U.S. Chamber of Commerce

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

April 7, 2025

VIA ELECTRONIC SUBMISSION

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington DC, 20515

The Honorable John Joyce
Vice Chair
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Re: Comments on Request for Information to Explore Data Privacy and Security Framework

The U.S. Chamber of Commerce ("Chamber") respectfully submits comments in response to the U.S. House of Representatives Privacy Working Group's Request for Information ("RFI") to explore a data privacy and security framework.[1] Data is foundational to the economic growth that boosts wages and creates jobs, allows small businesses to compete, promoting societal welfare like public safety and healthcare, and allows the United States to lead the globe in key emerging technologies such as Artificial Intelligence. At the same time, Americans should be assured that their privacy is protected in a consistent manner across the entire country and businesses must have the means necessary to comply with those requirements and while being able to innovate.

Accordingly, Congress should enact national data privacy legislation that has strong preemption and appropriate enforcement mechanisms. Such legislation should also enable reasonable and responsible uses of data by businesses for societally beneficial uses and allow for continued innovation. At the same time, there needs to be appropriate government enforcement to prevent fraud and increase the security and safety of all Americans.

The RFI appropriately recognizes that the United States digital economy adds $2.6 trillion to the economy and employs millions of Americans.[2] One of the benefits of the data-driven economy is the empowerment of small businesses and startups. The Chamber recently published the third installment of its *Empowering Small Business* report which found that 40 percent of small businesses are employing a generative AI

[1] Chairman Guthrie and Vice Chair Joyce Press Release (February 21, 2025) *available at* https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework.
[2] *Id*.

tool and 98 percent are using an AI-enabled tool.[3] Businesses that are greater adopters of data-driven technologies, such as AI, were found to be more likely to have higher sales growth and job creation as compared to their counterparts who are not.[4]

The data-driven economy provides economic benefits to all sectors. Data is driving solutions to societal issues such as public safety, healthcare, and financial inclusion.[5] Data-enabled AI and secondary uses of data are already helping researchers to diagnose diseases, such as cancer, quicker and more accurately, develop new medical treatments, help emergency responders track wildfires, and for the government to operate more efficiently. To obtain these benefits, Congress needs to preempt the complex patchwork of state laws by adopting national privacy legislation.

A limited bipartisan consensus has been achieved through the sixteen states, including Kentucky, Texas, Virginia, that have adopted the Consensus Privacy Approach which gives over 100 million Americans consistent and reasonable data protections.[6] The Consensus Privacy Approach has data protections like the right to access, delete, and correct data held by companies and opt out of certain data processing and sharing practices. These states all vest their enforcement authorities in experienced government agencies and rejects private lawsuits which could be abused, while leading to decreased innovation and higher prices. This is why the Chamber and nearly 40 other trade associations called for Congress to draw upon the Consensus Privacy Approach in national legislation.[7]

I. Roles and Responsibilities.

To achieve these goals, Congress must delineate roles in the data processing ecosystem for controllers, processors, and third parties.

---

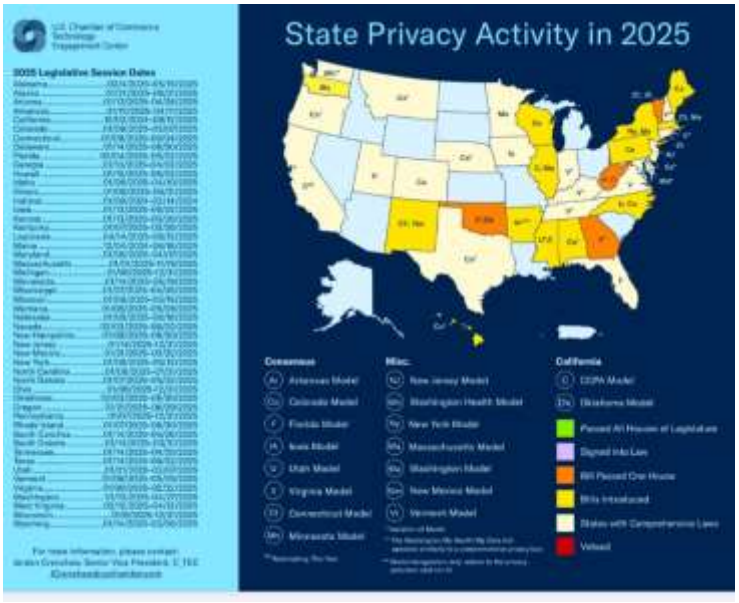
[3] U.S. Chamber of Commerce, *Empowering Small Business: The Impact of Technology on U.S. Small Business* (September 2024) *available at* https://www.uschamber.com/assets/documents/Impact-of-Technology-on-Small-Business-Report-2024.pdf.

[4] *Id*.

[5] U.S. Chamber of Commerce, *Data for Good: Promoting Safety, Health, and Inclusion* (January 2020) *available at* https://www.uschamber.com/assets/documents/ctec_dataforgood_v4-digital.pdf.

[6] Jordan Crenshaw, "What Congress Can Learn from the States on Data Privacy," Real Clear Policy (January 30, 2024) *available at* https://www.realclearpolicy.com/2024/01/30/what_congress_can_learn_from_the_states_on_data_privacy_1008521.html.

[7] Letter to Chairmen Cruz and Guthrie and Ranking Members Cantwell and Pallone (January 24, 2025) *available at* https://www.uschamber.com/assets/documents/Coalition_PrivacyDay_SenateCommerceHouseEC_2025-01-28-143316_mbsb.pdf.



A. Controllers

"Controllers" under the Consensus Privacy Framework are "the natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data."[8] Generally, controllers are responsible for honoring consumer rights requests[9], data limitation requirements, seeking consumer consent for processing sensitive information, and providing consumers with meaningful and clear privacy notices.[10] Considerations for appropriate obligations for controllers include safe harbors. Additionally, safe harbor considerations should be discussed.

B. Processors

"Processors" in states that have adopted the Consensus Privacy Approach are "a natural or legal entity that processes personal data on behalf of a controller."[11] Generally, processors are to adhere to controller instructions and assist controllers in meeting their obligations under the privacy law. Such assistance includes where practicable assisting with consumer rights requests. States adopting this approach also require a contract between a controller and processor to ensure binding processing terms are agreed upon. Additionally, determining whether an entity is a controller or processor is a fact-based determination depending on the context in which personal data is processed.[12]

[8] Va. Code Ann. § 59.1-575.
[9] *See e.g.* Ct Gen Stat § 42-518.
[10] *Id*. at § 42-520.
[11] Ky Rev Stat § 367.3611(22).
[12] CT Gen Stat § 42-521.

C. Third Party

A "Third Party" is a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."[13] Under the Consensus Privacy Approach, consumers have the right to opt out of the sale of personal data to unaffiliated third parties.[14] It is also important to note that third parties can also operate as controllers subjecting them to obligations.

D. Small Businesses

National data privacy legislation should be appropriately scoped so as not to overly burden small businesses. According to Chamber research, nearly three quarters of U.S. small businesses believe that limiting access to data will harm their operations.[15] Small businesses will also disproportionately bear the burden of compliance costs without appropriate protections.

Small businesses should benefit from federal preemption while having a scaled compliance regime versus larger companies. To provide for such scaling privacy law requirements should only apply to companies that process the personal data of over 200,000 people or those who process the personal data of over 50,000 and derive at least 50 percent of revenue from personal data sales. Legislation should also substantively promote use—with appropriate privacy protections—of digital tools like personalized advertising and analytics that give small businesses a competitive edge.

II. Personal Information, Transparency, and Consumer Rights

A. Definitions of Personal Information and Sensitive Personal Information

Personal information covered by national privacy legislation should be "any information that is linked or reasonably linkable to an identified or identifiable natural person."[16] Personal information should not include de-identified data, aggregated, or publicly available information. Furthermore, consistent with the approach taken at the state level, the definition of personal data should also exclude data used in the employment context or commercial context, which generally represent a lower risk of harm or are otherwise subject to existing protections at the state level in various employment and anti-discrimination legislation.

[13] VA Code Ann § 59.1-575.
[14] *Id*. at § 591-577(A)(5).
[15] *Supra* n. 3 at 25.
[16] Ky. Rev. State § 367.3611(19).

States that have adopted the Consensus Privacy Approach have defined "sensitive information" which triggers an opt-in requirement for processing. In Virginia for example, sensitive personal information includes among other things data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, genetic or biometric information, personal information from a known child, or precise geolocation information.[17]

B. Consumer Disclosures

Federal privacy legislation should require controllers to disclose their data practices in a public privacy policy including[18]:

- The categories of data processed by companies;
- The general purposes for processing data;
- How consumers can exercise their rights; and
- Categories of third parties with whom companies share data

C. Consumer Protections

Consumers should have the right to determine how personal information is used, collected, and shared. For this reason, properly scoped and subject to reasonable exemptions to allow for beneficial data uses, we believe individuals should be given the right to:

- Know whether a company is processing their personal information;
- Correct and delete their personal information;
- Obtain a portable copy of their personal information; and
- Opt out of targeted advertising (as defined in the Consensus Privacy Approach) that is based upon activities across unaffiliated websites, the sale of their personal information, and automated profiling that facilitates significant decisions that produce adverse legal or similarly significant effects on a consumer.

Companies should limit the collection of personal data to what is reasonably necessary in relation to the purposes for which that personal data is processed as *disclosed* to the consumer. A national privacy law should prohibit unlawful discrimination using data, including retaliating against consumers for exercising their privacy rights.

[17] VA Code Ann § 59.1-575.
[18] Tex. Bus. § Comm. Code § 54.102(a).

D. Sensitive Data Protections

National privacy legislation should require controllers obtain consent before processing sensitive consumer data, properly scoped to allow for beneficial data uses as discussed below in Section VII(B) of our comments.

III. Existing Privacy Frameworks and Protections

Congress should pass a fully preemptive privacy law that eliminates a state patchwork of laws and prevents States from drafting laws that survive preemption in the future. Simply adopting a national privacy law without strong preemption would enable a state patchwork of laws that will be confusing to both consumers and potentially impossible for small businesses to comply.

A 2022 report from ITI 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.[19] Most small businesses are worried a patchwork of state laws will increase litigation and compliance costs.[20]

To achieve the goal of strong preemption, a national privacy law must explicitly state that it preempts or supersedes all state privacy laws and regulations *related to* data privacy and security. Recent legislation like the American Privacy Rights Act failed to achieve this needed language by mere proposing to preempt what was *covered by* the national privacy law.

To provide the strongest preemption, according to a Congressional Research Service report, Congress should use stronger language that "covering" or "covered by" in order to achieve the goal of ending a patchwork.[21] According to the Supreme Court, "'Covering' is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[22] Under a "covered by" approach, Congress would have to insert in a national privacy law all the obligations and requirements that all states have in order to fully preempt what has been passed. This approach also does not account for future laws passed by states that do not match requirements to the federal approach.

---

[19] 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/.

[20] *Supra* n. 3 at 25.

[21] Congressional Research Service "Federal Preemption: A Legal Primer," (May 2023) *available at* https://crsreports.congress.gov/product/pdf/R/R45825

[22] *CSX Transportation, Inc. v. Easterwood*, 507 U.S. 663 (1993.)

We would also encourage Congress to refrain from excessive exceptions to preemption that could be interpreted by courts as language showing Congress did not intend for there to be strong preemption. For example, Congress should avoid carving out from preemption biometric[23] and broad health privacy laws.[24] At the same time, privacy legislation should not broadly preempt against laws of general applicability like state consumer protection and civil rights laws so long as the underlying claim is not based in a privacy violation.

IV. Data Security

National privacy legislation should establish baseline security requirements. All the states that have adopted the Consensus Privacy Approach require organizations processing consumer data should establish, implement, and maintain reasonable administrative, technical, and physical security practices that are appropriate to the volume and nature of the data being used.[25]

In addition, Congress should consider data security legislation that recognizes businesses' use of existing standards, guidelines, and frameworks to meet a law's and/or a regulation's requirements. In exchange, businesses would qualify for congressionally crafted regulatory and legal protections to invest in and meet heightened security requirements that are based on risk.

V. Artificial Intelligence

The Chamber appreciates the question regarding how a federal comprehensive data privacy law should address state-level AI frameworks. We have significant concerns that a fragmented policy landscape will result in a patchwork of potentially conflicting federal and state artificial intelligence laws, which would adversely impact entrepreneurs, small businesses, and the broader business community.

In an Open Letter to State Leaders on Artificial Intelligence, over 50 State and Local Chambers emphasized that "A federal framework is the best option to provide American businesses with the certainty they need to invest in AI development and adoption."[26] The letter highlighted how Artificial Intelligence, particularly generative AI, "has entered the public consciousness and has brought a new age of possibility for

[23] *See e.g.* 740 ILCS 14/1.
[24] *See* RCW § 19.373.005 *et al.*
[25] Tex. Bus. $ Comm. Code § 541.101(a)(2).
[26] U.S. Chamber of Commerce. "Open Letter to State Leaders on Artificial Intelligence." *U.S. Chamber of Commerce*, 29 Nov. 2023, https://www.uschamber.com/technology/artificial-intelligence/open-letter-to-state-leaders-on-artificial-intelligence.

businesses and workers, with the potential to solve some of society's most pressing challenges."[27]

This sentiment aligns with Vice President JD Vance's recent remarks that AI will serve as the foundation for "innovation, job creation, national security, health care, free expression, and beyond. And to restrict its development now would mean paralyzing one of the most promising technologies we have seen in generations."[28]

The Chamber believes that a patchwork of state and federal laws would impede this technology's promising potential and undermine U.S. leadership in artificial intelligence development.

The Chamber provides the following recommendations on how the Privacy Working Group should address the growing state-level actions related to automated decision-making:

A. A Federal Privacy Law will empower consumers and mitigate AI risk:

The Chamber believes that a fully preemptive national privacy law, reflecting the Consensus Privacy Approach, is essential. This approach adopts a general framework of various consumer rights, including opting out of use of personal information in automated profiling that result in significant decisions that produce adverse legal or similarly significant effects on a consumer, opting out of the use of personal information in targeted ads, deleting and correcting data, and requiring consent for the processing of sensitive data use. By including these requirements in a national law and providing strong preemption, consumers' data will be protected from misuse, regardless of the type of technology a business is using - including AI.

B. Congress Should Review Gaps in Current AI Regulation Laws:

As Congress looks at AI risks beyond the context of privacy, we should note that many state legislators working on AI bills do so from the misconception that existing federal laws and regulations inadequately address the use of technology. This notion is mistaken.

First, many AI activities, such as machine learning or chat-bots have been used for years and many AI uses are already covered by law. As we have written before, the Chamber believes that Congress and the Executive Branch should inventory existing laws and regulations pertaining to AI. That inventory should identify potential gaps

[27] *Id*.

[28] Remarks by the Vice President at the Artificial Intelligence Action Summit, Paris, France." (February 11, 2025) *available at* https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france.

and then use a risk-based analysis to determine if new laws and regulations are needed. Last year, the House AI Task Force recommended the "use of a sectoral regulatory structure[29]" and taking an "[i]ncremental Approach[30]" should be the foundation for Congressional efforts to build a long-standing and "durable policy framework[31]" to govern AI.

VI. Accountability and Enforcement

Federal privacy legislation should encourage cooperation between the business community and government, not promote adversarial action that results in frivolous litigation. The Federal Trade Commission and State Attorneys General should have exclusive enforcement authority. In the case where companies already fall under sectoral regulations like the insurance industry, national privacy legislation should allow for these companies to continue to be regulated by their current regulators like state insurance commissioners where appropriate. In other areas, such as the online ecosystem, more harmonized treatment of comparable information under the authority of a single, federal regulator, the FTC, is advisable for consistency.

Businesses should be given a reasonable opportunity to cure violations of the law that do not result in harm before enforcement actions can be taken. Additionally, including a safe harbor provision that offers an affirmative defense for entities complying with established security standards.[32]

Federal privacy legislation should follow the Consensus Privacy Approach by stating that nothing in the law "shall be construed as providing the basis for, or be subject to, a private right of action for violations...under any other law."[33]

Data protection legislation should avoid empowering the private trial bar at the expense of business innovation and viability. Frivolous, non-harm-based litigation has been used in the past to extract costly settlements from companies, even small businesses, based on privacy law provisions granting a private right of action. Private rights of action are ill-suited in privacy laws because:[34]

---

[29] Bipartisan House Task Force Report on Artificial Intelligence (December 2024) *available at* A163BDBF496ADA741F831E5BEBBCA06699B6AFF8CC34F4FDC4065BDA298295DF.ai-task-force-report-final.pdf

[30] *Id.*

[31] *Id.*

[32] *See e.g.* Tenn Code Ann. § 47-18-3213.

[33] Va. Code Ann. § 59.1-584(E).

[34] 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.

- Private rights of action undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections. By contrast, statutes enforced exclusively by agencies are appropriately guided by experts in the field who can be expected to understand the complexities of encouraging compliance and innovation while preventing and remediating harms.

- They can also lead to a series of 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.

- Combined with the power handed to the plaintiffs' bar in Federal Rule of Civil Procedure 23, private rights of action are routinely abused by plaintiffs' attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionally benefit plaintiffs' lawyers rather than individuals whose privacy interests may have been infringed. It may force businesses to focus their resources on defending this time-consuming and expensive private litigation rather than towards compliance with the law and protecting consumer rights.

- They also hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technologies.

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.

VII. Additional Considerations

A. Data Minimization

Data minimization is critical toward safeguarding the privacy and security of individuals. At the same time, data minimization standards that are too strict could impede innovation and the ultimate goal of protecting people and systems. States that have passed the Consensus Privacy Approach have enacted a balanced and workable data minimization standard.

For example, states like Colorado, Kentucky and Texas mandate companies limit data collection to what is "adequate, relevant, and reasonably necessary" related to a *disclosed or specified* purpose.[35] By contrast, states like Maryland have enacted strict data minimization requirements that only allow the collection of data for "what is necessary and proportionate to provide or maintain a specific product or service requested by the consumer whom the data pertains."[36] Maryland further imposes a restriction that prohibits the collection or processing of sensitive data unless it "is strictly necessary to provide or maintain a specific product or service..."[37] Maryland's law also does not permit consent to collect or process sensitive data.

Such a strict data minimization approach could limit companies' ability to use personal data for important purposes such as anti-fraud protections, Know Your Customer, and other web-based security applications (used by federal programs to reduce theft of benefits and identity fraud.) Data has also enabled law enforcement to stop criminal activity such as human trafficking and organized criminal activity.[38]

Finally, strict data minimization standards are threatening to create conflicting regulations in states. For example, Colorado's new AI law imposes liability on AI developers and deployers who fail to take reasonable care to prevent "unlawful differential...impact" that disfavors individuals or groups on the basis of certain protected classes like race and gender.[39] Many of these protected categories align with definitions of sensitive personal information in privacy laws. Strict data minimization laws would deprive companies of the data necessary to comply with other laws like state AI and anti-discrimination requirements.

B. Societally Beneficial Uses of Data

Federal privacy legislation should explicitly preserve and exempt the processing of personal data for beneficial purposes like offering goods, and services; using payment data to complete transactions; maintaining business operations; offering of bona fide customer loyalty programs; First Amendment protected activities like journalism; effectuating product recalls; publicly available records, employment and worker information; compliance with laws; and supporting law enforcement; fulfilling warranties; promoting and enabling security; preventing, detecting, protecting

[35] *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) (emphasis added).
[36] Md. Code Ann. Comm. Law § 14-4606(B)(1)
[37] *Id.* at § 1404607(A)(1).
[38] 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.
[39] CRS § 6-1-1701.

against, and responding to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or illegal activity; independent measurement and market research; commercial, medical, and scientific research; improving products and services; allowing product recalls; deal with technical errors; and reasonable internal operations.

C. Personalized Advertising

Congress should recognize the value of personalized advertising. In fact, most Americans prefer personalized advertising.[40] Personalized advertising has driven the internet-based economy and enabled access to free or reduced-priced content online. Personalized advertising also helps small businesses compete against larger firms by targeting potential customers who are inclined to engage with their products and services, This makes their advertising spending more efficient and nearly two thirds of small businesses reported that losing their ability to engage in personalized and targeted advertising will harm their business.[41] Personalized advertising also helps consumers by enabling them to see content and ads and marketing that are more likely to resonate and be of interest to them.

The Chamber urges Congress not to impose default bans or opt-in consent requirements for targeted advertising. Additionally, for reasons, stated above, Congress should adopt a data minimization standard in line with the Consensus Privacy Approach and not a strict data minimization standard that would prevent data from being used for advertising. Consumers instead should have the right to opt out of targeted advertising from data collected across unaffiliated websites.

We look forward to working with you to ensure that Congress passes strong, durable, preemptive comprehensive privacy legislation.

Sincerely,

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

[40] IAB, "Nearly 8 in 10 Consumers Would Rather Receive More Ads Than Pay for Digital Content and Services, According to IAB Research" (January 2024) *available at* https://www.iab.com/news/consumer-privacy-research/#:~:text=When%20it%20comes%20to%20personalized,interested%20in%20or%20shopping%20for.
[41] *Supra* n. 3 at 25.