U.S. CHAMBER PRIVACY PRINCIPLES

The United States Chamber of Commerce believes that consumers benefit from the responsible use of data. Technology and the data-driven economy serve as the twenty-first century's great democratizer by empowering and enabling increased access to educational, entrepreneurial, health care, and employment opportunities for all Americans.

Consumers have more options than ever when it comes to goods, services, information, and entertainment. Data-driven innovation and investment enable consumers to take advantage of faster, higher quality, and customized services at lower or no costs. This Fourth Industrial Revolution, relying on data and technology, requires policies that promote innovation, regulatory certainty, and respect for individual privacy and choice. Underpinning these efforts is a recognition that consumers must have assurance that data is safeguarded and used responsibly.

The Chamber offers the following principles to achieve this goal:

A NATIONWIDE PRIVACY FRAMEWORK

Consumers and businesses benefit when there is certainty and consistency with regard to regulations and enforcement of privacy protections. They lose when they have to navigate a confusing and inconsistent patchwork of state laws. While the United States already has a history of robust privacy protection, Congress should adopt a federal privacy framework that preempts state law on matters concerning data privacy in order to provide certainty and consistency to consumers and businesses alike.

PRIVACY PROTECTIONS SHOULD BE RISK-FOCUSED AND CONTEXTUAL

Privacy protections should be considered in light of the benefits provided and the risks presented by data. These protections should be based on the sensitivity of the data and informed by the purpose and context of its use and sharing. Likewise, data controls should match the risk associated with the data and be appropriate for the business environment in which it is used.

TRANSPARENCY

Businesses should be transparent about the collection, use, and sharing of consumer data and provide consumers with clear privacy notices that businesses will honor.

INDUSTRY NEUTRALITY

These principles apply to all industry sectors that handle consumer data and are not specific to any subset of industry sectors. These principles shall be applied consistently across all industry sectors.

U.S. CHAMBER PRIVACY PRINCIPLES

FLEXIBILITY

Technology evolves rapidly; laws and regulations should focus on achieving these privacy principles. Privacy laws and regulations should be flexible and not include mandates that require businesses to use specific technological solutions or other mechanisms to implement consumer protections. A federal privacy law should include safe harbors and other incentives to promote the development of adaptable, consumer-friendly privacy programs.

HARM-FOCUSED ENFORCEMENT

Enforcement provisions of a federal data privacy law should only apply where there is concrete harm to individuals.

ENFORCEMENT SHOULD PROMOTE EFFICIENT AND COLLABORATIVE COMPLIANCE

Consumers and businesses benefit when businesses invest their resources in compliance programs designed to protect individual privacy. Congress should encourage collaboration as opposed to an adversarial enforcement system. A reasonable opportunity for businesses to cure deficiencies in their privacy compliance practices before government takes punitive action would encourage greater transparency and cooperation between businesses and regulators. In order to facilitate this collaboration, a federal privacy framework should not create a private right of action for privacy enforcement, which would divert company resources to litigation that does not protect consumers. Enforcement authority for a federal privacy law should belong solely to the appropriate state or federal regulator.

INTERNATIONAL LEADERSHIP

Congress should adopt policies that promote the free flow of data across international borders for consumer benefit, economic growth and trade. A national privacy framework will bolster continued U.S. leadership internationally and facilitate interoperable cross-border data transfer frameworks.

ENCOURAGING PRIVACY INNOVATION

Incorporating privacy considerations into product and service design plays an important role and benefits all consumers. A national privacy framework should encourage stakeholders to recognize the importance of consumer privacy at every stage of the development of goods and services.

DATA SECURITY AND BREACH NOTIFICATION

As part of a national privacy framework, Congress should include risk-based data security and breach notification provisions that protect sensitive personal information pertaining to individuals. Keeping this information secure is a top industry priority. Security is different for individual businesses and one-size-fits-all approaches are not effective; therefore, companies should have flexibility in determining reasonable security practices. Preemptive federal data security and breach notification requirements would provide consumers with consistent protections and would also reduce the complexity and costs associated with the compliance and enforcement issues resulting from different laws in the 50 states and U.S. territories.