Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

April 8, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable John Joyce, M.D.
Vice Chairman
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Re: Privacy Working Group – Request for Information

Dear Chairman Guthrie and Vice Chairman Joyce,

These comments are submitted on behalf of Business Roundtable, an association of more than 200 chief executive officers (CEOs) of America's leading companies, representing every sector of the U.S. economy. Business Roundtable CEOs lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. GDP. Our companies—from technology, communications, retail, financial services, health, public safety and security, manufacturing, hospitality, insurance, and others—rely on data and data-driven processes and solutions every day to deliver, improve and market innovative products and services across the United States and around the world. Consumer trust and confidence are essential elements of our businesses and our relationships with our customers. Consistent with consumer expectations, our companies already undertake significant efforts to be responsible about the collection, use, and sharing of consumer data and to protect the security of such data.

Introduction

Business Roundtable strongly supports the establishment of a comprehensive, fully preemptive federal privacy framework that would foster innovation and competitiveness while championing consumer privacy and promoting accountability. Consumers' digital lives and experiences are not restricted by state boundaries. A preemptive national consumer privacy law would strengthen protections for consumers across the country, while providing consistency and understanding of consumer rights, regardless of where consumers reside. At the same time, such a law would reduce the uncertainty and compliance burden faced by companies under the current patchwork of state laws – thereby enabling greater innovation. Consumers and businesses alike would benefit from halting the growing trend of fragmentation and burdensome compliance.

A strong national privacy law should:

- Fully preempt any provision of a statute, regulation, rule, agreement or equivalent of a state or local government concerning the collection, processing or sharing of personal information (including biometric information) by companies;
- Not provide for a private right of action;
- Establish a consistent, uniform federal privacy framework across industry sectors that preserves existing federal sector-specific regulations in limited cases and supplants federal sectoral regulations that have not kept pace with market and technology shifts;
- Provide consumers with reasonable access to clear, understandable statements about the company's practices and policies with respect to personal information;
- Allow consumers opportunities to exert reasonable control regarding the collection, use and sharing of personal information; and
- Enable innovative and beneficial uses of data by businesses, including product improvement, fraud prevention and security.

A fully preemptive federal law should set reasonable standards that build on what works in current state laws to protect consumers, deliver economic growth and prevent outlier jurisdictions from adversely impacting the national data-driven economy. We appreciate the opportunity to respond to specific questions in the Privacy Working Group's Request for Information.

Roles and Responsibilities

Consumers and companies should be the primary stakeholders considered when drafting a fully preemptive federal law. Consumers deserve strong privacy and data security protections to safeguard their personal information, maintain trust in digital services and products, and prevent identity theft and fraud. At the same time, companies need regulatory certainty to build robust data privacy and security compliance programs aligned with responsible business practices that account for the various relationships between companies.

A federal law should mirror the prevailing approach of assigning businesses to a "controller," "processor" or "third party" role in data processing activity based principally on the nature of their relationship with the consumer and other companies. Companies should appropriately monitor their uses of personal information and when sharing personal information should be responsible for contractually imposing the compliance obligations on the third parties and processors with whom they share such information.

Congress should also consider an entity's size when crafting a federal framework. Care should be taken not to overburden small businesses, whose collection and use of personal information may be minimal or low-risk for consumers.

Personal Information, Transparency and Consumer Rights

Personal information should be defined as consumer data that is held by the company and identifies or is identifiable to a natural, individual person. This information may include but is not limited to name and other identifying information, such as government-issued identification numbers, and personal information derived from a specific device that reasonably could be used to identify a specific individual. This definition should exclude de-identified data, aggregated data, personal information used in the employment context and data in the public domain.

In addition, categories of sensitive personal information that may present increased risk should be expressly defined and subject to additional obligations and protections. Categories of increased risk should be appropriately scoped to allow companies to properly prioritize stricter controls in the cases where they are necessary. The definition of sensitive personal information should be limited to data elements that present an increased risk of actual harms to consumers and avoid overly broad classifications that stifle innovation.

Consent or other requirements for the sensitive information classification should be contextual and risk-based, taking into account the nature of both the personal information and the purpose for which sensitive information is collected, processed, or maintained. For example, leveraging non-consent bases for data processing is essential for fraud prevention; required controls should be designed contextually to facilitate consumer safety. These risk-based controls should include privacy by design throughout a product or service lifecycle and privacy impact assessments for potentially high-risk processing activities, including "sensitive information," that are based on the purposes for data processing, data security measures and risk-mitigation processes.

With regard to consumer controls, rights and transparency, consumers should have reasonable access to clear, understandable statements about the company's practices and policies with respect to personal information, including: information on the types of personal information collected; the purposes for which the personal information will be used; whether and for what purposes personal information may be disclosed or transferred to non-affiliated third parties; the choices and means for exercising individual rights with respect to personal information; and how to contact the company with questions. Statements should be in a format that is reasonable and appropriate for the point of collection and is accessible through new and emerging technologies. Transparency requirements should avoid being overly prescriptive to allow companies flexibility to provide information to consumers in a clear manner.

Consumers should also have opportunities to exert reasonable control regarding the collection, use and sharing of personal information, while preserving the ability of companies to use information for innovative and beneficial purposes. This should include the rights to access, correction and deletion of data with reasonable exceptions and controls. With regard to

deletion rights specifically, exceptions should account for circumstances where the rights of other individuals outweigh deletion, the data is required for freedom of expression and information, and when deletion is not reasonably feasible due to the manner in which the personal information is collected or maintained. Operational exceptions for use cases including security, fraud prevention and legitimate business needs such as legal obligations and product or service improvement and delivery, which are consistent with consumer expectations, are necessary. Deletion should also allow companies to use alternatives such as placing the data beyond practical use. No one specific mechanism for consumer control is suitable in all instances, and companies should be permitted flexibility in how these controls may reasonably be exercised considering the sensitivity of the personal information and the risks and context of specific data processing. In addition, Congress should avoid establishing extreme and broad data minimization standards that would lead to significant inconsistencies in how requirements are applied across businesses, harming both companies and consumers and leading to confusing and vague permitted purposes.

Existing Privacy Frameworks & Protections

Business Roundtable supports a national consumer privacy law that fully preempts any provision of a statute, regulation, rule, agreement or equivalent of a state or local government concerning the collection, processing or sharing of personal information (including biometric information) by companies.[1] Without strong preemption, a single state with highly restrictive laws can effectively dictate national policy because companies will seek to avoid unintentional non-compliance due to the borderless nature of the digital economy.

A growing number of states have enacted comprehensive data privacy and security laws, some of which have elements that have proven effective and could be replicated at the federal level. Examples of consistent elements across state laws that could be incorporated into a fully preemptive federal consumer privacy law include:

- Personal Information: Most states with consumer privacy laws address protections for consumers acting in their personal, household or individual capacity, excluding activity collected about an individual acting in their employee or commercial role.[2] Personal information is generally defined by most states as "any information that is linked or reasonably linkable to an identified or identifiable" natural person or individual.[3] States

[1] For example, preemption should be broad enough to protect the "Essential Exceptions" noted below from older privacy laws. For instance, some courts have refused to dismiss class action lawsuits brought under state wiretapping laws against banks and other organizations using fraud detection software to find bad actors who call or use system portals to steal money from customers. A preemptive federal consumer privacy standard should ensure that those legacy frameworks do not impede responsible and routine modern data processing practices that protect consumers.

[2] *See, e.g.,* Neb. Rev. Stat. § 87-1102(7); Va. Code Ann. § 59.1-575.

[3] *See, e.g.,* Conn. Gen. Stat. § 42-515 (26); N.J. Stat. Ann. § 56:8-166.4; Va. Code Ann. § 59.1-575.

also typically exclude publicly available information and de-identified information from the definition of personal information.[4]

- Transparent, Public Disclosures: Companies are required to disclose through a publicly available, understandable privacy notice how personal information is collected, processed, sold, shared or otherwise used.[5] Companies are generally allowed to process data for those purposes detailed in their public disclosures.[6]

- Consumer Rights: Consumers typically have the right to access, transfer, correct or delete their personal information subject to reasonable verification requirements and exceptions for routine business practices and operations like fraud prevention and security.[7] Companies also have a reasonable amount of time to respond to rights requests.[8]

- Opt-out Mechanisms: Consumers have access to opt-out mechanisms for the sale of personal information to third parties, profiling with significant legal effects, and targeted advertising that do not unfairly disadvantage responsible companies and take into account the context of the consumer's interaction with a business and appropriate transparency.[9]

- Essential Exceptions: Most states with privacy laws recognize essential exceptions, including those that allow companies to engage in vital activity that prevents, detects, protects against, and responds to security incidents, fraud and criminal activity.[10] This practical approach allows companies to implement necessary actions designed to prevent data security breaches, fraud and other illegal activity without compromising privacy standards.

While the examples above show consistent elements across many jurisdictions, in practice these regimes have nuanced differences. Businesses are increasingly facing significant challenges navigating a fragmented state-by-state data security and privacy landscape, leading to increased costs and complexities to manage compliance. For instance, initial compliance costs for the California Consumer Privacy Act (CCPA) alone were estimated to be $55 billion for California firms.[11] This example is not an outlier, and additional studies confirm the substantial costs associated with divergent state privacy legislation. One report estimated that state

[4] *See e.g.,* Cal. Civ. Code §§ 1798.140 (v)(2)-(3); Tex. Bus. & Com. Code § 541.001(19); Va. Code Ann. § 59.1-575.
[5] *See, e.g.,* Or. Rev. Stat. § 646A.578 (4); Colo. Rev. Stat. § 6-1-1308 (1).
[6] *See, e.g.,* Va. Code Ann. § 59.1-578 (A)(1); N.H. Rev. Stat. Ann. § 507-H:6 (I)(a).
[7] *See, e.g.,* Fla. Stat. § 501.705 (2); N.J. Stat. Ann. § 56:8-166.10 (a).
[8] *See, e.g.,* Neb. Rev. Stat. §87-1108(2) Tex. Bus. & Com. Code § 541.052(b).
[9] *See, e.g.,* Ky. HB 15, §§ 3(2)(e), 4(3)(c); Va. Code Ann. §§ 59.1-577(A)(5), 59.1-578(C)(3).
[10] *See, e.g.,* Cal. Civ. Code § 1798.105 (d); Tex. Bus. & Com. Code § 541.201(a)(6).
[11] *See* State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019), located here.

privacy laws could impose out-of-state costs exceeding $1 trillion over a decade if a 50+ jurisdiction patchwork were to develop.[12] As more states enact their own version of novel consumer privacy legislation including terms related to artificial intelligence (AI), the costs are likely to increase further.[13]

In regard to the existing federal sectoral privacy laws, a comprehensive consumer privacy law should establish a harmonized framework that avoids duplication and confusion. In some cases existing sectoral privacy laws are highly effective and should remain in place. For example, Congress should exempt Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates from comprehensive federal privacy law and extend similar exemptions for research purposes as commonly exists under state privacy laws. Additionally, Congress should avoid disrupting the strong existing protections in the financial sector under the Gramm-Leach-Bliley Act (GLBA) and other current laws. However, in cases where existing sectoral law does not include appropriate provisions that reflect activity in the current marketplace, and where it will create overlapping or duplicative requirements, Congress should harmonize sectoral laws with the new framework to update privacy regimes in alignment with current market and technology landscapes. In particular, the law should establish a consistent privacy regime for the online ecosystem and eliminate disparate treatment of companies based on their legacy regulatory classification under certain existing laws.

Data Security

Federal legislation should not prescribe or otherwise require specific safeguards, tools, strategies or tactics. Rather, companies should have the flexibility to develop a risk-based approach and tailor their data security measures to best fit their unique operational needs, the specific risks they face, and the type and sensitivity of data, leveraging generally accepted industry standards as a foundation. Congress should look to existing state approaches[14] as well as National Institute of Standards and Technology guidance for language that facilitates a flexible, risk-based approach to data security controls. Encouraging innovation and adaptability in security practices will also allow companies to stay ahead of emerging threats and protect personal information more effectively. This balance between data protection and flexibility is important to enhance data security for consumers without stifling business growth and innovation.

Artificial Intelligence

State regulation of "automated decision making" should also be preempted to allow for a consistent national framework of AI-specific requirements that allows American leadership and

[12] Daniel Castro, Luke Dascoli, and Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws* (Jan. 24, 2022), available here.
[13] *Id.*
[14] Va. Code Ann. § 59.1-578 (A)(3)

innovation to drive AI's future. In today's global economy, American companies need to leverage AI and other similar technologies to deliver products and services, run day-to-day operations, and personalize offerings to fit customers' needs. A comprehensive, preemptive federal data privacy law should protect consumer data rights regardless of technology. This will further encourage the growth of the American AI industry without ceding ground to international competitors. A fully preemptive federal consumer data privacy law should also align with existing, effective domestic policies and industry risk management strategies to promote a harmonized approach and avoid introducing uncertainty and conflicting compliance requirements.[15]

Accountability & Enforcement

Empowering a single agency, such as the Federal Trade Commission (FTC)[16], to enforce a preemptive consumer privacy law would allow the creation of a body of consistent enforcement actions. This consistency will provide guidance and predictability to help companies understand enforcement priorities and afford consumers with equal rights across the country. In addition, State attorneys general may bring an action in federal court on behalf of their state's residents but should be required to coordinate with the FTC. The law should also bar duplicative actions arising from the same conduct to avoid uncertainty and the potential for differential enforcement to enter a preemptive regime. This enforcement approach would allow businesses to focus their resources on compliance with the law and protecting consumer rights, rather than defending against private litigation.

In the case of particular sectors outlined in the *Existing Privacy Frameworks and Protections* section above and as appropriate—specifically, entities regulated under HIPAA and GLBA—existing enforcement authorities and structures should be preserved.

While Business Roundtable believes the FTC has an important role to play enforcing a national consumer data privacy framework, clear direction and a long-term foundation for its rulemaking and enforcement responsibilities should be provided to the agency as part of legislation. For example, companies should only be required to submit assessments to the FTC or to Congress if there is cause to believe that a violation of the law has occurred, consistent with Business Roundtable's recommendation to policymakers that enforcement standards should be adaptive, clear, targeted and well-calibrated.

Business Roundtable does not support a private right of action in a national consumer privacy law, just as no comprehensive state consumer privacy law has included a broad private right of

[15] Business Roundtable, Artificial Intelligence Policy Recommendations available here.
[16] The FTC is the appropriate federal agency to enforce a national consumer privacy law, unless a determination is made that it is appropriate for a different regulator to be the enforcement agency. Care should be taken to avoid duplication of enforcement across federal agencies.

action.[17] Consumer privacy rights are better served by regulatory enforcement, with the ability for businesses to remedy and cure privacy deficiencies. A private right of action and the associated penalties for violations create an excessively punitive framework that fails to address consumer privacy concerns or deter undesirable business practices effectively. Further, a private right of action would also hinder companies' efforts to innovate by exposing them to costly, unpredictable and often frivolous litigation. Enforcement and fines related to violations of data privacy law should be informed by the actual harm directly caused by, and severity of, a company's conduct as well as any actions taken by the company to avoid and mitigate the harm, the degree of intentionality or negligence involved, the degree of cooperation and the company's previous conduct involving personal information privacy and security.

Finally, a national consumer privacy law should encourage the development and use of voluntary codes of conduct and assessment bodies by industry self-regulatory groups to aid in compliance and drive consistent approaches in the marketplace to help both consumers and companies. If a code receives approval from an appropriate federal agency and a company's compliance with such code is validated by third party or independent assessments, the company should be presumed to be in compliance with the law for the covered activity.

Conclusion

Business Roundtable shares the Privacy Working Group's goal of establishing a national privacy framework to protect consumers and support companies in providing services and products.

We urge Congress to forge a path forward to address these important issues through comprehensive, fully preemptive federal legislation. The current state-by-state patchwork has not only driven up compliance costs but has also diverted valuable resources away from innovation, economic growth and the United States' leadership role in the data-driven economy. Federal legislation will provide the clarity and stability needed for companies to thrive, fostering an environment where companies can innovate with confidence while protecting consumers.

Business Roundtable appreciates the opportunity to provide our input during this process. For any questions, please contact Amy Shuart, Vice President, Technology and Innovation at Business Roundtable at ashuart@brt.org or (202) 496-3290.

C: Members of the Privacy Working Group

[17] The CCPA's private right of action is limited to certain data security breach occurrences, and Washington's My Health My Data Act's private right of action is not part of a comprehensive consumer privacy law. Cal. Civ Code § 1798.105; Wash. Rev. Code § 19.373.090.