April 4, 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: Internet Works

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

Internet Works appreciates the opportunity to share insights and suggestions with the Data Privacy Working Group as it considers a federal data privacy and security framework.

Internet Works (IW) is a trade association of diverse technology companies working together to right-size technology policy, particularly for technology firms that fall outside of "Big Tech" — a sector more appropriately referred to as Middle Tech. Our mission is centered on two key objectives:

- advocating for policies that promote innovation and competition while preventing harmful regulations that create unnecessary barriers for diverse and emerging technology businesses; and
- ensuring policymakers recognize the unique challenges and regulatory burdens that disproportionately impact Middle Tech companies and the communities they serve.

The following section summarizes the key points we urge the Privacy Working Group to consider. This is followed by detailed responses to relevant questions for our industries.

EXECUTIVE SUMMARY

Enacting a federal privacy law that protects consumers and supports business growth is essential to fostering innovation, competition, and consumer trust. A single national framework that fully pre-empts state laws would eliminate the costly regulatory patchwork that burdens startups, smaller businesses, and Middle Tech companies - driving up compliance costs, stifling AI adoption, and reinforcing dominance of large incumbents.

IW 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. Clear and predictable enforcement should be entrusted to the Federal Trade Commission (FTC), while sectoral-specific regulators retaining oversight within their domains.

Further, as businesses that operate internationally, we support a federal law that aligns closely with the requirements laid down in the US-EU Data Privacy Framework, so as to minimize risks of challenge and barriers to data flows and resultant negative economic impact to U.S. businesses.

Finally, safe harbor provisions should protect businesses that make good-faith compliance efforts, limiting unnecessary penalties for minor infractions. In sum, a federal privacy law should strengthen U.S. economic leadership, reinforce digital innovation, and ensure strong consumer protections without stifling growth.

DETAILED RESPONSES

I. 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 should clearly define the roles of controllers and processors, ensuring practical compliance pathways:

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

When defining the scope of responsibilities, it is essential to avoid overbroad definitions to minimize any unintended consequences that would make it more difficult for start-ups, smaller businesses, and Middle Tech companies to operate in today's economy. It is critical that the definitions that would outline the contours and scope of entities' roles in the data ecosystem be narrowly scoped, targeted, and proportionate to the diverse roles that exist within the tech ecosystem.

Taking a risk-based and role-specific approach to privacy - where the law imposes greater requirements based on the sensitivity of the data and the potential harm from its processing - would be key to ensuring clarity, avoiding redundant compliance obligations, and supporting competition in the digital economy.

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 an entity's degree of control over personal data and its relationship with consumers, avoiding unfair compliance burdens.

- Controllers: ensuring transparency around data practices, consumer consent

where needed, responding to consumer rights requests, and implementing reasonable security safeguards.
- Processors: implementing contractual and security obligations. While they should not be required to provide direct consumer-facing privacy controls that are outside their authority, they should be obligated to support controllers in responding to consumer rights requests in a timely and effective manner.

Often, actors function as both controllers and processors across different services. Regulations must reflect this operational reality and account for industry complexities, ensuring flexible, role-specific compliance requirements.

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 structure obligations based on the sensitivity and volume of data processed, not arbitrary size thresholds. Companies processing high-risk data — such as biometric or health data — may warrant additional safeguards, including risk assessments and enhanced transparency measures. However, compliance requirements should be proportional to actual risks, ensuring that businesses handling lower-risk data are not necessarily burdened.

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

- Phased implementation timelines based on data risk and processing volume, recognizing that some actors may need additional time to adjust.
- Proportional obligations that reflect the nature and sensitivity of data being processed, rather than company revenue or user metrics.
- Secure safe harbor provisions for businesses, ensuring that good-faith compliance efforts[1] are not penalized. (More on safe harbors in ***VI. Accountability and Enforcement*** below).

II. 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 of personal and sensitive data, for example:

- "**Personal Information**" should be narrowly defined as data that identifies or can reasonably be linked to an individual, while excluding publicly available, de-identified, or aggregated data to ensure businesses can use non-personal data for analytics, security, and innovation.
- "**Sensitive Personal Information**" should include,
    1. Personal data revealing:
        - Racial or ethnic origin
        - Religious beliefs

[1] Examples of 'good faith' would be companies implementing industry-standard security measures (e.g., NIST framework), or conducting regular (but not necessarily exhaustive) data protection audits.

    - Mental or physical health diagnosis
    - Sexual orientation
    - Citizenship or immigration status
2. Processing of genetic or biometric data for the purpose of uniquely identifying a natural person.
3. Personal data collected from a known child (i.e., an individual under the age of 13).
4. Precise geolocation data (i.e., data derived from a device and used or intended to be used to locate a consumer within a radius of 1,750 feet).

When defining the scope of a federal privacy law, it is important to consider how personal data is used in practice - such as in targeted advertising. To support both privacy and innovation, the definition of "targeted advertising" should avoid overly broad restrictions that could hinder reasonable data use. A balanced approach should: (1) permit ads based on consumer preferences derived from data collected over time and across third party sites; and (2) include clear 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 avoiding unduly burdensome disclosure requirements that disrupt business operations or overwhelm consumers with redundant notices. The law should:

- Focus on high-risk data uses, requiring enhanced notices only where there is real potential for consumer harm.
- Avoid one-size-fits-all mandates, allowing startups, smaller businesses and Middle Tech companies to scale disclosures based on risk and data sensitivity.
- Minimize redundant pop-ups and consent fatigue, emphasizing quality over quantity of disclosures.
- Require notices to include key information: categories of data collected, how it's used or shared, and consumers rights.

Notices should be both consumer-friendly and practical for businesses — i.e., written in plain language, easy to navigate, and structured to highlight the value of data use where appropriate.

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 balance the needs of both consumers and businesses alike. Key components to achieving this include:

- **Right to access** - Consumers can confirm whether a business processes their data without unnecessary bureaucratic hurdles.
- **Right to correction** - Individuals can request corrections to inaccurate personal data, taking into account the nature of the personal data and processing purposes, ensuring reasonable, business-friendly compliance standards.
- **Right to deletion** - Consumers can request deletion of data collected directly from them, incorporating necessary exceptions and avoiding mandates that

require businesses to erase operationally necessary data or pass on data deletion signals to third-parties.
- **Right to portability** - Businesses should provide personal data provided directly by the consumer in a portable format to the individual when technically feasible and commercially reasonable.
- **Right to opt-out of targeted advertising** - Consumers can opt out of third-party targeted ads, but not routine analytics or internal data processing, ensuring businesses can still provide personalized services and improve operations.

As for enforcement, a federal privacy law should ensure strong consumer protection while preventing abusive litigation that has a disproportionate impact on startups, smaller businesses and Middle Tech companies. The law should adopt a shared enforcement model between the FTC and sectoral regulators, and not allow for private rights of action. (More on this in section ***VI. Accountability and Enforcement*** below.)

Further, it should provide safe harbors for good-faith compliance to ensure that businesses that take reasonable steps to comply have a clear, structured opportunity to remedy unintentional violations before facing penalties. (More on this in ***III. Existing Privacy Frameworks and Protections***, ***IV. Data Security*** and ***VI. Accountability and Enforcement*** below).

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

A federal privacy law should take a risk-based approach, preventing misuse of sensitive data while allowing businesses to process necessary data for security, fraud prevention, and innovation. Specifically, it should:

- Limit heightened protections to high-risk uses of sensitive data.
- Require explicit consent only for sensitive data processing and processing inconsistent with the purposes of collection.
- Avoid excessive consent requirements that disrupt user experience or create compliance hurdles for routine, low-risk business functions.
- Ensure consent mechanisms align with VCDPA's opt-in requirements for sensitive data.
- Require consent to avoid Big Tech using data collected via one product or service for a very different and unrelated product or service without clear consumer notice and consent.

III. 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 privacy frameworks while avoiding their unintended consequences. Two key models to consider are the EU's *General Data Protection Regulation* (GDPR) and the VCDPA.

The GDPR has set a global benchmark for privacy protections, providing strong consumer rights, clear data processing principles, and requirements for transparency and accountability. Additionally, its risk-based approach tailors compliance requirements based on data sensitivity and processing impact, rather than imposing a one-size-fits-all

mandate.

Many Middle Tech companies already operate globally and have invested significantly in GDPR compliance, meaning they have existing infrastructure and practices in place to support strong privacy protections. These efforts can and should be leveraged in the U.S. context.

However, the GDPR's complex and prescriptive requirements have led to excessive compliance costs, disproportionately impacting startups, smaller businesses, and Middle Tech companies. The regulatory burden has, in practice, helped entrench Big Tech, as larger firms are better positioned to absorb legal and operational costs, while smaller companies struggle to meet the same standards.

This challenge is recognized across the policy spectrum in Europe. There is broad consensus that certain aspects of GDPR require reform, and the regulation will be included in an upcoming omnibus simplification package, with a focus on easing burdens for smaller players.[2] This underscores the importance of calibrating privacy frameworks to support innovation and competition without compromising strong privacy protections. The VCDPA incorporates many of the GDPR's strongest protections while avoiding some of the GDPR's pitfalls. Key advantages of the VCDPA that would warrant inclusion in a federal privacy law, include:

- **Risk-Based, Business-Friendly Approach:** Compliance measures are proportional to data sensitivity, ensuring businesses that process low-risk data are not burdened with unnecessary regulations.
- **No Private Right of Action:** This prevents excessive litigation, reducing legal uncertainty and compliance costs, while still ensuring strong enforcement through regulatory authorities.
- **Opportunity to Cure:** Businesses have 30 days to remedy alleged violations after receiving notice from the Attorney General, promoting good-faith compliance and reducing the risk of punitive enforcement.
- **Flexible and Innovation-Friendly:** This avoids overregulating routine business activities and allows for industry-led best practices, ensuring that privacy protections evolve alongside technology.

A federal privacy law should blend the GDPR's strong consumer protections and risk-based approach with the VCDPA's flexibility and business friendly design. This balanced model would safeguard privacy while fostering innovation and economic growth.

Finally, a federal law should include carve-outs for data processing already subject to industry-specific privacy regulations (e.g., *Health Insurance Portability and Accountability Act* (HIPAA), *Gramm-Leach-Bliley Act* (GLBA), *Fair Credit Reporting Act* (FCRA)). Instead of layering on duplicative compliance burdens, the law should recognize existing frameworks as sufficient and allow appropriate industry regulators to maintain oversight. (More on this in ***D. Harmonizing Federal Privacy Law with Existing Sectoral Protections*** below)

---

[2] See European Commission, "Commission proposes to cut red tape and simplify the business environment," 26 February 2025, https://commission.europa.eu/news/commission-proposes-cut-red-tape-and-simplify-business-environment-2025-02-26_en.

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 bureaucratic nightmare, effectively acting as an unsustainable tax on Middle Tech companies. These businesses may spend millions navigating duplicative and often conflicting state regulations.

Regulatory fragmentation also harms businesses that rely on technology — the majority of the American economy — weakening America's competitive edge. A patchwork of conflicting state laws creates confusion and undermines consumer trust, making it harder for people to understand their rights. A clear, national standard will enhance consumer protection while preventing excessive government interference in business operations.

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 a patchwork of conflicting regulations that lead to uneven consumer rights and impose costly burdens on startups, small businesses, and Middle Tech companies. Partial pre-emption would preserve this fragmentation and uncertainty and should be avoided.

A strong national law would give businesses clarity, reduce compliance costs, and support innovation - while ensuring all Americans receive the same level of privacy protection. It would also promote consistent, transparent user experience, building consumer trust.

Just as the Internet, telecom, and financial sectors benefit from clear federal rules, privacy law should follow suit to advance economic growth and U.S. competitiveness - especially for companies that rely on technology to succeed.

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 sectoral laws like HIPAA, FCRA, GLBA, and COPPA, rather than override or create conflicting obligations.[3] To harmonize regimes and prevent duplicate compliance burdens, it should:

- Maintain sectoral exemptions for existing federal laws.
- Clarify that when a sectoral law governs specific data processing activities, its requirements take precedence over the general federal privacy law.
- Align data rights and transparency obligations to avoid duplication.

The FTC should serve as the primary enforcer of a national privacy framework, ensuring consistent enforcement across industries that do not already have dedicated privacy regulators. A single, predictable enforcement structure:

[3] Note that whereas we recommend 'full preemption' with respect to state privacy laws, we advocate for harmonization at the federal level between a federal privacy law and sectoral laws.

- Provides clear, uniform national rules, reducing compliance uncertainty for businesses.
- Streamlines enforcement, preventing a costly and confusing patchwork of overlapping state and federal regulators.
- Keeps enforcement focused on real consumer harms, rather than turning privacy law into a battleground for politics or selective enforcement.

For industries already subject to sectoral privacy laws, existing federal regulators — e.g., the Department of Health and Human Services (HHS) (for health data under HIPAA), the Consumer Financial Protection Bureau (CFPB) (for financial privacy under GLBA), the Federal Communications Commission (FCC) (for telecom data), etc.) — should retain their enforcement authority while ensuring that sector-specific rules remain consistent with the broader national privacy framework. (More on this in ***VI. Accountability and Enforcement*** below)

IV. Data Security

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

To improve data security for consumers, a federal privacy law should:

- Maintain the well-established 'reasonable security' standard, which requires organizations to implement safeguards appropriate to the nature and sensitivity of the data and the context in which it is processed.
- Encourage the FTC to provide additional guidance on what constitutes reasonable security practices, tailored to the type of data and the purposes of processing.
- Emphasize data minimization as a foundational principle - limiting the collection, use, and retention of personal data reduces the overall risk surface and strengthens security outcomes.
- Support public-private collaboration to promote innovation and market-driven solutions to cybersecurity challenges.
- Allow for flexibility so that organizations can adopt security measures proportionate to their size, resources, and risk exposure.

Security obligations should remain technology-neutral and scalable, ensuring that startups, smaller businesses and Middle Tech companies are not overburdened, while still maintaining high standards for entities processing sensitive or high-risk data. A proportional approach also promotes international interoperability and trust in the global economy.

Finally, a uniform federal breach notification standard should replace the current state-by-state patchwork. Consumer notifications should be required only for significant breaches that pose a real risk of harm, preventing unnecessary panic and compliance costs tied to minor incidents.

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 data privacy and security law should pre-empt state AI regulations to prevent a

costly, fragmented compliance landscape. Conflicting state rules on automated decision-making, transparency, and risk assessments drive up costs, hinder AI adoption, and create legal uncertainty — weakening U.S. competitiveness.

To harmonize AI-related privacy protections, the U.S. should prioritize industry collaboration, flexible guidelines, and global alignment. Policymakers should work with industry stakeholders to establish voluntary AI governance best practices rather than imposing rigid, one-size-fits-all regulations.

A federal privacy law should clearly define the scope of automated decision-making using AI systems that would trigger consumer opt-out rights. In this context, "AI decisions" refer to outcomes generated through automated decision processing - often using machine learning or other AI techniques - that rely on personal data to make individualized predictions, classifications or determinations.

Importantly, Congress has an opportunity to appropriately align what constitutes a high-risk automated decision. While Virginia's privacy law is an effective model for data privacy - its definition of "decisions that produce legal or similarly significant effects concerning a consumer" was not intended nor should it extend to AI or other automated decisions. Doing so would label entire sectors such as "financial services" and "healthcare" as high risk and apply strict requirements to many low or no risk use cases. This could deprive consumers of beneficial AI powered products and services. Additionally, routine AI-driven functions, such as personalization, advertising, fraud detection, and content recommendations, should not trigger opt-out requirements.

To support startups, smaller businesses, and Middle Tech companies, the law should establish safe harbors exempting them from complex AI compliance mandates unless they engage in high-risk AI decision-making, such as biometric surveillance or predictive hiring. It should exclude private rights of action in the AI context as well, and ensure enforcement remains with expert agencies, particularly the FTC and relevant sectoral regulators.

The law should standardize data protection assessments (DPAs) for AI, limiting requirements to high-risk AI models. Businesses that follow industry-recognized AI risk management standards, such as the NIST AI Risk Management Framework, should be deemed compliant, reducing regulatory uncertainty.

AI transparency obligations should focus on general decision factors, not proprietary algorithms, ensuring clarity without exposing trade secrets. Algorithmic fairness audits should apply only to high-risk AI applications to prevent unnecessary compliance burdens.

NIST should be responsible for developing flexible AI guidelines, modeled after the widely adopted NIST Cybersecurity Framework, allowing businesses to implement risk-based, tailored compliance measures. Additionally, U.S. AI privacy laws should align with international frameworks, such as the OECD AI principles, to support American businesses in global markets. A flexible, industry-driven, and innovation-friendly AI governance framework will ensure U.S. leadership in AI development while maintaining consumer protections.

VI. Accountability and Enforcement

Internet Works advocates for a shared enforcement model where the FTC has primary oversight, while sectoral agencies retain enforcement authority within their respective

jurisdictions. The FTC would be well-positioned to take a comprehensive approach to compliance, considering not only enforcement of consumer privacy concerns, but balancing those interests against other considerations like free speech. A new separate privacy enforcement agency may not be as likely to consider these broad and sometimes competing considerations.

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

Benefits

- Regulatory consistency and predictability
  - Businesses can comply with a unified federal framework, reducing the risk of conflicting interpretations across different enforcement agencies.
  - The FTC, in coordination with sectoral regulators, can provide clear guidance on compliance expectations.
- Balanced, expertise-driven enforcement
  - The FTC ensures broad oversight while sectoral agencies (e.g., HHS for health data, CFPB for financial data, FCC for telecom data) retain jurisdiction-specific enforcement to address sector-specific risks and requirements.
- Prevention of politicized enforcement
  - Keeping enforcement at the federal level (FTC + sectoral agencies) prevents state Attorneys General from using privacy laws selectively to target businesses based on political motivations.
  - A coordinated federal approach enhances legal certainty and prevents regulatory overreach.
- Reduced compliance costs for businesses
  - Eliminates duplicative audits, redundant investigations, and inconsistent state-level enforcement.
  - Businesses can focus on innovation and growth rather than navigating overlapping privacy enforcement regimes.
- Focus on real harms, not technical violations
  - The FTC and sectoral regulators should prioritize enforcement against bad actors engaging in deceptive practices or harmful data misuse, rather than penalizing technical infractions that do not pose significant consumer risks.

Costs

- Potential for overlapping jurisdictions
  - Some gray areas may arise where multiple federal agencies have jurisdiction over a case, requiring strong interagency coordination to avoid conflicting enforcement.
    - Solution: The law should mandate formal coordination mechanisms between FTC and sectoral agencies to streamline enforcement.
- Risk of bureaucratic complexity
  - A shared model may require more structured communication and coordination between agencies to avoid delays or inefficiencies.
    - Solution: Agencies should implement memorandums of understanding (MOUs) and regular reporting requirements to ensure efficient enforcement without unnecessary bureaucracy.
- State Attorneys General may still attempt to intervene
  - Even with clear federal pre-emption, some state AGs may attempt to assert enforcement authority.

- Solution: The law should limit state AG involvement to cases where federal agencies fail to act or where states coordinate under clear federal guidelines.

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?

To ensure fair, predictable, and effective enforcement, the FTC should have:

- Clear authority to issue guidance and enforcement policies, ensuring businesses understand their compliance obligations.
- Technical expertise in privacy and data security investigations, enabling proactive enforcement against emerging cyber threats.
- Resources to conduct risk-based investigations, focusing on bad actors rather than imposing excessive scrutiny on compliant businesses.

Sector-specific agencies should retain enforcement authority over privacy and security issues specific to their regulated 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. 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, startups, smaller businesses, and Middle Tech companies 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.

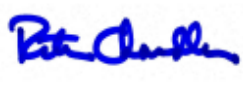
CONCLUSION

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.

Internet Works 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.

Respectfully submitted,



Peter Chandler
Executive Director, Internet Works
https://www.theinternet.works/