U.S. Chamber of Commerce

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

March 17, 2026

Hearing Before the House Committee on Financial Services Entitled: Updating America's Financial Privacy Framework for the 21st Century

Chairman Hill, Ranking Member Waters, and Members of the Committee,

Thank you for the opportunity to testify on the modernization of the Gramm Leach Bliley Act ("GLBA") and the future of data privacy. The U.S. Chamber of Commerce appreciates the leadership of Chairmen Hill and Barr on this critical issue by seeking comment last year on how to modernize GLBA. We also recognize the leadership of Chairman Guthrie and Vice Chair Joyce in the Energy & Commerce Committee for establishing a robust and transparent process for developing comprehensive privacy legislation.

For nearly 25 years, the GLBA[1] has provided a reliable foundation for financial privacy. Updating the existing framework—rather than creating a new one—is the most targeted and effective path forward. Modernization should strengthen clarity, streamline compliance, and preserve the law's proven protections.

As data increasingly fuels economic growth and innovation, consumers deserve privacy rules that are consistent, clear, and enforceable. While we appreciate the Committee's work to modernize the GLBA, we must underscore the broader need for Congress to pass a comprehensive national privacy law to ensure true uniformity across the country. Updates to GLBA should be harmonized, avoid duplicative regulation, and be interoperable with any potential comprehensive privacy law. My testimony today will focus on four key priorities for any federal privacy law:

1. **Establishing strong federal preemption to ensure a uniform national standard;**
2. **Providing clear, predictable enforcement mechanisms; and**
3. **Preserving access to data that enables socially beneficial uses, innovation, and risk management**
4. Essential Modernizations Considerations for the GLBA

I. The Importance of Federal Preemption and Harmonized Rules

[1] 15 U.S.C. § 6801 et seq.

A. Creating a Uniform National Standard.

A national privacy framework must include strong federal preemption to eliminate the growing patchwork of state privacy laws. The current state-by-state approach creates confusion for consumers and imposes significant compliance burdens on businesses, particularly small businesses. A 2022 report highlighted that a fragmented privacy landscape could cost the U.S. economy $1 trillion, with $200 billion of that burden falling on small businesses[2]. Just recently, the California Privacy Protection Agency finalized its California Consumer Privacy Act ("CCPA") cyber, risk assessment, and automated decision-making technology, and insurance rulemaking which was estimated to cost businesses at least $4.8 billion over 10 years with small businesses incurring annual costs of $16,377.[3]

Without federal preemption, businesses are forced to navigate conflicting state laws, which increases litigation risks and compliance costs. This complexity disproportionately impacts small businesses, which often lack the resources to manage multiple regulatory regimes. The Chambers *Empowering Small Business: The Impact of Technology on U.S. Small Business Report, highlights* that 65% of small businesses are "worried that having to comply with different state laws on privacy, AI, and technology in states where I am not headquartered will expose me to higher compliance and litigation costs.[4]"

Only through a fully preemptive federal privacy law can Congress provide needed clarity and consistency, enabling businesses to focus on innovation and growth while ensuring robust consumer protections.

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 merely proposing to preempt what was "*covered by* "the national privacy law.

To provide the strongest preemption, as noted by a Congressional Research Service report, Congress should use stronger language than "covering" or "covered by" in order to achieve the goal of ending a patchwork.[5] According to the Supreme

---

[2] 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/.

[3] *See* Economic Impact Assessment for CCPA Updates, Cyber, Risk, ADMT and Insurance (2025) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_eis.pdf.

[4] **U.S. Chamber of Commerce.** *Empowering Small Business: The Impact of Technology on U.S. Small Business. 2025*, **U.S. Chamber of Commerce, 2025.** https://www.uschamber.com/assets/documents/20251621-CTEC-Empowering-Small-Business-Report-2025-v1-r10-Digital-FINAL.pdf

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

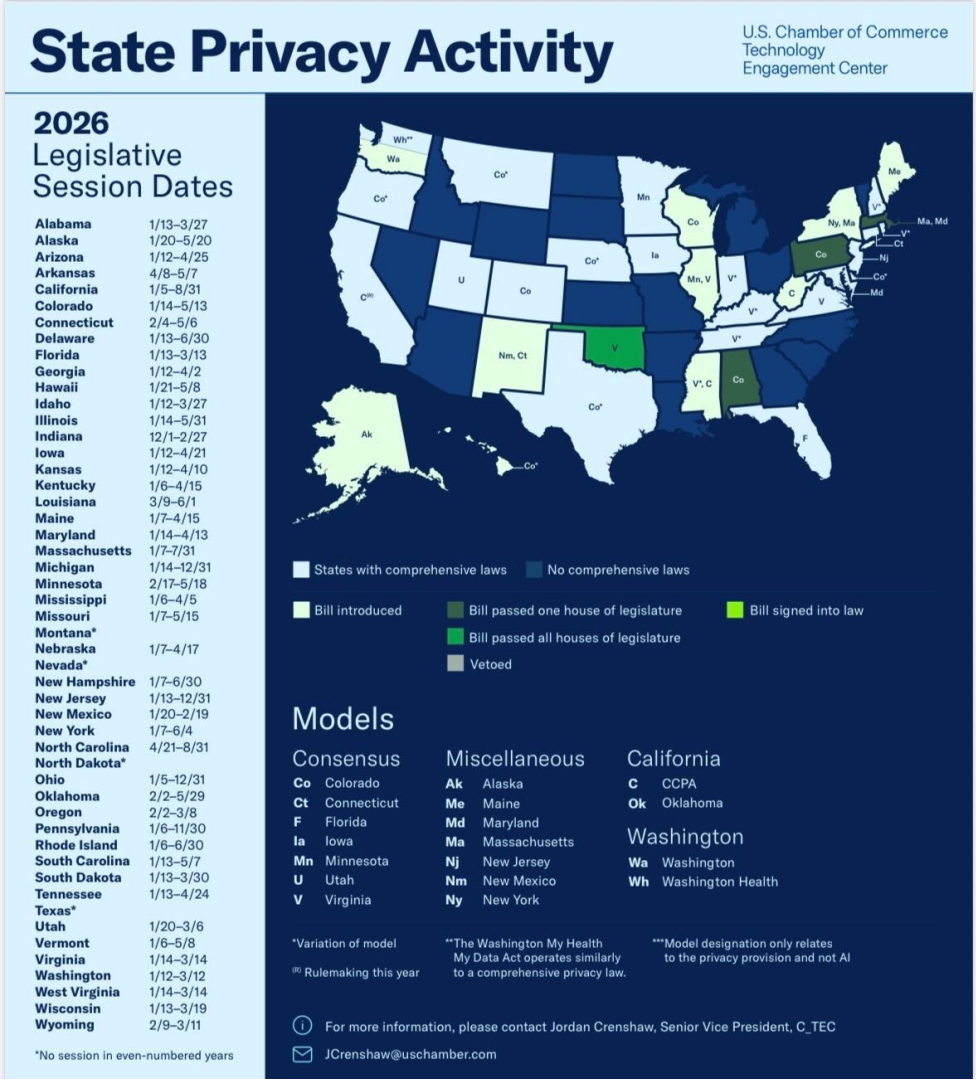
Court, "'Covering' is a more restrictive term which indicates that preemption will lie only if the federal regulations substantially subsume the subject matter of the relevant state law."[6] Under a "covered by" approach, Congress would have to insert in a national privacy law all the obligations and 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.

B. Harmonization and Interoperability

Updates to GLBA and any future national privacy legislation should avoid duplicative regulations and promote harmonization. The Chamber strongly supports a federal privacy law modeled upon the bipartisan Consensus Privacy Approach which has emerged within seventeen states, including Kentucky, Texas, Iowa, Colorado, Florida, Tennessee and Nebraska. This approach has already given over 100 million Americans consistent and reasonable data protections.[7] The Consensus Privacy Approach has data protections like the right to access, delete, and correct.

Under this Consensus Privacy Approach, *entities* regulated under GLBA are exempt which contrasts with the approach taken by CCPA which undermines clarity by only exempting *data* collected and use by GLBA-regulated entities.[8] Congress should avoid the approach taken by CCPA which threatens to create multiple layers of privacy regulation for the financial services industry. Any updates to GLBA and potential comprehensive privacy legislation should respect the Fair Credit Reporting Act ("FCRA") which also has protected consumers for over half a century. Federal policy should seek to impose one set of rules on regulated entities—not a patchwork of state and federal regulations.

[6] CSX Transportation, Inc. v. Easterwood, 507 U.S. 663 (1993.)
[7] 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.
[8] Cal Civ. Code §1798.145(e).



II. Appropriate State and Federal Regulators Should Enforce Privacy Laws

Effective enforcement of a national privacy law is critical to protecting consumers and ensuring compliance. The Chamber supports enforcement authority being vested in appropriate federal agencies and state attorneys general. For example, GLBA-regulated entities should be under the jurisdiction of their appropriate banking and financial regulators. Other entities, regulated by a general consumer privacy law, should be under the jurisdiction of the Federal Trade Commission. These entities have the expertise and resources to enforce privacy laws effectively while maintaining a balanced approach that encourages compliance and innovation.

However, the Chamber strongly opposes the inclusion in privacy laws of private rights of action. Private rights of action have historically led to abusive litigation, with plaintiffs' attorneys benefiting disproportionately from settlements while providing little relief to consumers. Such litigation diverts resources away from

compliance and innovation, forcing businesses to focus on defending frivolous lawsuits rather than protecting consumer privacy. Private rights of action codified in statutes also incentive novel theories of law to pursue claims for activities that are routine and do not cause harm. For example, in recent years, plaintiffs' attorneys have looked to expand state wiretapping statutes, which were written to address telephone eavesdropping[9], to bring lawsuits against U.S. companies for routine and widely accepted online practices, including the use of cookies and other standard web analytics tools. These claims assert that long-standing technologies used to understand website performance, improve user experience, and support basic digital operations amount to unlawful "interception" under state wiretap laws[10]. There have been over 4000 of these types of suits filed nationwide, with over 240 being filed against financial services firms.

Private rights of action also create inconsistent enforcement, as individual judicial districts may interpret privacy laws differently. This inconsistency undermines the goal of a uniform national standard and increases uncertainty for businesses. Instead, enforcement should remain with expert regulators who can provide consistent guidance and ensure that privacy laws are applied fairly and effectively.

III. Congress Must Encourage Societally Beneficial Uses of Data

Data is a cornerstone of the modern economy and plays a critical role in addressing societal challenges. From improving public safety and healthcare to enabling financial inclusion and combating fraud, data-driven technologies have transformed how we solve complex problems.[11]

A. Data Minimization

Data minimization is critical to safeguarding consumer privacy and security. 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 Kentucky, Tennessee, Nebraska, Florida and Texas mandate companies limit data collection to what is "adequate, relevant, and reasonably necessary" related to a *disclosed* purpose.[12] By contrast, states like Maryland have enacted stricter data minimization requirements that only allow the collection or processing of data for "what is necessary and proportionate to provide or

---

[9] See Amicus of U.S. Chamber of Commerce, Guiterez v. Converse (C.D. Cal January 22, 2025) *available at* https://www.uschamber.com/assets/documents/U.S.-Chamber-Coalition-Amicus-Brief-Gutierrez-v.- Converse-Inc.-Ninth-Circuit.pdf.

[10] Fisher Phillips. *Digital Wiretapping Litigation Map.* Fisher Phillips LLP, 31 May 2022, https://www.fisherphillips.com/en/resources-and-innovation/trackers-and-maps/wiretapping-litigation-map.

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

[12] Tenn. Code Ann § 47-18-3208(a)(1); Tex. Bus. & Com. Code Ann § 541.101(1) (emphasis added).

maintain a specific product or service requested by the consumer to whom the data pertains."[13] Congress should avoid the approach taken by Maryland which further imposes a restriction that prohibits the collection or processing of sensitive data - even with consent - unless it "is strictly necessary to provide or maintain a specific product or service..."[14]

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 crime.[15]

Finally, strict data minimization standards conflict with other regulations in states. For example, Colorado's new AI law, which deems financial services as a "consequential decision[16]" and 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.[17] 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. Necessary Exceptions

Although a reasonable data minimization standard is necessary to promote innovation, states adopting the Consensus Privacy Approach have also provided explicit exceptions for data processing already being undertaken. For example, the Virginia Consumer Data Protection Act (VCDPA) excempts data regulated under FCRA and the Drivers Privacy Protection Act.[18] Additionally, the VCDPA explicitly exempts data used for[19]:

- Compliance with federal, state, or local laws;
- Compliance with legal investigations;
- Cooperating with law enforcement;
- Investigating and defend against legal claims;
- Providing a product or service;
- Protecting against threats to physical safety and protect life;

[13] Md. Code Ann. Comm. Law § 14-4606(B)(1)
[14] Id. at § 1404607(A)(1).
[15] *Supra* n. 9.
[16] **Colorado General Assembly.** *Senate Bill 24-205*. **Colorado General Assembly, 2024.** https://leg.colorado.gov/bill_files/47770/download
[17] **Colorado General Assembly.** *Senate Bill 24-205*. **Colorado General Assembly, 2024.** https://leg.colorado.gov/bill_files/47770/download.
[18] Va. Code Ann §
[19] *Id.* At § 59.1-582.

- Preventing, detecting, and protecting against security incidents and illegal activitiy; and
- Engage in research.

IV. Additional Considerations for Updating the GLBA

As Congress considers updating GLBA, the Chamber offers recommendations regarding issues like the definitions of “non-public personal information,” the consumer and customer relationship, and “financial institutions,” as well as consent mechanisms, mandated deletion, disclosure, and liability.

A. Definition of Non-Public Personal Information

The definition of "non-public personal information" in the GLBA context should remain as it is currently defined. However, "publicly available data" should be explicitly defined to include both data contained in publicly available records and other data reasonably believed to be accessible to the public. Additionally, data that has been de-identified should not be subject to the new law. The definition of de-identified data should apply to any data that does not identify or is not associated with an individual and could not reasonably be used to identify an individual.

B. Definitions of Consumer and Customer Relationship

The GLBA’s current distinctions between when an individual is a consumer and when a customer relationship is formed are appropriate and should be maintained. These distinctions provide clarity and ensure that obligations are applied correctly based on the nature of the relationship.

C. Definition of Financial Institution

The current definition of "financial institution" under the GLBA sufficiently covers entities that should be subject to Title V requirements. Expanding this definition to include additional entities, such as data aggregators, could create regulatory overlap with a new general data privacy and protection law. Careful consideration is needed to avoid unnecessary complexity and duplication.

D. Consent for Collecting Certain Data Types

Financial institutions should not be required to obtain consent for the collection and use of information that is reasonably necessary to provide a financial product or service or for other important purposes, such as fraud prevention. Data elements like PIN numbers, IP addresses, and other similar information are essential for fraud prevention and information security purposes and are already protected by existing information security standards.

E. Mandated Deletion of Inactive Account Data

Mandating the deletion of data for accounts inactive for over a year, even with customer notification, is impractical for regulated financial institutions. Many institutions are subject to prescriptive record retention requirements that make such

mandates infeasible. For example, life insurers often retain data for longer periods due to regulatory obligations, and this data has proven beneficial to customers in certain cases. Any such provision should consider exemptions for specific industries and align with existing state and federal requirements.

F. Disclosure of Entities Receiving Consumer Data

Requiring financial institutions to provide consumers with a list of entities receiving their data would be impractical and could raise significant security risks. Financial institutions often work with hundreds of service providers, and these relationships frequently change. Providing a list of entities would not only be burdensome but could also expose service providers to coordinated attacks. Instead, disclosing categories of service providers, as is common in many state laws, is a more practical and secure approach.

V. Conclusion

In conclusion, the U.S. Chamber of Commerce urges Congress to modernize GLBA in a manner that provides regulatory certainty and to adopt broader comprehensive privacy legislation. Both efforts should:

- Include strong federal preemption to eliminate the patchwork of state laws and provide a uniform standard for businesses and consumers.
- Vest enforcement authority with appropriate Federal and state agencies while avoiding private rights of action that lead to abusive litigation and inconsistent enforcement.
- Strike a balance on data minimization to protect privacy while enabling the beneficial uses of data that drive innovation and address societal challenges.

By addressing these priorities, Congress can ensure that the United States remains a global leader in innovation, economic growth, and consumer protection.

Thank you for the opportunity to testify today. I look forward to answering your questions and working with the Committee to advance these important goals.

Sincerely,

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