U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

July 11, 2024

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

Dear Chair Cantwell and Ranking Member Cruz:

The U.S. Chamber of Commerce ("Chamber") respectfully submits the following statement for the record for the Senate Committee on Commerce, Science, and Transportation hearing titled "The Need to Protect Americans' Privacy and the AI Accelerant."

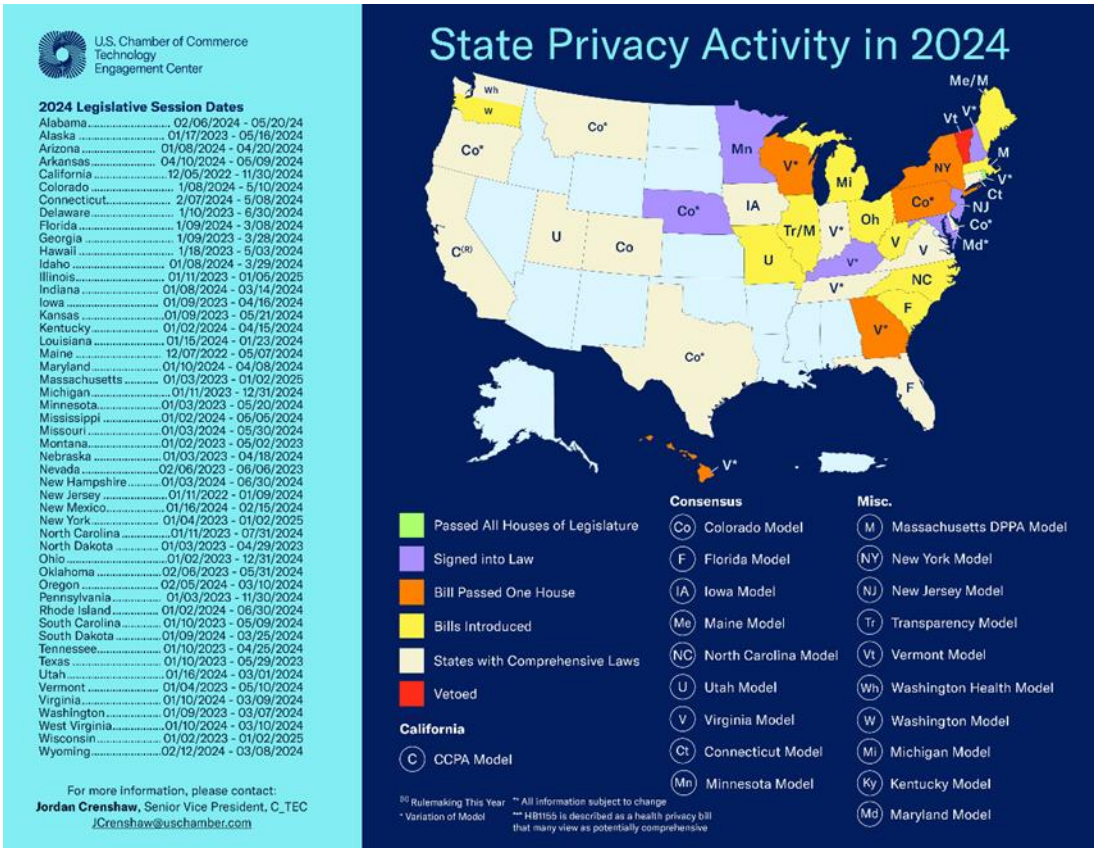
America needs a national data privacy law that ensures equal protection nationwide. In response to the enactment of the California Consumer Privacy Act, the Chamber became the first national business association to propose model legislation that encompassed opt-out, deletion, and transparency rights.[1]

In 2021, the Chamber endorsed Representative Suzan Delbene's (D-WA) Information Transparency and Personal Data Control Act[2] ("ITPDCA") that would have required companies to obtain affirmative consent before the sharing, selling, or disclosing consumers' sensitive data.[3]

In the absence of federal privacy legislation, the Chamber supported the passage of commonsense bills in states like Texas[4], Virginia[5], and Tennessee[6], which have embraced the Consensus Privacy Approach. This approach, which protects over 100 million Americans in sixteen states, most recently including Rhode Island, incorporates the protections in the Chamber's Model Privacy Legislation and the ITPDCA, but also provides consumers with a right to correct inaccurate information as well as opt out of targeted advertising and certain automated profiling.

---

[1] Chamber Model Privacy Legislation (2019) *available at* https://www.uschamber.com/assets/archived/images/uscc_data_privacy_model_legislation.pdf.
[2] H.R. 1816 (117th Congress) *available at* https://www.congress.gov/bill/117th-congress/house-bill/1816/text?s=4&r=1&q=%7B%22search%22%3A%22information+transparency+and+personal+data+control+act%22%7D.
[3] https://americaninnovators.com/wp-content/uploads/2021/03/210310_InfoTransparencyPersonalDataControlAct_Rep.DelBene.pdf
[4] Letter to Texas House *available at*https://americaninnovators.com/wp-content/uploads/2023/04/State_HB4_TexasDataPrivacyandSecurityAct_TXHouse.pdf
[5] Letter to Virginia Governor, *available at*https://americaninnovators.com/wp-content/uploads/2022/08/Virginia-Data-Privacy-Act-Letter.pdf
[6] Letter to Tennessee Legislature, *available at*https://americaninnovators.com/wp-content/uploads/2023/04/230417_State_BS73_TNPrivacy_TNSenate.pdf



Two primary issues continue to drive whether national data privacy legislation will strike the right balance in protecting consumers and enabling entrepreneurship and innovation—preemption of state laws and enforcement. As incorporated into the Chamber's Model Privacy Legislation and ITPDCA, successful national data protection legislation must have strong preemption of state laws related to data privacy and security to avoid a confusing and costly patchwork of future local and state regulations. A national privacy law should follow what all nineteen states enacting privacy laws have done by empowering expert agencies and State Attorneys General as enforcers and not establishing private rights of action which would be subject to abuse.

We applaud the Committee for addressing the impact of data protection on Artificial Intelligence ("AI"). America finds itself in a race against non-democratically aligned nations like China to lead in the development and deployment of AI. Public trust is crucial for the implementation of AI. This is why we have prioritized the need to build public trust in AI through our continued efforts. The Chamber established a bipartisan Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation led by former members of Congress John Delaney (D-MD) and Mike Ferguson (R-NJ) which released a report detailing how to regulate AI.[7] The Commission recommended that Congress should evaluate existing law and

[7] U.S. Chamber Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation Final Report (March 2023) *available at* https://www.uschamber.com/technology/artificial-intelligence-commission-report.

appropriately fill in gaps with a risk-based approach. We urge Congress to pass national privacy legislation before enacting AI-specific laws. Concurrently, Congress must conduct a legal gap analysis as proposed by Senators Schumer, Young, Rounds, and Heinrich.[8]

The Chamber provides the following recommendations on preemption, enforcement, data minimization, small business, and AI as Congress contemplates privacy protections.

I. The Need for a Single, National Privacy Standard

Congress should include in any federal privacy legislation full preemption of state standards. A national privacy law without strong preemption would enable a state patchwork of laws that would confuse consumers and potentially make it impossible for small businesses to comply. To ensure full preemption, national privacy legislation must preempt all state laws *related* to broad categories of data privacy and security practices and not preempt state rules and regulations merely covered by a law.

A recent report highlighted that a national patchwork of privacy laws would cost the United States economy $1 trillion and disproportionately impact small businesses with a $200 billion economic burden.[9] Many small businesses are worried that a patchwork of state laws will increase litigation and compliance costs.[10]

The recently introduced H.R. 8818, the "American Privacy Rights Act ("APRA") unfortunately follows the approach of only preempting what is in a national bill as opposed to strong preemption. Although APRA's advocates express an intention to create "uniform national data privacy and security standard," the actual provisions of the draft provide only limited preemption and would allow states to pass more restrictive privacy laws. APRA only preempts "any law, regulation, rule, or requirement *covered by* the provisions of this Act or a rule, regulation, or requirement promulgated under this Act."[11]

To ensure full preemption, a national privacy law must expressly preempt all law related to broad categories of activity. APRA's preemption language fails to meet this standard. According to a Congressional Research Service report, to provide the strongest preemption, Congress should use clearer and more forceful terms than "covering" or "covered by."[12] Congress should avoid merely preempting what a proposed bill is "covering" or "covered by," because such clauses are considered by the Supreme Court "to have a narrower effect than 'related to' preemption clauses.[13] The Supreme Court has stated that "covered by"

---

[8] Bipartisan Senate Working Group AI Roadmap (May 2024) *available ati* https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf.
[9] ITIF, "The Looming Cost of a Patchwork of State Privacy Laws," (January 2022) *available at* https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.
[10] U.S. Chamber "Empowering Small Business: The Impact of Technology on U.S. Small Business," (September 2023) *available at* https://americaninnovators.com/wp-content/uploads/2023/09/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf.
[11] H.R. 8818 (118th Congress) § 118(a)(2) (emphasis added).
[12] Congressional Research Service "Federal Preemption: A Legal Primer," (May 2023) *available at* https://crsreports.congress.gov/product/pdf/R/R45825.
[13] *Id.* at 10.

language "indicates that pre-emption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[14]

A national privacy law that merely preempts what it "covers" and then provides for exceptions to that preemption would likely be viewed by courts as evidence that Congress has not intended to "substantially subsume" regulation. The APRA draft would also create exceptions to preemption in the areas of consumer protection, health data, and remedies based on California's Consumer Privacy Act and highly abused lawsuits under the Illinois Biometric Privacy Law. These exceptions could easily be exploited by the trial bar in lawsuits and state legislatures to circumvent preemption in APRA.

There are better models. Congress, like it did when passing the Airline Deregulation Act, should craft preemption language that supersedes laws related to broad categories of potentially regulated activities. In recent years, legislation has been authored by both Republicans and Democrats that would provide strong preemption, including:

- H.R. 3388, the "SELF DRIVE Act," from the 115th Congress, which preempted broad categories of activities and passed the House by unanimous consent.
- H.R. 1816, the Information Transparency and Personal Data Control Act, from the 117th Congress, that provided: "No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard *related to* the data privacy or associated activities of covered entities."[15] Representatives Carter (R-GA) and Obernolte (R-CA) suggested similar language to amend APRA.[16]
- Financial Services Committee Chairman Patrick McHenry's "Data Privacy Act of 2023" draft from the current Congress, which provides that federal legislation "supersedes any statute or rule of a State."[17]

II. Enforcement

Comprehensive privacy legislation should leave enforcement to agencies like the Federal Trade Commission and state attorneys general, not the private trial bar. Such private rights of action would invite unwarranted lawsuits that would hamstring innovation and the viability of some innovators. Frivolous, non-harm-based litigation has been used in the past to extract costly settlements from companies, including small businesses. Private rights of action ("PRA") are ill-suited in privacy laws because they:[18]

---

[14] See e.g., *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 658, 664 (1993).
[15] *Supra* n. 2 (emphasis added).
[16] Amendment to APRA (June 2024) *available at* https://docs.house.gov/meetings/IF/IF00/20240627/117487/BILLS-118-HR8818-C001103-Amdt-15.pdf.
[17] H.R. 1165 at § 6 (118th Congress) *available at* https://www.congress.gov/bill/118th-congress/house-bill/1165/text?s=1&r=1&q=%7B%22search%22%3A%22mchenry+data+privacy+act%22%7D.
[18] U.S. Chamber Institute for Legal Reform, "Ill-Suited: Private Rights of Action and Privacy Claims," (July 2019) *available at* https://instituteforlegalreform.com/wp-content/uploads/2020/10/Ill-Suited_-_Private_RIghts_of_Action_and_Privacy_Claims_Report.pdf.

- Undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who are best positioned to understand the complexities of compliance, promote innovation, and prevent and remediate harms.

- Entail inconsistent and dramatically varied, district-by-district court rulings. Agency enforcement can provide constructive, consistent decisions that shape privacy protections for all American consumers and provide structure for companies aiming to align their practices with existing and developing law.

- Are, when combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers.

- Hinder innovation and consumer choice by the uncertain and pervasive threat of lawsuits, particularly for companies at the forefront of transformative new technologies.

None of the nearly 20 states that have enacted comprehensive legislation have adopted private rights of action as an enforcement mechanism for privacy violations. In fact, states like Vermont, Washington, and Maine have failed to enact legislation because of proposed PRAs. Most recently, Governor Phil Scott of Vermont issued a veto of a privacy bill with that was sustained by both Democrat and Republican state senators because it would "create an unnecessary and avoidable level of risk" and "make Vermont a national outlier, and more hostile than any other state to many businesses and non-profits."[19] He cited concerns from mid-size and small businesses about the negative impact of private lawsuits.

Private rights of action would be particularly devastating for business under a privacy law that does not have a strong preemptive effect. Not only would states be able to continue passing their own laws, but individual judicial district precedent could also create further confusion and conflict.

III. Data Minimization

The Chamber recommends that national data minimization standards align with the Consensus Privacy Approach. Data minimization can be an important component of regulation to ensure the privacy and security of individuals, but overly broad, unnecessarily strict, or poorly crafted data minimization standards would impede innovation. The State Consensus Approach achieves the right balance.

States adopting the Consensus Privacy Approach have enacted a balanced and workable data minimization standard. For example, states like Colorado, Tennessee, and

[19] Governor Scott Veto Statement (June 2024) *available at* https://governor.vermont.gov/press-release/action-taken-governor-phil-scott-legislation-june-13-2024.

Texas mandate that companies limit data collection to what is "adequate, relevant, and reasonably necessary" related to a disclosed or specified purpose.[20]

By contrast, APRA would limit all data collection and processing to "necessary, proportionate, and limit[ed] to provide or maintain" a specific product or service or consumer or anticipated communications.[21] Although both the Consensus Privacy Approach and APRA have exceptions for certain practices like security, APRA would limit companies from collecting data that may be necessary for providing a service but can also have a societally beneficial purpose utilized by other companies. These secondary purposes include anti-fraud protections, Know Your Customer, and other web-based security applications, including those used by federal programs to reduce theft of benefits and identity fraud. Secondary data sets have also enabled law enforcement to intervene and stop incidents of violence, human trafficking, and organized crime.[22]

In the AI context, overly strict data minimization could potentially harm algorithmic accuracy and fairness. Safe and responsible AI is contingent upon good data. Therefore, in any potential privacy legislation Congress must be mindful that specific limitations around what data is allowed to be collected could have profound consequences for ensuring systems outputs remain lawful and non-discriminatory.

This sentiment is not isolated. Stanford University Human-Centered Artificial Intelligence (HAI) recently highlighted within their policy brief: "As companies and regulators step up efforts to protect individuals' information privacy, a common privacy principle (data minimization) can come to clash with algorithmic fairness."[23]

IV. Small Business Impacts

National data privacy and AI regulation will have significant impacts on small businesses who use technological tools and data analytics to compete with larger companies. According to recent research by the U.S. Chamber of Commerce, as of 2023, **one quarter** of U.S. small businesses were using AI.[24] Another **39 percent** are planning to use it in the future.[25] Nearly **seven in ten** small businesses believe that technology and data enable them to compete with larger companies. For example, AI is helping small business owners cut down on marketing time and costs during a tight economy.[26] **73 percent** of small businesses state that losing access to data will harm their ability to grow. **65 percent** worry that losing targeted advertising will harm their business. As noted, most small businesses are concerned that a patchwork of state AI and privacy laws will increase their compliance and litigation costs.

---

[20] *See, e.g.* Colo. Rev. Stat. § 6-1-1308(3); Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1).
[21] *Supra* n. 11 at § 102(a).
[22] Chamber Technology Engagement Center, "Data For Good: Promoting Safety, Health and Inclusion," (January 2020) *available at* https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.
[23] Stanford HAI "The Privacy-Bias Tradeoff" (October 2023) *available at* https://hai.stanford.edu/policy-brief-privacy-bias-trade.
[24] *Supra* n. 10.
[25] *Id.*
[26] Jordan Crenshaw, "Enhancing Entrepreneurship: AI's Big Impact on Small Business, (May 2024) *available at* https://www.uschamber.com/technology/enhancing-entrepreneurship-ais-big-impact-on-small-business.

The Chamber offers several recommendations to ensure small businesses are not disproportionately harmed by national data privacy and AI legislation:

- **Exceptions.** Privacy exceptions for small businesses should mirror the Consensus Privacy Approach. For example, Virginia's privacy law clearly exempts small businesses that "control or process personal data of at least 100,000 consumers or control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."[27]

  By contract, APRA would require businesses meet a three-prong test to obtain an exemption. In addition to revenue and data retention thresholds, the test would require small businesses not transfer data "in exchange for revenue or anything value" in order to avail themselves of the small businesses exemption.[28] Such vague terminology like "exchange for anything of value" would likely lead to prolonged litigation to define what "value" is for small businesses to even prove they are exempt from a privacy law in the first place.

- **Data Minimization Requirements.** National privacy legislation should allow for tailored, contextual, and targeted advertising. Congress should not ban the use of data for such advertising by default by strict data minimization requirements. Instead, Congress should follow the Consensus Privacy Approach and enable customers the ability to opt out of such advertising or automated profiling.

- **Preemption.** Data privacy legislation must ensure small businesses are not subject to a patchwork of state laws if they do receive an exemption. As noted previously, it is important that Congress preempt all state laws related to data privacy and security as opposed to only preempting laws "covered by" a national standard. In fact, the Congressional Research Service noted about APRA that "[t]here may also be litigation over the scope of the APRA's preemption provisions. For instance, questions may arise as to whether the APRA preempts state privacy laws that regulate entities not covered by the APRA, such as small businesses."[29]

V. Artificial Intelligence.

AI is a driver of U.S. economic growth. Generative AI has the potential to increase global GDP by $7 trillion over the next ten years.[30] AI is helping us discover cures quicker, securing our networks, and alleviating worker shortages in critical areas like healthcare. The Chamber has long understood that for the United States to continue to reap the benefits of the 21st-century digital economy and continue to be a global leader in emerging technologies

---

[27] Va. Code § 59.1-576(A).
[28] *Supra* n. 11 at § 101(51)(a)(iii).
[29] Congressional Research Service, "Legal Sidebar: The American Privacy Rights Act," (May 2024) *available at* https://crsreports.congress.gov/product/pdf/LSB/LSB11161.
[30] Goldman Sachs, "Generative AI could raise global GDP by 7%," (April 2024) *available at* https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html.

such as AI, we need a fully preemptive national privacy standard to provide necessary market certainty around data usage.

The Chamber has strong concerns regarding recent calls from Congress and Agencies which would limit data and have extreme implications on AI governance, as safe and responsible AI is contingent upon good quality data. Therefore, in any potential privacy legislation, Congress must be mindful that specific limitations around what data is allowed to be collected could have profound consequences for ensuring systems outputs remain lawful and non-discriminatory.

The Chamber believes that Congress's bicameral and bipartisan working groups to develop recommendations on US AI leadership is both timely and imperative. The Chamber has taken similar actions to provide policymakers a bi-partisan consensus path forward, by establishing its own independent commission on Artificial Intelligence on Competitiveness, Inclusion, and Innovation ("Commission"). The Commission tackled many of the issues which Congress is examining today including the correct manor to regulate AI to ensure that society can obtain the great benefits of AI, while simultaneously ensuring necessary guardrails are in place. The Commission's final report advocated for five-pillars of regulating AI[31]:

- Efficiency: Policymakers must evaluate the applicability of existing laws and regulations. Appropriate enforcement of existing laws and regulations provides regulatory certainty and guidance to stakeholders and would help inform policymakers in developing future laws and regulations. Moreover, lawmakers should focus on filling gaps in existing regulations to accommodate new challenges created by AI usage.

- Neutrality: Laws should be technology neutral and focus on applications and outcomes of AI, not the technologies themselves. Laws regarding AI should be created only as necessary to fill gaps in existing law, protect citizens' rights, and foster public trust. Rather than trying to develop a one- size-fits-all regulatory framework, this approach to AI regulation allows for the development of flexible, industry-specific guidance and best practices.

- Proportionality: When policymakers determine that existing laws have gaps, they should attempt to adopt a risk-based approach to AI regulation. This model ensures a balanced and proportionate approach to creating an overall regulatory framework for AI.

- Collegiality: Federal interagency collaboration is vital to developing cohesive regulation of AI across the government. AI use is cross-cutting, complex, and rapidly changing and will require a strategic and coordinated approach among agencies. Therefore, the government will need to draw on expertise from the different agencies, thus allowing sector and agency experts the ability to narrow in on the most important emerging issues in their respective areas.

[31] *Supra* n. 7.

- **Flexibility:** Laws and regulations should encourage private sector approaches to risk assessment and innovation. Policymakers should encourage soft law and best practice approaches developed collaboratively by the private sector, technical experts, civil society, and the government. Such nonbinding, self-regulatory approaches provide the flexibility of keeping up with rapidly changing technology as opposed to laws that risk becoming outdated quickly.

These recommendations would establish a sensible path towards ensuring that businesses have the necessary certainty when it comes to the use of these important tools. The Chamber has strongly supported previous congressional efforts, such as the American Competes Act, which would require a legal gap analysis to be conducted. We urge Congress to complete a review of current laws that may implicate AI safety and trustworthiness before passing AI-specific legislation.

We look forward to working with you to make the goal of national privacy legislation and American AI leadership a reality.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce