BR Business Roundtable

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

June 22, 2022

The Honorable Jan Schakowsky
Chairwoman
Subcomm. on Consumer Protection & Commerce
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Gus Bilirakis
Ranking Member
Subcomm. on Consumer Protection & Commerce
Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

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

The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

Dear Chairwoman Schakowsky, Ranking Member Bilirakis, Chairman Pallone, and Ranking Member McMorris Rodgers:

On behalf of Business Roundtable, thank you for the opportunity to submit feedback ahead of the subcommittee's markup of the American Data Privacy and Protection Act ("ADPPA"). Since 2018, Business Roundtable has consistently called for a federal consumer data privacy law that will protect and empower consumers and provide clear obligations for how companies handle personal data, while fostering American innovation and global competitiveness.

Business Roundtable is an association of chief executive officers of America's leading companies. Business Roundtable member companies operate across all sectors of the domestic and global economy, employ 20 million people, and reach virtually every American consumer. 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, such as digital platforms, every day to deliver and improve innovative products and services across the U.S. and around the world. Consumer trust and confidence are essential elements of our businesses and our relationship with our customers.

A national data privacy framework with clear, consistent requirements to strengthen consumer trust and enable new services and technologies to flourish within a well-understood legal and regulatory structure is critically needed. We appreciate your leadership and your focus on moving towards a bipartisan consensus on comprehensive privacy legislation to accomplish this shared goal. While our members support many aspects of the ADPPA, we have concerns with some of the provisions and look forward to engaging constructively around these issues as discussions progress.

To provide a detailed guide for addressing key issues integral to an effective federal data privacy law, Business Roundtable released in 2018 a *Framework for Consumer Privacy Legislation* which includes the creation of robust protections for consumers by requiring businesses to take responsibility for the

collection, use and sharing of personal information, regardless of jurisdiction. Our privacy framework also includes sections on enforcement, data security and breach notification, governance, risk-based privacy practices and covered organizations, and the effect on other laws.

Business Roundtable also supports strong personal data rights for consumers, including transparency, control, access, correction, and deletion, with application and enforcement in a consistent manner across federal and state governments to provide accountability and protection. However, we have serious concerns about the inclusion of a private right of action. Federal privacy legislation should avoid putting into place an enforcement system that encourages excessive and frivolous litigation that diverts company resources away from actual security and privacy compliance while providing little relief to actual victims.

A national consumer privacy law should be strong and provide consistent protections to consumers across every state in the country. U.S. privacy laws are highly fragmented across industries and jurisdictions, creating a patchwork of regulations, which hurts both consumers and companies. Business Roundtable supports total preemption of state and local privacy laws, including those already enacted. State exceptions and carve outs to a federal privacy framework would lead to inconsistent protections for consumers, disjointed user experiences, and an unworkable compliance structure for companies of all sizes. Federal privacy legislation should preclude these challenges by standardizing protections nationwide while also promoting global interoperability to meet the adequacy standards of our major trading partners. As a result, we are concerned that the ADPPA draft includes too many exceptions to preemption, undermining the scope and effectiveness of a national framework. We will engage the Committee on recommended changes.

Business Roundtable is also troubled by provisions in the bill that include overly broad definitions, which could lead to interpretations that differ from legislative intent with unintended consequences for American consumers and businesses. For example, the term "algorithm" is defined so broadly that it would encompass virtually any decision that involves modern workplace technology. ADPPA's language regarding the "algorithmic impact assessment" requirement is also broad and unspecific. The language as currently written could be understood to require assessments of an extraordinary range of data processing activities. Business Roundtable and its members support approaches to regulation and assessments that are contextual, proportional, risk-based and use-case specific, in line with global policy and standards taking shape, and consistent with the recommendations outlined in our *Policy Recommendations for Responsible Artificial Intelligence*. We welcome an opportunity to further refine these key terms.

While Business Roundtable believes the Federal Trade Commission ("FTC") has an important role to play enforcing a national consumer data privacy framework, we urge the Committee to provide clear direction to the agency and a long-term foundation for its rulemaking and enforcement responsibilities. For example, the bill should not automatically require assessments to be provided to the FTC or to Congress. The bill should require assessments be only provided to the relevant authorities 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.

Finally, we are concerned that additional reporting requirements like executive officer certification would create burdensome obligations on companies while doing little to add to consumer protection or increase privacy security.

Given the importance of this issue and its potential impact on the innovation economy, Business Roundtable encourages a thorough legislative review and the incorporation of additional stakeholder engagement. We look forward to working with you and your staff to ensure that any final product enhances consumer data privacy protections and provides the certainty American businesses need to compete and remain at the forefront of global innovation.

Sincerely,

Kristen Silverberg
President & Chief Operating Officer
Business Roundtable

Attachments:

BRT Framework for Consumer Privacy Legislation
BRT Policy Recommendations for Responsible Artificial Intelligence

Business Roundtable

Business Roundtable Policy Recommendations for Responsible Artificial Intelligence

U.S. leadership in artificial intelligence (AI) innovation strengthens all sectors of the U.S. economy. AI is actively improving the lives of individuals through better functioning of businesses, government and civil society. Trust fuels the healthy adoption of AI, and the responsibility for furthering this trust is shared by industry and government. Businesses developing and using AI technologies should align their internal practices and governance to key principles of Responsible AI, while regulators and policymakers should account for the complex, context-dependent and rapidly evolving AI ecosystem.

From development to deployment to end-user engagement, Business Roundtable is committed to working with regulators and policymakers to ensure that AI governance and regulation build trust in and acceptance of AI, enable innovation and promote continued U.S. leadership. Accordingly, Business Roundtable calls on the Administration, Congress and regulators to establish practices, rules and guidelines consistent with 10 policy recommendations:

1. Adopt regulatory approaches to AI that are contextual, proportional and use-case specific.
2. Embed AI rules and guidelines into existing frameworks, as appropriate.
3. Employ an agile and collaborative approach to AI governance.
4. Adopt an adaptive approach to enforcement.
5. Calibrate targeted and clear enforcement standards.
6. Prioritize strategic international engagement on AI issues.
7. Engage on global AI standards and guidelines.
8. Strive for common principles and interoperability.
9. Invest in AI education and proficiency at all levels.
10. Support industry training and reskilling efforts.

Targeted and Flexible Governance

Encourage AI innovation through targeted and flexible governance and oversight.

1. Adopt regulatory approaches to AI that are contextual, proportional and use-case specific.

- Tailor standards, guidance and regulation to specific AI use cases within well-defined deployment contexts and/or industries, rather than broadly regulating any technology or application outright.
- Direct governance efforts to consider the benefits and risks of AI relative to alternatives.

2. Embed AI rules and guidelines into existing frameworks, as appropriate.

- Assess regulatory gaps before considering new regulations. If new rules or guidance are necessary, narrowly scope the new rules or guidance to address the gaps. Where appropriate, seek to apply, extend or update existing frameworks or rules.
- Design any new rules to be interoperable with industry regulations, laws and technology standards (see, for example, cybersecurity and **Business Roundtable's *Framework for Consumer Privacy Legislation***).
- Empower agencies with relevant expertise to clarify existing standards and address inconsistencies across industries.

3. Employ an agile and collaborative approach to AI governance.

- Adopt an incremental approach to regulating AI, acknowledging that technical standards, use cases and private-sector governance evolve over time.
- Use evidence-based regulatory approaches and tools that allow for the iteration of governance practices (e.g., sandboxes, safe harbors) and opportunities for industry to discover and share best practices.
- Incentivize industry to engage in self-assessments.

Transparent and Rational Enforcement

Account for the evolving and differentiated nature of AI, focusing enforcement efforts on bad actors.

4. Adopt an adaptive approach to enforcement.

- Craft governance mechanisms that incentivize good-faith and demonstrated efforts to adhere to requirements, norms and standards.
- Engage with leadership from industry, academia and community organizations to inform AI best practices and enforcement mechanisms, recognizing substantive differences within and across industries.

5. Calibrate targeted and clear enforcement standards.

- Specify which entities, uses and/or impacts along the AI supply chain are subject to regulatory oversight.
- Issue guidance on the applicability of existing regulations to specific AI use cases and deployment contexts.
- Hone effective, proportional and clearly articulated enforcement standards that focus on bad actors and reflect the contextual and evolving nature of AI and its uses.

Global Coordination on Key Issues

Participate in global dialogues to support common principles and understanding of AI.

6. Prioritize strategic international engagement on AI issues.

- Develop U.S. government strategy for AI that can be consistently advanced in bilateral and multilateral consultations and negotiations.

7. Engage on global AI standards and guidelines.

- Prioritize U.S. participation in global standards-setting bodies and regulatory forums, working closely with private-sector stakeholders.
- Develop international guidelines for cyber, data/model and system-level security best practices that address unique AI vulnerabilities.

8. Strive for common principles and interoperability.

- Promote alignment of common principles for a targeted and flexible governance approach across the global AI regulatory landscape to minimize conflicting requirements and promote innovation, trade and investment.
- Leverage existing U.S. agency frameworks and guidance in international regulatory cooperation and standards-setting.
- Focus efforts on aligning key definitions (e.g., AI, explainability, classifications of risk) and promoting interoperability.
- Support digital trade frameworks and confront data localization requirements that impair cross-border data flows and the collection of fully representative training data.

AI Education, Training and Awareness

Partner with industry to build AI literacy and relevant skill sets across the United States.

9. Invest in AI education and proficiency at all levels.

- Support AI education at academic and trade institutions to broaden AI knowledge and prepare students for AI-compatible roles in the 21st century workforce.
- Develop early education curricula and consumer literacy programs.
- Make AI educational resources and training programs widely accessible across geographic areas and socio-economic backgrounds.

10. Support industry training and reskilling efforts.

- Support multisectoral partnerships among education institutions, industry and government entities to promote applied AI learning and apprenticeships.
- Enhance technical AI capacity within and across federal agencies by expanding investments in talent recruitment and modernizing government information technology.
- Augment private-sector investments in employee training, reskilling and upskilling to fully realize the benefits of widespread AI integration.

FRAMEWORK FOR CONSUMER PRIVACY LEGISLATION

OBJECTIVES

This framework is a call to action: The United States should adopt a national privacy law that protects consumers by expanding their current rights and fosters U.S. competitiveness and innovation. The time to act is now.

A national consumer privacy law should:

- **Champion Consumer Privacy and Promote Accountability.**
  It should include robust protections for personal data that enhance consumer trust and demonstrate U.S. leadership as a champion for privacy by including clear and comprehensive obligations regarding the collection, use, and sharing of personal data, and accountability measures to ensure that those obligations are met.

- **Foster Innovation and Competitiveness.**
  It should be technology neutral and take a principles-based approach in order for organizations to adopt privacy protections that are appropriate to specific risks as well as provide for continued innovation and economic competitiveness in a dynamic and constantly evolving technology landscape.

- **Harmonize Regulations.**
  It should eliminate fragmentation of regulation in the United States by harmonizing approaches to consumer privacy across federal and state jurisdictions through a comprehensive national standard that ensures consistent privacy protections and avoids a state-by-state approach to regulating consumer privacy.

- **Achieve Global Interoperability.**
  It should facilitate international transfers of personal data and electronic commerce and promote consumer privacy regimes that are interoperable, meaning it should support consumer privacy while also respecting and bridging differences between U.S. and foreign privacy regimes.

FRAMEWORK

1. Covered Organizations and Effect On Other Laws.

A. A national consumer privacy law should apply a consistent, uniform framework to the collection, use, and sharing of personal data across industry sectors. In order to advance a comprehensive approach, it may be appropriate to harmonize certain sector-specific regulations in order to bring those standards in-line with a national privacy law so that consumers are not disserved by multiple and conflicting standards over personal data, which undermine consumer expectations and trust.

B. Care should be given to how or if small companies that do not process much personal data or engage in low risk processing of data should be covered, with consideration of how those companies may be covered under existing law.

C. A national consumer privacy law should not interfere with government or law enforcement activities with regard to personal data.

D. A national consumer privacy law should pre-empt any provision of a statute, regulation, rule, agreement, or equivalent of a state or local government for organizations with respect to the collection, use, or sharing of personal data.

2. Definition of Personal Data.

A. Personal data should be defined as consumer data that is held by the organization 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.

B. Personal data should exclude de-identified data and data in the public domain.[1]

C. Categories of sensitive personal data that may present increased risk should be defined and subject to additional obligations and protections.

3. Risk-Based Privacy Practices.

Organizations should employ risk-based privacy practices that apply greater protections to data processing that may present higher risks to the rights and interests of consumers and to address emerging risks as business practices and technologies evolve. Specific risk-based practices should not be prescribed by regulation or otherwise required; rather, organizations should have flexibility in how they leverage risk-based privacy practices. Risk-based privacy practices can include:

A. Assessing and balancing the interests in and benefits of the processing to organizations, individuals, and society against the potential risks and applying appropriate mitigations.

B. Implementing privacy by design and taking privacy risks into account starting from the design phase of a proposed data processing activity and continuing throughout the entire life-cycle of that processing.

C. Conducting privacy impact assessments where high-risk data processing activity is involved, and applying greater protections, such as de-identifying techniques, data minimization, or encryption, to those activities.

[1] *There should be limitations to this exclusion; certain data within the public domain is properly considered personal data.*

4. Individual Rights.

Organizations should recognize and facilitate the following individual rights of consumers with regard to personal data.[2] Facilitation of these rights may be limited where required by law,[3] and should be informed by the legitimate interests of the organization, which may include protecting the health and safety of individuals, preventing fraud and addressing security risks, supporting legitimate scientific and research purposes, and satisfying business (including contractual) obligations.

A. **Transparency:** Consumers should have reasonable access to clear, understandable statements about the organization's practices and policies with respect to personal data, including: information on the types of personal data collected; the purposes for which the personal data will be used; whether and for what purposes personal data may be disclosed or transferred to non-affiliated third parties; the choices and means for exercising individual rights with respect to personal data; and the contact details of persons in the organization who can respond to questions regarding personal data. Statements should be in a format that is reasonable and appropriate for the point of collection and is accessible through new and emerging technologies.

B. **Consumer Control:** Consumers should have opportunities to exert reasonable control with regard to the collection, use, and sharing of personal data. No one specific mechanism for consumer control is suitable in all instances, and organizations should be permitted flexibility in how these controls may reasonably be exercised in light of the sensitivity of the personal data, as well as the risks and context of the specific data processing and sharing with non-affiliated third parties. Where organizations rely upon "consent" to collect and use personal data, the type of consent required should be contextual, taking into account the nature of both the personal data and its proposed uses.[4]

    i. Consumers should also have the opportunity to make choices with respect to the sale of personal data to non-affiliated third parties.

    ii. Consumers should understand under what circumstances their decision to opt-out (or not opt-in) may result in the organization no longer providing them certain goods and services (for example, free content).

    iii. Organizations should be obligated to inform its service providers of the choices made by consumers with respect to the processing of personal data. The service provider would be responsible for protecting the personal data from improper processing throughout the data life-cycle, but should not be expected to provide transparency or control directly to consumers.

C. **Access and Correction:** Consumers should have a reasonable right to access and correct any inaccuracies in personal data collected about them by an organization, taking into account security and operational considerations.

---

[2] *In addition to these rights, special protections should be applied to personal data of children.*

[3] *Such legal obligations may include, for example, adherence to Know Your Customer (KYC) and Anti-Money Laundering (AML) laws.*

[4] *For example, opt-in consent may be required as part of a risk-based privacy practice for data processing that presents higher risks to the rights and interests of individuals. In addition, where not previously disclosed, organizations should provide consumers with clear mechanisms to control whether an organization can use or further share the personal data they have already collected from them if they intend to use that personal data for a new purpose that is not compatible with the purpose described in the previous disclosure.*

D. **Deletion:** Consumers should be able to require an organization to delete their personal data collected by an organization, when such data is no longer required to be maintained under applicable law or is no longer necessary for legitimate business purposes of the organization. Organizations may limit a consumer's right to delete in circumstances where the rights of other individuals outweigh deletion, or the data is required for freedom of expression and information. Deletion should not be required where disposal is not reasonably feasible due to the manner in which the personal data is maintained and alternatives such as placing the data beyond practical use are available.

5. Governance.

A. **Governance:** Organizations should implement policies and procedures that reflect these principles and appropriately monitor their uses of personal data to ascertain that such uses are legitimate and consistent with their internal policies, procedures, and notices to consumers.

B. **Onward Responsibility:** Organizations that share personal data with service providers should be responsible for contractually imposing the obligations and protections associated with that personal data on such service providers.

C. **Review and Redress:** Organizations should put appropriate mechanisms in place to handle consumers' inquiries or complaints regarding the organization's personal data practices.

6. Data Security and Breach Notification.

A. Organizations should implement reasonable administrative, technical and physical safeguards designed to reasonably protect against the unauthorized access to or disclosure of personal data, or other potentially harmful misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened and the sensitivity of the personal data. Regulation should not prescribe or otherwise require specific safeguards, tools, strategies, or tactics.

B. A consumer privacy law should establish a national standard for breach notification that preempts state laws. Consumers have the right to be notified within a reasonable timeframe if there is a reasonable risk of significant harm as a result of a personal data breach.

7. Enforcement.

Consistent and coordinated enforcement across the federal government and states is needed to provide accountability and protect consumer privacy rights.

A. **FTC Enforcement:** 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. The FTC should have adequate funding and staffing to effectively enforce the consumer privacy law.

B. **State Attorneys General:** State Attorneys General (AGs) should be permitted to bring an action in federal court to enforce these requirements on behalf of their state's residents. State AGs should be required, where appropriate, to coordinate with the FTC and other federal agency authorities to avoid duplicative or conflicting enforcement actions.

C. **Enforcement Actions and Fines:** Enforcement actions and fines should be informed by the harm directly caused by, and severity of, an organization's conduct as well as any actions taken by the organization to avoid and mitigate the harm, the degree of intentionality or negligence involved, degree of cooperation, and the organization's previous conduct involving personal data privacy and security.

D. **Codes of Conduct and Assessments:** A national consumer privacy law should encourage the development and use of codes of conduct by industry groups. If a code receives approval from an appropriate federal agency, and an organization's compliance with such code is validated by third party or independent assessments, the organization should be presumed to be in compliance with the law.

E. **No Private Right of Action:** A national consumer privacy law should not provide for a private right of action.