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.