regulations appropriately address genuine risks without inadvertently capturing routine or low-risk technologies.

We also emphasize that, in order to address ADMT, AI, and federal privacy standards comprehensively, it will almost certainly be necessary to craft multiple pieces of legislation. Given the complexity of the task, Congress should first prioritize a comprehensive privacy framework, and then separately tackle regulation of AI and ADMT through targeted, specialized legislation. Combining comprehensive privacy and AI regulation into a single legislative effort risks significant overreach and regulatory confusion. Moreover, because numerous states have already addressed ADMT in their privacy statutes, we urge Congress to enact clear preemption of state ADMT laws to provide consistency and prevent harmful regulatory fragmentation.

While the complexity, rapid evolution, and diverse applications of AI technologies counsel addressing AI regulation separately from comprehensive privacy legislation, we acknowledge that some concerns surrounding AI systems do intersect significantly with general privacy concerns. The appropriate response to these intersections is not to embed expansive or overly broad definitions of AI directly within privacy law. Rather, privacy legislation should maintain a fundamentally tech-neutral approach. This would ensure that privacy harms arising from AI systems can be effectively remedied using well-established, consistent privacy frameworks that are applicable to any technological context.

Congress must avoid inadvertently creating regulatory frameworks that unnecessarily burden innovation or complicate enforcement through overly broad AI-specific language. It is crucial that privacy law be sufficiently flexible to adapt to technological advancements, thereby providing clarity and efficiency for regulators and regulated entities alike.

Given the complexity and rapid evolution of AI technologies, Congress must pursue a thoughtful and targeted approach, crafting careful regulation that accurately reflects the diverse nature and varying risks associated with AI and ADMT. Such regulation must avoid overly broad definitions and standards that could stifle innovation and impose unnecessary burdens, particularly on smaller businesses and innovators.

II. Risks of Overly Broad AI Definitions and Regulation

The Privacy Working Group is correct to be concerned about the profusion of state-level regulations of AI and ADMT. Recent state-level proposals illustrate precisely the pitfalls that accompany fragmented approaches. The California Privacy Protection Agency (CPPA), for example, has promulgated regulations that define AI in such overly expansive terms that they would encompass virtually any system capable of generating outputs that influence physical or virtual environments.¹ Such definitions lack analytical precision; risk encompassing low-risk, commonplace technologies; impose unjustified compliance burdens; and create regulatory ambiguity.

Other states have similarly included ADMT provisions within various privacy laws, leading to varying standards and requirements across jurisdictions.² This patchwork regulatory landscape threatens to create significant confusion, disrupt interstate commerce, and ultimately undermine national competitiveness and innovation in critical AI sectors. There are several lessons to draw from this patchwork of state efforts.

A common pitfall associated with regulations for ADMT and AI is to adopt overly expansive or otherwise ambiguous definitions. For instance, California's Privacy Protection Agency recently proposed defining AI as any "machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments."³ Similarly problematic are expansive interpretations of ADMT to include not only systems that autonomously make decisions or replace human judgments, but also technologies that merely "substantially facilitate human decision-making," or whose outputs constitute a "key factor" in human decisions.⁴

Defining AI broadly without accounting for the diversity of AI applications—ranging from large language models (LLMs) and computer-vision systems to predictive-analytics tools—risks creating counterproductive and analytically unsound regulatory frameworks. Treating diverse AI technologies as functionally equivalent inevitably captures some low-risk software applications alongside genuinely high-risk systems. Such regulatory outcomes also threaten to impose unnecessary compliance burdens and potentially to distort competition by favoring large incumbents.

These excessively inclusive definitions often encompass a wide variety of routine business operations, from basic spreadsheet analyses and customer profiling to common marketing analytics. This could inadvertently impose stringent regulatory obligations on common practices that have minimal, if any, adverse impacts on consumer welfare or privacy interests. Small and medium-sized enterprises,

¹ California Privacy Protection Agency, *Proposed Regulations* (2024), available at https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter "CPPA Proposal"].

² See Jennifer Johnson et al., *State Legislatures Consider New Wave of 2025 AI Legislation*, COVINGTON & BURLING LLP (Feb. 21, 2025), <https://www.insideglobaltech.com/2025/02/21/state-legislatures-consider-new-wave-of-2025-ai-legislation> ("Lawmakers in more than a dozen states have introduced legislation that would regulate the use of AI or automated decision-making tools ('ADMT') in specific sectors, including healthcare, insurance, employment, and finance.").

³ See CPPA Proposal, *supra* note 1 at § 7001(c).

⁴ *Id.*, § 7001(f).

in particular, would face significant uncertainty and disproportionately high compliance burdens.⁵ Indeed, smaller firms already rely heavily on low-risk AI applications to boost productivity and maintain competitiveness in an increasingly technology-driven marketplace.⁶

Moreover, these broad definitions do not reflect the true diversity and heterogeneity inherent in AI technologies.⁷ They fail to appropriately calibrate oversight to actual levels of risk, thereby threatening to stifle beneficial innovation and creating unnecessary economic burdens without corresponding consumer protections.⁸ By contrast, adopting precise, harm-sensitive definitions would help ensure that regulatory efforts are targeted effectively, providing appropriate safeguards without undermining technological innovation and economic growth.⁹

Indeed, overly generalized regulations are likely to over-index toward conceptualizing AI in ways that presume the need for strong centralized control over development and distribution of AI technologies. This would bias regulatory frameworks toward proprietary, corporate-controlled AI products and may inadvertently disadvantage open-source AI initiatives, which would face disproportionate compliance burdens or inapposite legal and regulatory obligations. Given that open-source methodologies underpin substantial portions of the AI-development ecosystem—fostering innovation, competition, and broad economic benefits—Congress should ensure that federal AI regulations explicitly consider the unique characteristics of open-source development, avoiding inadvertently shifting innovation toward proprietary, closed models controlled by larger incumbents.

III. Benefits of an Incremental, Sector-Specific Regulatory Approach

The process of adopting ADMT and AI regulations should be incremental and tailored to specific sectors.¹⁰ Such sector-specific regulation offers clear advantages by aligning regulatory oversight more closely with actual sector-specific risks. AI applications differ significantly across industries; for example, AI utilized in health-care diagnostics poses different regulatory challenges and risk profiles

⁵ See *Empowering Small Business: The Impact of Technology on U.S. Small Business*, U.S. CHAMBER OF COM. TECH. ENGAGEMENT CTR. (Sep. 14, 2023), at 3, available at <https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf>; *Open Source AI Is Leading to Breakthroughs in Healthcare, Education, and Entrepreneurship*, META (Dec. 11, 2024), <https://about.fb.com/news/2024/12/open-source-ai-is-leading-to-breakthroughs-in-healthcare-education-and-entrepreneurship>.

⁶ *Id.*; see also Julian Jacobs, *Evidence Shows Productivity Benefits of AI*, CTR. DATA INNOV. (Jun. 11, 2024), <https://datainnovation.org/2024/06/evidence-shows-productivity-benefits-of-ai>.

⁷ See Lazar Radic & Kristian Stout, *What Is the Relevant Product Market in AI?*, CONCURRENCES: ARTIFICIAL INTELLIGENCE AND COMPETITION POLICY 107 (Sep. 16, 2024), at 109, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4927505.

⁸ *Id.* at 110.

⁹ See Kristian Stout et al., *NIST AI 800-I, Managing Misuse Risk for Dual-Use Foundation Models*, INT'L CTR. L. & ECON. (Sep. 9, 2024), at 8-13, available at <https://laweconcenter.org/wp-content/uploads/2024/09/NIST-AI-comments-final.pdf>.

¹⁰ See 118th Congress, *Bipartisan House Task Force Report on Artificial Intelligence* vi-vii, 85 (2024), available at <https://republicans-science.house.gov/cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/E4AF21104CB138F3127D8FF7EA71A393.ai-task-force-report-final.pdf>.

than AI used for retail inventory management, financial services, or marketing analytics.¹¹ By recognizing these differences, policymakers can craft targeted regulations that specifically address high-risk applications without unduly burdening low-risk uses.

Moreover, adopting sector-specific regulations would allow policymakers to leverage existing industry-specific regulatory frameworks and expertise, enhancing both the effectiveness and efficiency of oversight.¹² Financial regulators, for instance, are better positioned to address concerns related to fairness and transparency in automated-lending decisions, while health authorities are more adept at addressing the privacy and accuracy considerations inherent in medical-diagnostic technologies. Thus, a sector-specific approach can help to ensure that consumer protections are robustly enforced in areas where they are genuinely needed, without imposing unnecessary restrictions on innovation and efficiency in lower-risk contexts.¹³

This incremental approach aligns closely with recent recommendations at the federal level. Notably, the House Bipartisan Task Force on Artificial Intelligence explicitly recommended addressing AI challenges through existing regulatory frameworks whenever feasible, advocating for sector-specific expertise to guide oversight.¹⁴ Similarly, the National Telecommunications and Information Administration (NTIA) has recommended adopting a marginal-risk framework, prioritizing empirically demonstrable harms and assessing the incremental risks posed by AI systems relative to existing alternatives or non-AI technologies.¹⁵ Recognizing the uncertainties inherent to such an endeavor, the NTIA's marginal-risk framework also cautions policymakers to remain modest in their expectations regarding *ex-ante* risk assessments. It would reserve heightened scrutiny only for genuinely high-risk applications in such sensitive domains as health care, criminal justice, and critical infrastructure.

By aligning federal policy with these targeted and empirically driven regulatory frameworks, Congress can better address legitimate AI risks without stifling technological advancement or economic innovation.¹⁶

IV. Impact on Small Businesses and Innovation

Adopting overly broad regulations to govern AI and ADMT would disproportionately affect small businesses, imposing excessive compliance costs and complexities that threaten their ability to compete and innovate.¹⁷ Unlike larger corporations that possess extensive legal resources, small businesses frequently lack the capacity to manage intricate regulatory frameworks. Consequently,

¹¹ *Id.*

¹² *Id.* at 6, 30.

¹³ *See Id.* at 7, 17.

¹⁴ *Id.*

¹⁵ *See Stout, supra* note 9, at 8-13.

¹⁶ *Id.*

¹⁷ *See U.S. Chamber, supra* note 5, at 3.

overly expansive definitions and regulatory requirements could become significant barriers to entry, discouraging smaller firms from adopting beneficial AI technologies critical to their operational efficiency and competitiveness.¹⁸

Indeed, evidence clearly demonstrates that AI technologies have already proven transformative for many small businesses, substantially enhancing their productivity, profitability, and capacity to innovate. Surveys indicate that approximately 95% of small businesses use at least one technology platform to streamline their operations, with nearly a quarter specifically adopting AI tools to improve marketing effectiveness, customer communications, and overall business performance.¹⁹ For many small enterprises, adopting AI solutions has produced measurable improvements in profit margins, sales growth, and operational efficiency.²⁰ Furthermore, AI's ability to automate routine tasks and reduce operational burdens has been particularly beneficial to smaller businesses, enhancing their ability to compete against larger market participants.²¹

By imposing disproportionate compliance obligations, overly broad regulatory approaches threaten to significantly diminish these productivity gains. Such regulations may deter small businesses from fully embracing AI solutions, potentially exacerbating existing challenges related to economic pressures, inflation, and workforce shortages.²² In this respect, narrowly tailored, risk-sensitive federal regulations are essential to sustain the productivity-enhancing benefits of AI for small businesses, while also ensuring appropriate consumer protections.

V. Avoiding Fragmentation Through Clear Federal Preemption

A fragmented state regulatory landscape significantly undermines U.S. competitiveness in AI development and deployment. The rapid proliferation of state-level AI regulations has created substantial challenges, particularly in complying with widely divergent definitions, scopes, and compliance obligations across jurisdictions.²³ This fragmented regulatory environment imposes increased operational complexity and costs on businesses that operate at a national or regional scale, forcing them to navigate inconsistent rules and duplicative compliance burdens.²⁴ For example, a business developing AI solutions for health care or financial services might need to simultaneously comply with divergent state-level regulatory frameworks, each potentially imposing unique definitions and standards for ADMTs.

¹⁸ *Id.*

¹⁹ *Id.* at 3-4.

²⁰ *Id.* at 2,23.

²¹ *Id.* at 5.

²² *Id.* at 2,15.

²³ See Rachel Curry, *How AI Regulation in California, Colorado and Beyond Could Threaten U.S. Tech Dominance*, CNBC TECH. EXEC. COUNCIL (Nov. 21, 2024), <https://www.cnbc.com/2024/11/21/how-ai-laws-in-california-states-threaten-us-tech-dominance.html>.

²⁴ See Kristian Stout, *The AI Legislative Puzzle*, TRUTH MARK. (Nov. 7, 2024), <https://truthonthemarket.com/2024/11/07/the-ai-legislative-puzzle>.

To mitigate these challenges and strengthen U.S. competitiveness in AI, Congress should implement a clear federal preemption framework designed to harmonize AI regulation across the states. Such federal preemption should establish uniform, precise definitions of key terms like AI and ADMT, as well as consistent, harm-based regulatory thresholds that would be applicable nationwide. By clearly delineating federal regulatory authority, Congress would significantly reduce compliance uncertainty, streamline operational efficiency, and facilitate investment decisions. This would allow businesses to confidently pursue AI innovation without fear of contradictory or unpredictable state-level regulatory interventions.

Ultimately, a harmonized national framework would provide essential regulatory certainty and predictability, essential for continued innovation and sustained investment in AI technologies. Clear federal preemption would not only simplify compliance, but also help to position the United States as a more attractive jurisdiction for AI developers and innovators. This approach would serve to safeguard the nation's global leadership in digital technologies and ensure robust protections for consumers.

VI. Conclusion

As Congress moves forward with developing federal legislation, it is crucial to adopt narrowly tailored definitions and targeted, harm-based regulatory approaches. Regulations must reflect the actual diversity and varying risks associated with AI and ADMT in order to avoid unnecessary burdens on beneficial, low-risk applications.

Congress should prioritize incremental regulation grounded in demonstrated harms, rather than speculative risks. We strongly recommend focusing initially on the development of a comprehensive federal privacy framework, separate from any AI-specific legislation. Addressing privacy comprehensively first, followed by separate specialized laws to govern AI and ADMT, would reduce complexity and regulatory overreach.

Given the existing fragmented state regulatory landscape, Congress must clearly define the scope of federal preemption, explicitly including state-level ADMT laws. This will significantly reduce compliance uncertainty, streamline regulatory consistency nationwide, and protect smaller businesses and innovators.

Ultimately, by clearly delineating comprehensive privacy and targeted AI legislation, Congress can seize the opportunity to enhance consumer protections effectively, while safeguarding and promoting U.S. technological innovation, competitiveness, and leadership in the rapidly evolving AI landscape.