April 9, 2025

The Honorable Dr. John Joyce
Vice Chairman, Committee on Energy and Commerce
Chairman, Privacy Working Group
U.S. House of Representatives

And Members of the Privacy Working Group:
Representative Morgan Griffith
Representative Troy Balderson
Representative Jay Obernolte
Representative Russell Fry
Representative Nick Langworthy
Representative Tom Kean
Representative Craig Goldman
Representative Julie Fedorchak

Re: *Response to the Privacy Working Group's Request for Information to Explore a Data Privacy and Security Framework for the U.S.*

Respondent: The Marketplace Industry Association

Dear Dr. Joyce and Members of the Privacy Working Group:

The Marketplace Industry Association (MIA) appreciates the opportunity to provide input to the Data Privacy Working Group as it considers a federal data privacy and security framework.

MIA is a trade association representing a diverse group of digital platforms and online marketplaces. Our mission is centered on advocating for policies that foster innovation and competition in the digital marketplace, while preventing harmful regulations that create unnecessary barriers for these dynamic businesses. We focus on ensuring policymakers recognize the unique challenges and regulatory burdens that disproportionately impact digital platforms and online marketplaces, and the communities they serve.

The following outlines key principles and recommendations that we urge the Privacy Working Group to consider, followed by detailed responses to specific questions impacting our members.

EXECUTIVE SUMMARY

Enacting a federal privacy law that protects consumers and supports the continued growth of the digital economy is essential. A single national framework that fully preempts state laws would eliminate the costly and complex patchwork of state-by-state regulations. This patchwork creates

uncertainty, drives up compliance costs, stifles innovation, and hinders the ability of digital platforms and online marketplaces to compete, ultimately benefiting larger, established players.

MIA supports a federal standard modeled after the Virginia Consumer Data Protection Act (VCDPA), as passed and unamended—a risk-based, pro-innovation approach that protects consumers without imposing overly rigid mandates. Enforcement should be primarily entrusted to the Federal Trade Commission (FTC), with sectoral-specific regulators retaining oversight within their domains.

To minimize conflicts and barriers to data flows, a federal law should align closely with the requirements of the US-EU Data Privacy Framework. Finally, safe harbor provisions should protect platforms and marketplaces that demonstrate good-faith compliance efforts.

In summary, a federal privacy law should strengthen U.S. economic leadership in the digital space, reinforce innovation, and ensure strong consumer protections without hindering the growth and dynamism of digital platforms and online marketplaces.

DETAILED RESPONSES

1. **Roles And Responsibilities**

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?

A federal framework must clearly define the roles of controllers and processors, providing practical compliance pathways for digital platforms and online marketplaces:

- Controllers (platforms and marketplaces that determine the purposes of data processing) should have primary responsibility for consumer transparency, choice, and data protection measures.
- Processors (service providers acting on behalf of platforms and marketplaces) should be responsible for data security and contractual compliance, but should not be held liable for privacy decisions made by the platforms or marketplaces.

It is essential to avoid overbroad definitions that could unintentionally hinder the operations of digital platforms and online marketplaces. Definitions must be narrowly scoped, targeted, and proportionate to the diverse roles within the digital ecosystem. A risk-based and role-specific approach to privacy is crucial, where requirements are aligned with the sensitivity of the data and the potential for harm from its processing.

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

Obligations should align with the entity's degree of control over personal data and its relationship with consumers, preventing unfair compliance burdens on digital platforms and online marketplaces.

- **Controllers (Platforms and Marketplaces):** Ensuring transparency around data practices, obtaining consumer consent where necessary, responding to consumer rights requests, and implementing reasonable security safeguards.

- **Processors:** Implementing contractual and security obligations. They should support controllers in responding to consumer rights requests but should not be required to provide direct consumer-facing privacy controls that are outside their authority.

Regulations must reflect the operational realities of the sector, where entities often function as both controllers and processors across different services.

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

A federal privacy law should base obligations on the sensitivity and volume of data processed, not on arbitrary size thresholds. While companies processing high-risk data (e.g., biometric or health data) may require additional safeguards, compliance requirements should be proportional to actual risks.

To balance consumer protection with business practicality, a federal law should allow for scaled compliance, including:

- Phased implementation timelines.
- Proportional obligations based on the nature and sensitivity of data.
- Secure safe harbor provisions for good-faith compliance efforts.

2. Personal Information, Transparency and Consumer Rights

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

A federal law should adopt clear and limited definitions:

- "Personal Information" should be narrowly defined as data that identifies or can be reasonably linked to an individual, excluding publicly available, de-identified, or aggregated data.
- "Sensitive Personal Information" should include specific categories, such as:
    - Data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship/immigration status.
    - Genetic or biometric data used for uniquely identifying a person.

- Data collected from a known child (under 13).
- Precise geolocation data.

The definition of "targeted advertising" should be balanced to support both privacy and innovation, allowing for preference-based ads while including exceptions for first-party and contextual advertising.

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

A federal privacy law should prioritize meaningful consumer transparency while avoiding unduly burdensome disclosure requirements. The law should:

- Focus on high-risk data uses.
- Allow for scaled disclosures.
- Minimize redundant pop-ups and consent fatigue.
- Require notices to include key information (data categories, usage, sharing, consumer rights).

Notices should be consumer-friendly and practical for businesses.

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?

Consumer rights should be targeted, practical, and balanced. Key components include:

- Right to access.
- Right to correction.
- Right to deletion (with exceptions).
- Right to portability (when feasible).
- Right to opt-out of third-party targeted advertising.

Enforcement should be a shared responsibility between the FTC and sectoral regulators, without a private right of action. Safe harbors for good-faith compliance are essential.

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

A risk-based approach is needed, preventing misuse while allowing necessary processing for security, fraud prevention, and innovation. This includes:

- Limiting heightened protections to high-risk uses.
- Requiring explicit consent only for specific processing activities.

- Avoiding excessive consent requirements.
- Aligning consent mechanisms with VCDPA.
- Requiring consent to prevent "Big Tech" from misusing data collected via one product or service for a very different and unrelated product or service without clear consumer notice and consent.

3. Existing Privacy Frameworks and 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-driven innovation and small businesses.

A federal privacy law should build on effective elements from existing frameworks, such as the EU's GDPR and the VCDPA, while avoiding unintended consequences.

The GDPR provides strong consumer rights and clear principles but has also led to excessive compliance costs, disproportionately impacting smaller players and hindering innovation. The VCDPA offers a more balanced approach with its risk-based model, no private right of action, opportunity to cure, and flexibility.

A federal law should blend the GDPR's strengths with the VCDPA's practicality to safeguard privacy while fostering innovation and economic growth in the digital marketplace. It should also include carve-outs for data processing already subject to industry-specific regulations (e.g., HIPAA, GLBA).

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.

State-by-state privacy laws create a complex and unsustainable burden, particularly for digital platforms and online marketplaces that operate across the country. This patchwork leads to:

- Significant compliance costs.
- Uneven consumer rights.
- Hindered innovation.
- Undermined consumer trust.

A national standard is essential to provide clarity, enhance consumer protection, and prevent excessive government interference.

C. Given the proliferation of state requirements, what is the appropriate degree of pre-emption that a federal comprehensive data privacy and security law should adopt?

A federal law must fully pre-empt state privacy laws to avoid the significant burdens and inconsistencies of a patchwork system. Full pre-emption will:

- Provide clarity for businesses.
- Reduce compliance costs.
- Support innovation.
- Ensure consistent consumer protection.
- Promote a consistent user experience.

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

A federal privacy law should complement existing sectoral laws, avoiding conflicts and duplicate obligations. This can be achieved by:

- Maintaining sectoral exemptions.
- Clarifying that sectoral law requirements take precedence.
- Aligning data rights and transparency obligations.

The FTC should be the primary enforcer, ensuring consistency, while sectoral regulators retain authority over their specific domains.

4. Data Security

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

A federal privacy law should improve data security by:

- Maintaining the "reasonable security" standard.
- Encouraging FTC guidance on reasonable security practices.
- Emphasizing data minimization.
- Supporting public-private collaboration on cybersecurity.
- Allowing for flexible security measures based on size, resources, and risk.
- Replacing the state-by-state patchwork with a uniform federal breach notification standard, focused on significant breaches that pose a real risk of harm.

5. 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 pre-empt state AI regulations to avoid a fragmented and costly compliance landscape that hinders AI adoption and innovation in the digital marketplace.

To harmonize AI-related privacy protections, the U.S. should prioritize:

- Industry collaboration.
- Flexible guidelines.
- Global alignment.

The law should clearly define the scope of automated decision-making using AI systems that triggers consumer opt-out rights, focusing on high-risk AI decisions. Routine AI-driven functions should not trigger opt-out requirements.

Safe harbors should exempt digital platforms and online marketplaces from complex AI compliance mandates unless they engage in high-risk AI decision-making. There should be no private rights of action in the AI context, and enforcement should remain with expert agencies.

AI transparency obligations and algorithmic fairness audits should be limited to high-risk AI applications. NIST should develop flexible AI guidelines. U.S. AI privacy laws should align with international frameworks.

A flexible, industry-driven, and innovation-friendly AI governance framework will ensure U.S. leadership in AI development and maintain consumer protections.

6. Accountability and Enforcement

MIA advocates for a shared enforcement model where the FTC has primary oversight, and sectoral agencies retain authority within their jurisdictions.

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

Benefits of this approach include:

- Regulatory consistency and predictability.
- Balanced, expertise-driven enforcement.
- Prevention of politicized enforcement.
- Reduced compliance costs for businesses.
- Focus on real harms, not technical violations.

Potential costs include:

- Potential for overlapping jurisdictions (addressed through coordination mechanisms).
- Risk of bureaucratic complexity (addressed through MOUs and reporting requirements).
- State Attorneys General may still attempt to intervene (addressed by limiting state AG involvement).

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?

The FTC should have:

- Clear authority to issue guidance and enforcement policies.
- Technical expertise in privacy and data security investigations.
- Resources for risk-based investigations.

Sector-specific agencies should retain enforcement authority within their industries.

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

Safe harbors are essential for a business-friendly compliance framework that encourages responsible data practices while preventing unnecessary legal risks for digital platforms and online marketplaces. Companies that make good-faith efforts to follow recognized best practices should be protected from frivolous lawsuits and excessive enforcement. Providing safe harbors incentivizes proactive compliance, as businesses are more likely to invest in strong privacy and security programs if minor infractions don't lead to disproportionate penalties. These provisions prevent regulatory overreach, ensuring enforcement targets intentional violations rather than punishing businesses navigating complex regulations.

In addition to safe harbors, a federal privacy law should include reasonable cure periods that allow businesses to remedy alleged violations after receiving formal notice from the relevant enforcement authority. This approach promotes good-faith efforts to comply, especially among those businesses that may inadvertently fall short of requirements despite best intentions. It can also increase regulatory efficiency by reserving more serious enforcement actions for willful, repeated, or harmful violations.

Without clear protections, digital platforms and online marketplaces face excessive legal and financial risks, diverting resources from innovation to legal defense. The risk of litigation abuse also rises when trial lawyers and state Attorneys General exploit privacy laws for political gain instead of genuine consumer protection.

CONCLUSION

A well-crafted federal privacy law should enhance consumer protections while fostering innovation. By pre-empting fragmented state laws, ensuring risk-based regulations, and maintaining sectoral expertise, policymakers can protect data security, promote AI adoption, and support U.S. economic growth.

The Marketplace Industry Association remains committed to advancing policies that balance security, innovation, and economic leadership. We appreciate the opportunity to contribute and look forward to shaping a pragmatic, pro-growth federal privacy framework.

Sincerely,

Jeremy Gottschalk
Executive Director
Marketplace Industry Association