Business Roundtable

300 New Jersey Avenue, NW, STE 800
Washington, DC 20001
202.872.1260
brt.org

May 31, 2019

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Comments of Business Roundtable
Via Regulations.gov

Re: Hearings on Competition and Consumer Privacy in the 21st Century: Consumer Privacy
Docket ID: FTC-2018-0098

Dear Mr. Clark:

On behalf of the members of the Business Roundtable, an association composed of chief executive officers of leading U.S. companies representing all sectors of the economy, I thank you for the opportunity to comment as the Federal Trade Commission (FTC) considers issues of consumer privacy.

Enhancing and sustaining consumer trust is vital for continued innovation and economic competitiveness. To achieve this, all companies that collect, use, share, or otherwise handle personal data must do so responsibly and with respect for individuals. As business leaders, we take this responsibility seriously and call for a national consumer privacy law that strengthens protections for consumers and achieves greater transparency without shortchanging innovation and growth. Business Roundtable has developed and released a legislative framework on privacy (attached) and continues to work across industries and sectors to build widespread support for a law based on the framework.

Why a National Consumer Privacy Law is so Urgently Needed

Companies rely on data to deliver products and services, conduct day-to-day operations, and deliver meaningful innovation that benefits consumers who have grown to expect increasingly data-driven and personalized products and services. Consumer trust forms the backbone of these efforts, and yet consumers have grown increasingly concerned over how some companies use and share data. Without consumer trust in how data is collected, used, stored, and shared, companies' abilities to deliver valuable user experiences, prevent fraud and cyberattacks, and enable greater productivity inevitably weaken. As a direct result of these

consumer concerns, we are now at a moment, perhaps for the first time in the United States, where there is widespread agreement among companies across all sectors of the economy on the need for a comprehensive federal consumer privacy law.

Across the world, the regulatory landscape around privacy is changing quickly. With the implementation of the European Union's General Data Protection Regulation, the enactment of new data protection laws in California and Brazil, and the development of a myriad of regulations at the state and local level and around the globe, data privacy regulations have grown more complex and fragmented. A patchwork of confusing data privacy requirements hurts consumers who deserve meaningful, understandable and consistent data privacy rights regardless of where they live or where their data may be located. Fragmentation also threatens the global digital economy by restricting the flow of data across borders. As a first step, the United States should eliminate fragmentation within its borders by establishing a comprehensive and consistent national privacy law.

To advance national consumer privacy legislation, government and the private sector must work together. Business Roundtable continues to support policymakers' efforts to advance consumer privacy, and we welcome future opportunities to work together to achieve our shared goals.

A National Consumer Privacy Law Must Champion Privacy While Facilitating Innovation

Business Roundtable believes a national consumer privacy law must advance four important objectives:

- Championing 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.

- Facilitating Innovation. It should be neutral as to technology 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.

- Harmonizing 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 helps ensure consistent privacy protections and avoids a state-by-state approach to regulating consumer privacy.

- Achieving 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.

Components of a National Consumer Privacy Law

Business Roundtable believes that these objectives can be achieved only through a national consumer privacy law that preempts state and local personal data privacy requirements. The result of increased certainty and predictability for both companies and consumers will make it easier for companies to protect consumers' personal data and materially enhance the ability of consumers to manage their privacy preferences.

To that end, Business Roundtable supports a national consumer privacy law with the following components:

Comprehensiveness and Uniformity. A national consumer privacy law should apply a consistent, uniform framework to the collection, storage, use and sharing of personal data by companies. As a threshold issue, data should be considered personal and covered by the law only if it reasonably may be deemed to identify or be identifiable to a natural, individual person. However, it is appropriate to exclude from the definition of "personal data" certain categories of information that cannot reasonably be deemed to identify a specific individual, do not relate to information collected from consumers, or are already (with certain exceptions) within the public domain. In addition, 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 consumers are not disserved by multiple and conflicting standards over personal data, which would undermine consumer expectations and trust.

Recognize Consumer Rights. A national consumer privacy law must be squarely focused on identifying and protecting consumer rights. A law should provide consumers with the following rights with regard to personal data, subject to legal obligations and limitations and informed by the legitimate interests of a business:

- Consumers should have the right to transparency regarding a company's data practices, including the types of personal data that a company collects, the purposes for which this data is used, whether personal data is disclosed to third parties and, if so, for what purposes, but companies should be allowed flexibility as to the form and manner in providing this information based on the context.

- Consumers should have opportunities to exert reasonable control in regard to the collection, use and sharing of personal data. Consumers should also have the opportunity to make choices with respect to the sale of their personal data to non-

affiliated third parties. 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, taking into account the sensitivity of the personal data and the risks associated with its collection, use and sharing.

- Consumers should have a reasonable right to access and correct inaccuracies in personal data about themselves, taking into account both security and operational risks and other considerations.

- Consumers should be able to require an organization to delete personal data about them when the personal data is no longer required for the organization's legitimate business purposes or legal obligations.

Require Data Stewardship and Accountability. In addition to providing for consumer rights, a comprehensive national consumer privacy law should also include responsible data practices and accountability requirements to ensure that companies are responsible stewards of consumer data. These obligations should focus on areas that present potentially higher risks to the rights and interest of consumers and provide flexibility for companies to manage risk based on the nature of the data use and the sensitivity of the data involved as well as the benefits that may be achieved. Companies should leverage established risk-based privacy practices to prioritize and adjust their compliance measures and apply greater focus and protections to data practices in higher-risk areas.

Enable Effective, Consistent Enforcement. In order to provide accountability and protect consumer rights, a national consumer privacy law must be consistently enforced, with coordination between the federal government and states. Business Roundtable supports the role of the FTC as the primary consumer privacy enforcement agency, and any law should ensure that the FTC is adequately funded and has appropriate staffing for effective enforcement. In the limited instances where another regulator is the primary enforcer of the law, care should be taken to promote consistent obligations on companies regardless of industry sector and to avoid duplication of enforcement across federal agencies. In addition, state attorneys general should be permitted to enforce the law on behalf of their state's residents while coordinating with the FTC in order to avoid duplicative or conflicting enforcement actions. A national privacy law should not provide for a private right of action.

The FTC should have the authority to impose fines taking into account a number of factors including the harm directly caused by, and the severity of, a company's conduct, as well as any actions taken by a company to avoid and mitigate the harm, the degree of intentionality or negligence involved, self-reporting of the issue, the degree of a company's cooperation, the types of data involved, and the company's previous conduct with respect to personal data privacy and security.

Furthermore, the FTC should play a significant role in furthering industry adoption of a national privacy law by facilitating and approving industry codes of conduct. The FTC also should play an important role as an enforcement backstop for companies that fail to honor a commitment to follow such a code of conduct. These codes of conduct serve an important function by helping to clarify a law's more general data privacy principles in response to specific consumer and industry considerations that may develop. Should Congress determine it necessary for the FTC to conduct notice and comment rulemaking pursuant to 5 U.S.C. § 553, that rulemaking should be clearly defined within the statutory framework to address the harms that Congress agrees warrant a remedy. In conducting such rulemaking, the FTC should adopt a regulation only upon a reasoned determination that its benefits justify its costs and seek input from its own economic and technical experts.

Business Roundtable appreciates the FTC's consideration of these comments and looks forward to continued collaboration in this area.

Sincerely,

Denise E. Zheng
Vice President, Technology and Innovation Policy
Business Roundtable

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.