1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

Via Electronic Filing to PrivacyWorkingGroup@mail.house.gov

April 7, 2025

The Honorable Brett Guthrie
Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Joyce
Vice Chairman
House Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

RE: Request for Information to Explore Data Privacy and Security Framework

Dear Chairman Guthrie and Vice Chair Joyce:

The Consumer Technology Association (CTA)[1] appreciates the opportunity to respond to the House Energy and Commerce Committee Privacy Working Group Request for Information (RFI) to explore data privacy and security framework.[2]

CTA's membership includes over 1200 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with startups or small and mid-sized companies comprising 80 percent of CTA's members. CTA also owns and produces CES – the world's most powerful tech event.

Privacy is a key public policy priority for CTA under our 2025 Innovation Agenda. As the digital economy expands, consumers expect both privacy protection and continued access to innovative, data-driven products and services. Data is used to provide consumers the products and services that they want, and CTA recognizes that this exchange should be complemented by strong privacy protections.

We need a uniform, risk-based, and innovation-friendly federal privacy law to achieve this balance. The absence of a comprehensive federal framework has led to an increasingly complex and fragmented patchwork of state rules, creating consumer confusion and placing undue

[1] As North America's largest technology trade association, CTA is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®— the most powerful tech event in the world.
[2] https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework

compliance burdens on small and medium-sized businesses. A well-structured federal framework without a private right of action would enhance consumer protection while fostering regulatory certainty that spurs American innovation.

Below, CTA responds to the RFI questions, offering insights based on our advocacy efforts, industry expertise, and prior policy recommendations.

I. Roles and Responsibilities

A. *How can a federal data privacy and security law account for different roles in the digital economy in a way that effectively protects consumers?*

A federal privacy law should establish clear definitions for entities such as **data controllers, data processers, and third parties** to ensure precise assignment of responsibilities.

- **Data controllers** determine the purpose and means of processing personal data and should be responsible for obtaining consumer consent, ensuring data accuracy, and maintaining clear data usage policies.
- **Data processors** handle data on behalf of controllers and the law should require robust security measures while processing data strictly as instructed. De-identified data should be excluded from the limitations placed on processors.
- **Third parties** that sell or pass on consumer data should be required to comply with original consent terms and maintain records of data sources.

This structured approach ensures that privacy obligations are tailored to an entity's role, minimizing unnecessary compliance burdens while maximizing consumer protections.

B. *What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?*

CTA supports role-specific obligations that align with an entity's direct interaction with consumer data.

- **Data controllers** should be responsible for transparency, consent management, data minimization, and user rights (e.g. access and deletion requests).
- **Data processors** should focus on security and compliance with controllers' directives, ensuring data integrity without independent decision-making.
- **Third parties** should adhere to strict data usage guidelines and/or terms and conditions of the applicable contract, preventing unauthorized data sharing.

By structuring obligations in this way, the framework ensures that consumer protections are enforced without stifling data-driven innovation or overburdening smaller companies with requirements meant for large enterprises.

C. *Should comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?*

While CTA recognizes that compliance capacity varies, we caution against exemptions based *solely* on entity size. A tiered compliance approach – based on both the size of the entity and the volume and sensitivity of data handled – would better ensure that smaller businesses can comply without unneeded burdens while protecting all consumers.

- **Tiered compliance requirements** based on data volume and sensitivity can ensure smaller entities remain competitive while protecting consumers.
- **Baseline protections** should apply universally to ensure trust in the digital ecosystem.

As noted in a public statement by CTA CEO and Vice Chair Gary Shapiro, overburdening smaller businesses with compliance costs could reduce competition and hinder innovation. Any federal privacy law should not include a private right of action. The risk of frivolous lawsuits and the associated cost hurts small businesses while not adding increased privacy protection for consumers.

II. Personal Information

A. *Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information".*

CTA supports a clear and practical definition of personal information:

- **Personal information** includes any data that identifies or can reasonably be linked to an individual.
- **Sensitive personal information** should include health data, financial data and biometric information that is not protected under existing laws. Alternatively, as stated in CTA comments to CISA regarding U.S. Sensitive Personal Data, precise geolocation data should be excluded from this definition given that it is not fundamentally individual. Creating a uniform, national definition of sensitive personal information (SPI) is essential to facilitate compliance and simplify interstate operations.

These definitions should be tailored to avoid overregulation of low-risk data categories while ensuring strong protections for highly sensitive data.

B. *What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?*

CTA advocates for concise and accessible disclosures that empower consumers with meaningful information, without overwhelming them with complex legal jargon. Required disclosures should:

- Inform consumers about what personal information is collected and purposes of its use;
- Disclose any selling of personal information to third parties, including the purpose and nature of such selling;
- Provide information on the criteria for determining retention periods;
- Include right to retain data for a legitimate business purpose; and
- Require public posting of a Notice of Privacy Practices (NOPP) for entities that fall under existing federal privacy law would enhance transparency.

Well-structured transparency measures ensure consumers understand their rights without hindering their ability to engage with digital services.

C. *Please identify consumer protections that should be included in comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?*

A balanced framework should grant consumers reasonable control over their personal data through rights such as:

- **Access & Correction**: Consumers should be able to review and update their information.
- **Deletion Requests**: Consumers should have the right to delete their data, except if retention is needed for legitimate reasons including security, contractual, or legal. Automated deletion of data which no longer has a business purpose should be allowed.
- **Opt-Out Rights**: Consumers should be able to opt out of data sales, targeted advertising, and profiling in solely automated decisions that produce legal or similarly significant effects concerning the consumer.

These rights reiterate CTA's statements to NTIA in 2023 regarding the intersection of Privacy, Equity, and Civil Rights. A CTA research report on consumer attitudes and behaviors on data privacy recommended that when engaging with consumers, companies and service providers should

- Provide data transparency;
- Ensure that consumers know how to protect themselves; and
- Focus on data security.

D. *What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?*

Along with the above-stated consumer rights, explicit consent should be required for collecting or processing sensitive personal information, ensuring heightened protections where necessary. These protections should be practical and should include reasonable exceptions. They should be enforceable, without undermining beneficial data uses that enhance consumer experiences.

III. Existing Privacy Frameworks & Protections

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-drive innovation and small businesses.

CTA strongly cautions against adopting overly restrictive models such as the EU's General Data Protection Regulation (GDPR), which has stifled European innovation and disproportionately harmed small businesses. Instead, a U.S. federal framework should:

- Align with successful industry-driven standards (i.e. NIST frameworks);
- Ensure compatibility with existing sectoral laws (HIPAA, GLBA, COPPA, etc.); and
- Avoid unnecessary duplication or conflicts with existing protections.

A flexible, risk-based approach ensures both consumer protection and continued U.S. leadership in global technology innovation.

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.

The current patchwork of state privacy laws leads to uneven consumer rights and increased compliance costs for businesses. This system creates:

- Uneven consumer rights across jurisdictions;
- High compliance costs, particularly for small businesses; and
- Legal uncertainty that discourages innovation.

A single federal standard would eliminate confusion and promote a fair, competitive market. As stated by CTA's CEO and Vice Chair, Gary Shapiro, "a state-centric approach simply doesn't work in a digital economy, where data flows across borders in a matter of seconds."

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?

CTA strongly supports full federal preemption of state privacy laws to ensure:

- Uniform consumer rights and protections nationwide;
- Simplified compliance for businesses operating across multiple states; and
- Reduced legal uncertainty that discourages investment in innovation

Without preemption, the existing patchwork of state laws will continue to create confusion for consumers and costly compliance burdens – ultimately hurting both consumers and businesses alike. It will fall especially hard on startups and smaller businesses.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (ex. HIPAA, FCRA, GLBA, COPPA)?

A comprehensive federal privacy law should harmonize with existing sector-specific regulations to ensure comprehensive protection without redundancy or conflict. CTA has previously encouraged such consistency in its comments to NTIA in 2023 regarding the intersection of Privacy, Equity, and Civil Rights: "Many companies abide by the requirements found in the GLBA, HIPAA, Children's Privacy Protection Act, and the FCC's customer proprietary network information rules…Regulators are effectively enforcing these sector-specific requirements, and [we] should avoid recommendations that conflict with current obligations under these existing laws. New recommendations should not seek to impose duplicative regulations or new enforcers where an area is already working."

We note, however, that each of these should be examined to assess whether a new comprehensive federal privacy law should supplant these legacy requirements because of changes in technology and the marketplace. A federal privacy law should also include an exemption for HIPAA covered entities when they are acting as a covered entity or business associate under the law.

IV. Data Security

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

CTA supports a risk-based approach that aligns security measures with data sensitivity, including:

- Encryption for sensitive data; and
- Industry-driven best practices that allow for adaptability

Public-private partnerships should be leveraged to enhance cybersecurity protections and educational initiatives to inform consumers of their rights. Additionally, deference to existing laws, where applicable, would leverage established protections and streamline integration.

V. Artificial intelligence

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

A federal privacy law should:

- Ensure federal preemption of state AI policies to prevent conflicting regulations;
- Encourage alignment with voluntary frameworks like the NIST AI Risk Management Framework; and
- Preempt state privacy law provisions that regulate automated decision-making.

VI. Accountability & Enforcement

A. *Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.*

CTA supports expert agency enforcement rather than private right of action, with the FTC as the primary enforcer in collaboration with agencies like NIST and CISA for technical guidance. This approach ensures:

- Consistency in enforcement;
- Avoidance of conflicting agency mandates; and
- Technical expertise in privacy and security compliance.

To create a uniform, federal system led by a singular agency, "Congress must ensure that any federal privacy law includes the necessary resources and authority for enforcement agencies to effectively carry out their mandates", as stated in CTA's comments to CISA regarding U.S. Sensitive Personal Data.

However, rulemaking and enforcement should not be in the same government body. Designating the FTC as the primary enforcement entity means the FTC should not also have rulemaking authority.

B. *What expertise, legal authorities, and resources are available – or should be made available – to the FTC and state Attorneys General for enforcing such a law?*

CTA emphasizes the importance of collaboration in these efforts:

- Cross-agency collaboration – under a preemptive federal law the FTC and state Attorneys General should partner with NIST and CISA to develop privacy risk frameworks and cybersecurity guidelines; and

- Public-Private collaboration – these relationships would help support voluntary frameworks and industry standards.

C. How could a safe harbor be beneficial or harmful in promoting compliance with obligations related to data privacy and security?

CTA sees the following as potential benefits of a safe harbor in promoting compliance with data privacy and security obligations:

- Encourage proactive compliance by offering protection to businesses that follow best practices and frameworks, such as NIST;
- Reduce legal uncertainty for businesses, especially small companies; and
- Prevent unnecessary litigation while maintaining strong consumer protections.

A well-structured safe harbor that offers an affirmative defense for entities complying with established measures incentivizes responsible privacy practices without enabling bad actors. As stated in CTA's letter to Chair Rogers and Ranking Member Pallone in Advance of the APRA and AM Radio Markup in 2024, "[without a safe harbor], companies acting in good faith, without any harmful intent, would be forced to shell out hefty settlements to avoid the exorbitant costs of litigation…This concern is particularly acute for small and medium-sized businesses that lack the resources to defend against multiple opportunistic legal actions."

VII. Additional Information

Congress should consider consumer attitudes and expectations about data privacy when crafting any legal framework. According to CTA research, consumers are concerned about privacy, but they want their lives to be easier. Consumers are willing to balance data privacy with ease of use:

- Better shopping suggestions with personalized product recommendations;
- Better streaming service suggestions; and
- Better banking options

Research also shows that 64% of consumers prefer to buy from companies that tailor their experience to their wants and needs, and according to Deloitte 78% of consumers surveyed believe their digital experiences have a positive impact on their lives.

Conclusion

CTA appreciates the Committee's efforts to establish a comprehensive, uniform federal privacy framework that protects consumers while fostering innovation. A risk-based, preemptive approach will ensure regulatory clarity, consumer trust, and continued American technological leadership.

We look forward to working with the Committee on balancing privacy and innovation enhancing American lives.

Sincerely,

Rachel Nemeth
Sr. Director, Regulatory Affairs
Consumer Technology Association

Tiffany M. Moore
SVP, Political and Industry Affairs
Consumer Technology Association