HOUSE COMMITTEE ON

ENERGY & COMMERCE

CHAIRMAN BRETT GUTHRIE

PRIVACY WORKING GROUP

REQUEST FOR INFORMATION

The United States digital economy adds $2.6 trillion in value and employs millions of American workers across nearly every sector of the broader economy. Leadership in digital technologies, including artificial intelligence, underpins U.S. economic and national security, provides American consumers with access to lower cost goods and services, and enables small businesses to reach markets around the world.

However, the challenge of providing clear digital protections for Americans is compounded by the fast pace of technological advancement and the complex web of state and federal data privacy and security laws, which in some cases create conflicting legal requirements. Members of Congress have spent many years working toward federal comprehensive data privacy and security standards to bring consumer protections into the digital age while ensuring that the U.S. continues to lead in a globally competitive environment.

On February 12, Energy and Commerce Committee Chairman Brett Guthrie (KY-02) and Vice Chairman John Joyce, M.D. (PA-13) announced the creation of a data privacy working group.[1] The working group is bringing members and stakeholders together to explore the parameters of a federal comprehensive data privacy and security framework.

To inform the working group's efforts, we invite stakeholders to provide written responses to the prompts below. **Stakeholders should submit their responses to PrivacyWorkingGroup@mail.house.gov no later than April 7, 2025.** We request that written responses be no longer than 3,500 words and be provided as a Word document and a PDF. Supplemental data, reports, and case studies are also welcome.

1 *Chairman Guthrie and Vice Chairman Joyce Announce Creation of Privacy Working Group*, Committee on Energy and Commerce, Feb. 12, 2025, https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-announce-creation-of-privacy-working-group.

I. Roles and Responsibilities

The digital economy includes a wide range of business models, including entities that collect information directly from consumers, those that process personal information on another business's behalf, and others that collate and sell personal information.

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?
B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?
C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

II. Personal Information, Transparency, and Consumer Rights

A federal comprehensive data privacy and security law should apply to personally identifiable information and provide consumers with clear disclosures and rights to their personal information.

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."
B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?
C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?
D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

III. Existing Privacy Frameworks & Protections

Since 2016, U.S. trading partners and a growing number of states have enacted comprehensive data privacy and security laws to govern the collection, processing, and transfer of personal information.

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.
B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.
C. Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?
D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?

IV. Data Security

A foundational goal for any federal comprehensive privacy law should be increased security of Americans' personal information.

A. How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?

V. Artificial Intelligence

Most state comprehensive data privacy and security laws regulate AI through "automated decision-making" requirements. A growing number of states are also enacting—or are seeking to enact—additional AI-specific laws. These developments raise questions about the role of privacy and consumer protection standards in AI regulation and the impact on U.S. AI leadership.

A. How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?

VI. Accountability & Enforcement

Accountability and enforcement are cornerstones of a data privacy and security regime that protects consumers, promotes compliance, and enables data-driven innovation.

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.
B. What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?
C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

VII. Additional Information

We welcome any additional information that may be relevant to the working group as it develops a comprehensive data privacy and security law.