November 9, 2018

The Honorable David J. Redl
Assistant Secretary for Communications and Information and Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725

Dear Secretary Redl,

We at Accenture appreciate the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA) consumer data privacy proposal. The NTIA astutely recognizes the tipping point that the U.S. has reached in its efforts to advance both consumer privacy and technological innovation. The implementation of the European General Data Protection Regulation (GDPR) and the consideration being given by other countries to establish national privacy laws could create a myriad of different privacy standards for consumers globally.

Domestically, the California Consumer Privacy Act (CCPA) in the short run could establish a de facto standard for Americans without the benefit of other state or national stakeholders' input. Other state governments are certain to respond with their own data privacy requirements, resulting in regulatory fragmentation that would have negative impacts for consumers and businesses.

Therefore, given these factors, a national consumer data privacy law is needed. The comments provided below outline Accenture's views on the scope and substance of a national privacy law.

<u>High Level Goals</u>
The digital era has dramatically changed the way personal information is used by organizations and how consumers use technology to obtain products and services. To protect individual privacy and foster innovation, the Administration and Congress should enact a national consumer data privacy law that is based on a defined set of rights that both empower and provide clarity to consumers. At minimum, a national consumer data privacy law should achieve the following goals:

- **Transparency:** Consumers should have a right to easy access, through a wide range of technologies, to clear, understandable statements about an organization's practices and policies with respect to personal data, including: information on the types of data collected; the purposes for which the personal data will be used, by the organization or by any related or unrelated third party; whether and for what purposes personal data may be disclosed or sent to related or unrelated 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.

- **Consumer Control:** Consumers should have a right to control the collection, use, and sharing of personal data they provide to organizations. No one specific mechanism for consumer control is suitable in all instances, and organizations should be permitted flexibility in how these controls may be exercised, while also responding to both the risks and the context of the specific data being collected, used, and shared.
    - Where organizations rely upon "consent" to collect and use personal data, the type of consent required should take into account the nature of both the personal data and its proposed uses. For example, opt-in consent may be required as part of a risk-based privacy practice for consumer data that presents higher risks to the rights and interests of individuals.
- **Harmonization and Interoperability:** Consumer privacy and prosperity would benefit from a harmonized national standard that preempts state law and maximizes potential interoperability with foreign privacy regimes.

Consumer Rights

A national privacy law should achieve consumer transparency and control, while enabling innovation by establishing the following rights:[1]

- **Access:** The right to reasonable access to the personal data a consumer provides to organizations;
- **Object to Sale:** The right to object to the sale of their personal data to non-affiliated third parties for direct marketing;
    - Personal data of children should not be sold unless the child's parent or guardian affirmatively "opts-in" to the sale of their personal data.
- **Correction:** The right to request the correction of any inaccuracies in the personal data a consumer provides to an organization.
- **Deletion:** The right to request deletion of personal data a consumer has provided to an organization, as long as the data is no longer required for the legitimate business purposes of the organization, and except where targeted disposal is not reasonably feasible due to the way the information is maintained.

Business Approach to Privacy

In addition to consumer rights, a national privacy law should also address business practices geared toward earning and maintaining consumer trust:

- **Risk-Based Privacy Practices:** Organizations should act responsibly by leveraging risk-based privacy practices to apply greater protections to consumer data that may present higher risks to the rights and interests of individuals and to

[1] Facilitations of these rights should take into account the legitimate interests of the organization, which may include compliance with applicable laws.

address emerging risks as business practices and technologies evolve. Organizations can demonstrate risk-based privacy practices by:

  - Taking privacy risks into account starting from the design phase of a proposed data processing activity and continuing throughout the entire life-cycle of the activity;
  - Assessing and balancing the interests and benefits of the processing to organizations, individuals and society against the potential risks and applying appropriate mitigations.
  - Conducting privacy impact assessments where more sensitive data or higher risk data processing activity is involved, and applying greater protections, such as data minimization and encryption, to those activities.
  - Assessing the lifecycle of the data and seeking to delete or anonymize consumer data as soon as it no longer needs to be retained for its original purpose or for any legal or regulatory purposes.

- **Governance:** Organizations should create and implement policies and procedures that reflect these principles and appropriately monitor uses of consumer data to ascertain that such uses are legitimate and consistent with the law, as well as internal policies, procedures, and notices to consumers. Implementing these policies would necessitate organizations putting appropriate mechanisms in place to handle consumer inquiries, requests, or complaints regarding the organization's consumer information practices.

- **Data Security:** Organizations should be required to implement reasonable technical and organizational safeguards to protect against the loss of or unauthorized access to consumer data, the unauthorized use or disclosure of data, or other potentially harmful misuses. Such safeguards should be proportional to the likelihood and severity of the financial harm threatened and the sensitivity of the consumer data. Companies should be required to assess the risks and determine appropriate security procedures for specific circumstances.

- **Third Parties:** Organizations that have consumer relationships should be obligated to contractually impose the same obligations on third-party service providers that process consumer information on their behalf.

Applicability

In applying these rights, a national consumer data privacy law should establish a consistent government-wide approach to defining consumer information and a clear framework for applicability of the law.

- **Consumer Information:** Consumer information should be defined as data that is held by the organization and identifies or is identifiable to a natural 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 is reasonably linked or linkable to

a specific individual. Sensitive categories of consumer data that may present increased risk should be subject to additional data obligations and protections.[2]

- **Small Businesses:** A national law should take into account limitations of small and medium-sized companies. Requiring smaller companies to incorporate privacy by design in their products and services, while holding them accountable for unfair or deceptive acts, should be sufficient to help them prepare and transition their data policies as they scale.

- **Breach Notification:** A consumer data privacy law should include a national standard for breach notification. 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 data breach.

Enforcement

A national data privacy law that preempts state law requires strong, consistent, and coordinated enforcement by federal and state governments to provide accountability and protect consumer data privacy rights. A private right of action, which would lead to a complex, conflicting legal and regulatory environment, would limit innovation and harmonization and would prevent international interoperability.

- **Federal Trade Commission (FTC):** A violation of this framework should be enforced by the FTC (or by another agency with enforcement powers over the organization). The FTC should be sufficiently resourced to enable effective enforcement. Enforcement actions and fines should be informed by the harm directly caused and severity of an organization's conduct as well as any actions taken by the organization to 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.

- **State Attorneys General:** A national consumer data privacy law should empower State Attorneys General to bring an action in federal court to enforce these requirements on behalf of their state's residents. States should be required, when appropriate, to coordinate with the FTC and to consolidate multiple state actions to avoid duplicative enforcement based on the same underlying conduct.

- **Codes of Conduct and Assessments:** A national consumer data privacy law should encourage the development and use of codes of conduct as well as the use of regular third-party assessments. Organizations that adhere to codes of conduct approved by the FTC and whose adherence is validated by regular third-party assessments should be presumed to be in compliance with the law.

Since the advent of online communications and commercial activity more than two decades ago, data has been central to numerous innovations and advancements that have served to benefit individual consumers and the broader global economy. And

[2] For example, sensitive data may include health information, financial information, personal data collected from children, biometric identifiers, and precise geolocation data.

those innovations will accelerate even more with emerging technologies like artificial intelligence and quantum computing.

It's in light of these current and emerging trends, and the critical role and importance of consumer trust, that necessitate action by Congress and the Administration to enact a national consumer data privacy law. We welcome this opportunity to provide our ideas on what such a law would look like. More important, we welcome the opportunity to work with you, your colleagues in the Administration, and Congress to achieve this objective.

Very respectfully yours,

Julie Sweet
Chief Executive Officer
North America Accenture