November 9, 2018

Via Electronic Submission to: privacyrfc2018@ntia.doc.gov

Mr. David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780– 8780–01

Dear Mr. Redl:

On behalf of the members of Business Roundtable, an association comprised of chief executive officers of leading U.S. companies representing all sectors of the economy, I want to thank you for the opportunity to comment on the National Telecommunications and Information Administration's (NTIA) Request for Comment (RFC) on Developing the Administration's Approach to Consumer Privacy.

Enhancing and sustaining consumer trust is vital for continued innovation and economic competitiveness. To achieve this, all companies must process personal data responsibly and with respect for individual consumers' privacy. As business leaders, we take this responsibility seriously. We are committed to advancing policies that protect consumer data while promoting innovation and growth.

As technology and the digital economy have evolved, so too has the regulatory landscape. With the implementation of the European Union's General Data Protection Regulation (GDPR), the recent 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.

Privacy regulation fragmentation leads to a disjointed user experience and misalignment of expectations for consumers. It 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 our own borders by establishing a comprehensive and consistent national privacy law, which does not exist today. Business Roundtable is working across industries and sectors to develop a framework for legislation that strengthens protections for consumers, achieves greater transparency, and enables innovation.

In order to advance a framework for national consumer privacy legislation, government and the private sector must work together. We support the Administration's efforts to advance consumer privacy and welcome future opportunities to work together to achieve our shared goals.

Objectives for Consumer Privacy Leadership

Business Roundtable believes a national consumer privacy law must advance four important objectives, and we believe any future Administration policy, actions, or engagement on consumer privacy should prioritize the following:

- 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.

- Facilitate Innovation. 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 helps ensure 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.

Importantly, Business Roundtable believes that the goals of championing privacy, facilitating innovation, harmonizing regulatory regimes, and achieving global interoperability – all shared by the Administration and included in your Request for Comment – 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 consumers' current ability to manage their privacy preferences.

Components of a National Consumer Privacy Law

The goals identified above can be achieved best through a national consumer privacy law that includes the components described below. These components will form the basis of a sound national framework, and we believe they align well with the Administration's privacy outcomes.

Applicability. A national consumer privacy law should apply to the collection, use, and sharing of consumers' personal data by private organizations. Information held by private organizations should be covered by such a law if it reasonably may be deemed to identify or be identifiable to a natural, individual person. However, it is appropriate for such a law to exclude from its 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 within the public domain.

Comprehensive Approach. 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.

Recognize Consumer Rights. A national consumer privacy law should provide consumers with certain rights with regard to their personal data, subject to legal limitations and informed by the legitimate interests of the organization:

- 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.

- 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 correct inaccuracies in personal data about them. NTIA appropriately recognizes the need to consider risks and other legitimate business considerations with respect to the accommodation of this right.

- Consumers should be able to delete personal data about them, with certain limited exceptions including when that personal data is required for legitimate business purposes or legal obligations of the company.

Governance and Accountability. Companies that collect or use personal data should have policies and procedures in place to ensure that data processing is consistent with a national consumer privacy law. Companies should be responsible for contractually imposing obligations associated with personal data on vendors with whom they share that data. Companies should have appropriate mechanisms in place to handle consumers' inquiries or complaints regarding personal data practices.

Risk-Based Privacy Practices. Companies should leverage risk-based privacy practices that apply greater protections to data practices that may present higher risks to the rights and interests of individuals. Companies should have flexibility in how they leverage risk-based privacy practices, which can include: balancing the interests a company has in the data processing with the potential risk to consumers; implementing privacy by design practices; and conducting privacy impact assessments for higher risk data processing.

Address Data Security. Companies 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. Given the evolving nature of cybersecurity threats, these safeguards should be risk-based, taking into account the sensitivity of the data and the potential harm that could result. A comprehensive federal standard should be implemented to ensure that consumers have the right to be notified within a reasonable timeframe if there is a personal data breach that presents a reasonable risk of significant financial harm to consumers.

Effective, Consistent Enforcement. Consistent and coordinated enforcement of a national consumer privacy law across the federal government and states is needed to provide accountability and protect consumer privacy rights. We support the role of the Federal Trade Commission (FTC) as the primary consumer privacy enforcement agency, 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. As such, the FTC should be adequately funded to enable its role as the primary enforcer of consumer privacy. In any case, enforcement actions and fines should be informed by 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, the degree of a company's cooperation, and the company's previous conduct with respect to personal data privacy and security. A national privacy law should not provide for a private right of action.

Business Roundtable appreciates NTIA's consideration of our comments and looks forward to continued collaboration as the Administration further develops its approach to consumer privacy.

Sincerely,

Julie Sweet
Chief Executive Officer - North America
Accenture
Chair, Technology Committee
Business Roundtable