The American Consumer Institute
Center for Citizen Research

Before the
HOUSE ENERGY & COMMERCE COMMITTEE'S DATA PRIVACY WORKING GROUP
Washington, D.C. 20515

In the Matter of Request for Information to Explore Data and Security Framework
(Released April 7, 2025)

Comments of the American Consumer Institute

The American Consumer Institute Center for Citizen Research (ACI) is a nonprofit 501 (c)(3) educational and research institute with the mission to identify, analyze, and protect the interests of consumers in legislative and rulemaking proceedings. ACI submits these comments in response to a request for information (RFI) exploring a data privacy and security framework.

Introduction

For the better part of two decades, Congress quietly debated the need for a federal privacy framework but failed to act. Instead, states have cobbled together their own rules and regulations—creating a complicated, confusing, uncoordinated, and expensive data privacy regime with regulations that vary by rule and by type. Many states have debated comprehensive rules while others have pursued fragmented sectoral approaches. More recently, states have been modifying these rules—and proposing entirely new regulatory regimes—to govern artificial intelligence. Those confusing and complicated rules threaten to derail the AI revolution before its promises are realized. Congress should pre-empt these laws and replace them with a clear and concise federal framework that carefully limits the power of the agencies that enforce it.

The Need for a Pre-emptive Federal Data Privacy Standard (Questions III(A) and (B))

In the absence of Congressional action, state governments have filled the void with their own data privacy laws. According to the International Association of Privacy Professionals (IAPP), 19 states have already passed comprehensive data privacy laws and 14 others are actively considering doing so.[1] Such fragmentation threatens to mire businesses—especially small businesses—in a costly web of rules and regulations that drive up compliance costs, raise prices, and harm consumers.

To the greatest extent possible, business will comply with the most stringent versions of state privacy laws so long as the requirements are duplicative—but since the laws often apply unequally and vary by rule and by type it is not as simple as complying with just one strict data privacy standard. Although some states agree on scope provisions, enforcement powers, and the need for data impact assessments, variations remain common. Tennessee, for example, largely mirrors Virginia's privacy framework, but still deviates in terms of cure periods, affirmative defenses, and data minimization provisions.[2] More generally, many states design scope provisions by revenue, processing, and broker thresholds, but those thresholds vary by state. Texas most uniquely only exempts businesses as defined by the Small Business Administration (SBA).[3] Most states carveout data already governed by existing federal laws such Health Insurance Portability and Accountability Act (HIPPA), Gramm-Leach-Bliley, federal financial and education data, and certain data pertaining to child information already governed by federal law.[4] Tennessee more narrowly tailors its data privacy law by exempting "government entities, nonprofit organizations, higher educational institutions, scientific research, insurance

[1] International Association of Privacy Professionals, "US State Privacy Legislation Tracker," Last visited April 6, 2025, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[2] Logan Kolas, "Key Principles for State Data Privacy Law," The Buckeye Institute, October 12, 2023, https://www.buckeyeinstitute.org/library/docLib/2023-10-Key-Principles-for-State-Data-Privacy-Laws-policy-report.pdf; Consumer Data Protection Act, Virginia Code Annex §§ 59.1-575–59.1-584 (2021), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/; and Tennessee Information Protection Act, Tennessee Public Chapter no. 408 (2023), https://publications.tnsosfiles.com/acts/113/pub/pc0408.pdf.
[3] Texas Data Privacy and Security Act, Texas Business & Commerce Code, § 541.001–541.205 (2023), https://statutes.capitol.texas.gov/Docs/BC/htm/BC.541.htm.
[4] Logan Kolas, "Key Principles for State Data Privacy Law," The Buckeye Institute, October 12, 2023, https://www.buckeyeinstitute.org/library/docLib/2023-10-Key-Principles-for-State-Data-Privacy-Laws-policy-report.pdf.

data, and motor vehicle records."[5] To build on the already existing—and successful—sectoral approach to data privacy, the federal government should follow Tennessee's lead and exempt data types already governed by other federal statutes.

To enforce state data privacy laws, states have generally avoided messy, expensive, and frivolous private rights of action in comprehensive data privacy legislation. Although California mistakenly provides a (limited) private right of action, Illinois is the exception that proves the rule. Courts have interpreted the Illinois Biometric Information Privacy Act (BIPA) to mean parties can be aggrieved even if they suffer no harm—sparking lawsuits and unleashing an overeager plaintiff's bar.[6] BIPA also highlights that states have pursued data privacy laws on a sectoral basis—not just comprehensively. Following Illinois' lead, Texas, Washington, and New York City have passed biometric data privacy laws of their own.[7] And although HIPAA remains the primary law governing health data information, Washington, California, Nevada, Connecticut, and Maryland have all passed healthcare specific data privacy laws.[8]

Two Option for Data Privacy Pre-emption (Questions III(C))

Option 1: Comprehensive Federal Framework

To ease the cost of compliance and reduce the confusion of complying with many different state and federal rules, each with their own unique compliance reporting requirements, Congress should pass a federal data privacy framework that pre-empts and replaces state privacy law. But Congress must only pass that framework if it is clear, concise, and limits the powers of the unelected agency bureaucrats that enforce it. At an absolute minimum, Congress must pass a data privacy law that pre-empts the emerging sectoral approach to privacy policy (healthcare, biometric, etc.) in the states. A sectoral approach to privacy may

[5] Ibid.
[6] Ill-Suited Privacy Rights of Action and Privacy Claims, Institute for Legal Reform, July 2019, https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.
[7] Lori S. Ross, Biometric Data Protection: A Growing Trend in State Privacy Legislation, Outside GC, February 7, 2024, https://www.outsidegc.com/blog/biometric-data-protection-a-growing-trend-in-state-privacy-legislation.
[8] Jim Potter, "Recap of New State Health Data Privacy Laws," PharmaLive, February 11, 2025, https://www.pharmalive.com/recap-of-new-state-health-data-privacy-laws/#:~:text=While%20HIPAA%20remains%20the%20primary,or%20extend%20beyond%20HIPAA's%20protections.

have been beneficial at the federal level insofar as it promoted a light-touch federal approach to privacy that enabled technological market experimentation and change in a manner that superseded state interventionism. But if such an approach is pursued by many states—both more heavy-handedly and with their own unique parochial variations—then the United States will not be contending with one data privacy patchwork but many. Congress can pre-empt that budding issue by creating a pre-emptive national framework.

Option 2: Sectoral Pre-emption with Choice of Law

With so many states having spent time debating and passing a data privacy law, it may be a political challenge to pass a framework that pre-empts all of those laws. If a national framework proves politically elusive, Congress should consider an alternative that at least pre-empts the emergence of sectoral privacy laws like BIPA in Illinois and My Health, My Data in the state of Washington. Here's how it could work. Congress applies a *choice of law* framework to comprehensive data privacy laws. Under such a framework, Congress would create a federal statute requiring states to recognize contractual choice-of-law provisions, giving companies a choice of which state comprehensive data privacy law to follow and thereby increasing competition among states to adopt the best law.[9] Companies looking to signal trust to consumers could adhere to more stringent state rules and advertise their choice to build trust. But small companies would not be forced into complying with more burdensome data privacy regimes. That is a win-win scenario for industry and consumers, which makes it a politically palatable compromise worth exploring if Congress continues to demonstrate an inability to compromise on an all-inclusive federal framework.

Pre-empt the Budding AI Patchwork (Question V)

Just like the privacy patchwork threatens data-reliant businesses—including AI—a growing patchwork of AI-specific laws in the states could derail the AI revolution by deterring investment and smothering businesses, especially small businesses, in costly, confusing, and expensive rules and regulations. Whatever the harms of the current data privacy patchwork, the

[9] Geoffrey A. Manne and Jim Harper, "A Choice-of-Law Alternative to Federal Preemption of State Privacy Law, International Center for Law & Economics," March 15, 2024, https://laweconcenter.org/resources/a-choice-of-law-alternative-to-federal-preemption-of-state-privacy-law/.

emerging artificial intelligence patchwork is worse—and it is also intrinsically linked to the privacy wars. When Chat-GPT rose in popularity in 2022, and then became increasingly popular in 2023, states immediately responded by amending their data privacy frameworks to reflect the rise in popularity of AI systems and applications, with 10 states including regulatory language changes and amendments to laws that were passed or becoming effective in 2023.[10]

The even bigger concern is that state data privacy policy will merge with a complicated web of state-level AI bias and algorithmic fairness legislation. More than 200 state lawmakers from over 45 states had met as a part of the Multistate AI Policymaker Working Group to coordinate AI policy across the country. Despite widespread and bipartisan participation, research from the American Consumer Institute (ACI) finds AI bias and fairness laws are spiraling into a patchwork nevertheless.[11]

Inside of this patchwork, data regulation runs rampant. Under the Colorado law (the only passed state-level AI bias law to date), developers must provide descriptions, summaries, and documentation of the training data, document biases of data sources, categorize the data itself, and even provide opt-out notices for data processing similar to how states provide opt-out provision in comprehensive state data privacy laws.[12] As Governor Jared Polis warned when signing the Colorado law, a state level "patchwork across the country can have the effect to tamper innovation and deter competition in an open market" and that these kind of laws would be better applied "by the federal government to limit and preempt varied compliance burdens on innovators."[13] Congress should avoid the temptation to replace bad state law with an even more broadly applicable federal version of the same distortionary rules—but Governor Polis is right to worry that a patchwork could harm AI innovation. Congress should pre-empt the Colorado law—and the privacy laws being used to regulate AI—with a different approach

[10] Katrina Zhu, "The State of State AI Laws: 2023," Electronic Privacy Information Center, August 3, 2023, https://epic.org/the-state-of-state-ai-laws-2023/.
[11] Logan Kolas and Nate Karren, "Irresponsible Collaboration: Evidence of a Growing AI Fairness Patchwork," American Consumer Institute, February 27, 2025, https://www.theamericanconsumer.org/2025/02/report-irresponsible-collaboration-evidence-of-a-growing-ai-fairness-patchwork/.
[12] Colorado Anti-Discrimination in AI Law, S.B. 24-205, https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.
[13] Future of Privacy Forum, "FPF Multistate AI Policymaker Working Group: Summary of October 2024 Meeting," Google Drive, May 2024, https://drive.google.com/file/d/1i2cA3IG93VViNbzXu9LPgbTrZGqhyRgM/view.

entirely: a streamlined federal framework that pre-empts state AI and data privacy laws, especially in instances where both are regulated as a package deal.

Limiting Bureaucracy in a Data Framework (Question VI(A))

A federal data privacy framework may be preferable to the current approach, but if a federal framework does not limit the power of the agencies that enforce it, then the provisions could be abused, and the law itself will be stretched beyond Congressional intent. Some fear that carveouts in privacy legislation will leave consumers exposed, the far bigger threat is that agencies will use existing laws to stretch the privacy law beyond its original intent. California provides a cautionary tale. Then-California Attorney General Xavier Becerra used discretion under the CCPA to "extend disclosure obligations, impose additional data privacy rules, and further regulate verification procedures and offline retailers" while also exposing California businesses to "prosecutorial 'sweeps' for everything from mobile applications to loyalty programs and employee data."[14] More recently, unelected bureaucrats within the California Privacy Protection Agency (CPPA)—the agency that enforces the CPPA—have explored using agency rulemaking to extend privacy regulations to automated decision-making technologies. As a matter of policy impact, the considered regulations were overly broad, the definitions of automated decision-making and artificial intelligence in that rulemaking were vague, and countless business activities would have been roped into heavy-handed and expensive compliance burdens.[15] While AI fairness legislation in other states had to undergo legislative scrutiny, unelected bureaucrats in California proposed rulemaking to consider risk assessments and other paperwork regulations on *significant* decisions.

Not only must Congress pre-empt this kind of state legislative tinkering in a federal data privacy framework, but it should also learn the lessons of ever-expanding privacy laws in the states by limiting the power of the agencies that will enforce a federal privacy law. As it stands

[14] Logan Kolas, "Key Principles for State Data Privacy Law," The Buckeye Institute, October 12, 2023, https://www.buckeyeinstitute.org/library/docLib/2023-10-Key-Principles-for-State-Data-Privacy-Laws-policy-report.pdf.
[15] Jon Neiditz, John M. Brigagliano, and Henry W. Tharpe, "Public comment period officially opens for California privacy and AI regulations," Kilpatrick Townsend & Stockton LLP, December 1, 2024, https://ktslaw.com/en/Insights/Alert/2024/12/Public-comment-period-officially-opens-for-California-privacy-and-AI-regulations.

now—in a world without a federal framework—the FTC engages in subjective gap-filling that varies by administration.

The FTC already enforces the Children's Online Privacy Protection Act (COPPA) and the Gramm-Leach-Bliley Act (GLBA), and also polices unfair or deceptive privacy practices under Section 5 authority of the FTC Act. But the FTC has also overstepped its authority in advanced notice of proposed rulemakings on commercial surveillance, signaling a desire to grow its regulatory apparatus. That is why Congress was on the right track with provisions in the imperfect American Privacy Rights Act of 2024 that would have terminated proposed expansionary privacy rulemakings by the FTC[16]—but Congress must be even more explicit in future proposals so that agencies due not expand a national framework beyond its original intent.

Conclusion

The United States needs a federal data privacy framework if only to pre-empt rampant and counterproductive state privacy policies and to clarify already existing federal rules around data use. A federal framework will be an improvement over the data privacy split that currently governs only if it is clear, concise, and limits the power of the agencies that enforce it. Importantly, Congress must also pre-empt state data privacy rules regulating artificial intelligence, which in some cases have been regulatory expansions of already existing data privacy rules, and in other cases manifest as entirely new AI regulatory regimes. Congress must act to establish a pro-innovation privacy framework.

Respectfully submitted,

Logan Kolas
Director of Technology Policy
The American Consumer Institute Center for Citizen Research

[16] United States Congress, "American Privacy Rights Act of 2024" discussion draft, https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf.