Issue One & Issue One Action
1401 K Street NW, Suite 350
Washington, DC 20005

Liana Keesing, *Policy Manager*
lkeesing@issueone.org

ISSUE ONE RESPONSE TO HOUSE ENERGY & COMMERCE REQUEST FOR INFORMATION ON FEDERAL COMPREHENSIVE DATA PRIVACY & SECURITY

Issue One welcomes the opportunity to respond to the House Energy and Commerce Committee's Request for Information on developing a comprehensive federal data privacy and security framework. As a nonpartisan nonprofit committed to strengthening American democracy, we advocate for strong data privacy protections rooted in data minimization principles. A healthy democracy requires that citizens have control over their personal information and are safeguarded from undue influence enabled by unchecked data collection.

I. ROLES AND RESPONSIBILITIES IN THE DIGITAL ECONOMY

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?

A federal comprehensive data privacy law must include strong definitions that distinguish between controllers, processors, and third parties while limiting possible exemptions. We recommend that a "controller" should be defined as "a person who, alone or jointly with others, determines the purpose and means of processing personal data," while a "processor" should be defined as "a person that processes personal data on behalf of a controller." These definitions align, with minor wording variations, with key state data privacy laws in Kentucky, Texas, Virginia, California, Maryland, and New Jersey. Similarly, a third party should be defined, at a minimum, as "a person other than the consumer, the controller, the processor, or an affiliate of the controller or processor," as established in the Texas Data Privacy and Security Act. Kentucky's data privacy law further strengthens this definition by explicitly stating that a third party is "a natural or legal person, public authority, agency, or body other than the consumer, controller, processor, or an affiliate of the processor or the controller."

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

Data minimization is essential for a strong federal data privacy law. Controllers, for example, should be required to minimize data collection, processing, and transferring to only what i*s reasonably necessary* for the product or service that an individual specifically requests. The Maryland Online Data Privacy Act provides a model for this standard. Moreover, a strictly necessary standard for controllers should be created for sensitive data such as biometric, genetic, and precise geolocation information. Controllers, on the other hand, should be required to delete personal data after the data is no longer necessary in order to prevent misuse and breaches. Finally, transfers of sensitive data to third parties (other than to processors) should be prohibited unless the transfer is strictly necessary and done with affirmative opt-in consent.

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

While we are not generally supportive of numerical thresholds for compliance—because they often result in arbitrary cutoffs that encourage avoidance strategies—we also believe strongly that small businesses should not be unduly burdened by requirements that hinder their ability to compete and provide essential services. Nebraska and Texas, for example, create separate compliance regimes for small businesses, as defined under the federal Small Business Act. For example, small businesses should not be subject to extensive audits, requirements to establish certain positions within their corporate structure, to implement enterprise-grade security measures, or to conduct comprehensive impact assessments or other forms of documentation. Still, small businesses that process sensitive data should not be exempt from regulations for that data, as the risks associated with sensitive information do not decrease based on the size of the business.

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."

"Personal information" should be defined as "information that identifies, or is linked or reasonably linkable to, an identifiable individual," including unique identifiers, online identifiers, and persistent identifiers. Crucially, this definition recognizes that even seemingly non-identifying data can be combined to accurately identify individuals. Several key states, including Texas, Virginia, California, Kentucky, and New Jersey, have adopted similar definitions.

"Sensitive personal information" should be understood as data that, if misused or exposed, could result in significant harm, discrimination, or intrusion into an individual's private life. This includes, but is not limited to, financial information, health data, biometric and genetic data, precise geolocation, government-issued identifiers (such as Social Security numbers), information about children, and data revealing race, ethnicity, religious beliefs, and other protected classes. Several state and federal legislative efforts, including the original American Data Privacy Protection Act (H.R. 8152), recognize these categories as warranting heightened protection.

Given our particular focus on national security, we consider protections for sensitive data to be essential for protecting members of the armed forces and intelligence communities. Data brokers compile extensive dossiers on Americans, including members of the armed forces. Research from Duke University, for example, has shown that data brokers sell sensitive information about active-duty military members, veterans, and their families for as little as $0.12 per record. Given these risks, any national security-relevant information—including military service records, data that could facilitate foreign influence operations, and political beliefs or affiliations when used for targeted political messaging—should be classified as sensitive.

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

Privacy disclosures should include just-in-time notices at the point of data collection, presented in plain language with layered privacy policies in a standardized, machine-readable format. Companies should be required to clearly state data retention periods, specific processing purposes—while prohibiting vague, open-ended language—and policies on third-party transfers. These disclosures should detail the categories of personal information collected, including sensitive data, the purposes for which it is used, whether the information is sold or shared, and the length of time each category of data will be retained. If a business sells or shares personal information, it should provide a clear link to a Notice of Right to Opt-out of Sale/Sharing, as well as a link to its full privacy policy.

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?

A comprehensive data privacy and security law should include key consumer protections such as the right to access personal information in a machine-readable format, correct inaccuracies, request deletion with limited exceptions, transfer data between platforms, and opt out of targeted advertising and profilings. Moreover, a strong data minimization framework should limit data collection, processing, and transfers to what is reasonably necessary for the requested product or service or a clearly defined, enumerated permissible purpose. Consent should only be relied upon in limited, appropriate circumstances, as it is often undermined by dark patterns, lengthy privacy policies, and imbalanced power dynamics that prevent individuals from making truly informed or voluntary choices. Controllers should be required to delete personal data once it is no longer necessary, and strict limits should be placed on the collection and processing of sensitive data—such as biometric, genetic, and precise geolocation information—under a "strictly necessary" standard. Secondary processing and transfers should generally be prohibited, with narrow exceptions, and transfers of sensitive data to third parties should be allowed only when strictly necessary and with affirmative opt-in consent. The sale of sensitive data can pose a national security threat by creating a market that allows foreign adversaries to access Americans' personal information. To prevent this risk, the sale of sensitive data should be prohibited. Additionally, processors must be explicitly barred from secondary data use or combining data from multiple sources. Moreover, processors should be explicitly barred from engaging in secondary uses or combining data from multiple sources.

Additionally, to ensure meaningful individual rights, companies should be required to honor universal opt-out signals, and deletion rights should apply to all data connected to a consumer, not just data collected directly from them. Importantly, companies should not be allowed to collect personal data under the guise of providing discounts or perks and then sell it for profit. Moreover, a federal standard should prohibit discrimination against consumers who exercise their privacy rights, ensuring businesses cannot charge higher prices to those who opt out of targeted advertising.

Finally, enforcement should be robust and multi-layered. State Attorneys General should play a critical role in this framework, serving as frontline enforcers who can address violations swiftly and hold companies accountable at the state level. Their ability to investigate and take action against noncompliance is crucial for ensuring that privacy rights are upheld across diverse jurisdictions. This mechanism has already been successful for enforcing state-level legislation; Texas AG Ken Paxton has emerged as a leader in prioritizing consumer privacy. Beyond state AGs, the Federal Trade Commission (FTC) should have rulemaking authority and the power to impose civil penalties, and a limited private right of action should be available for data breaches and willful violations.

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

As discussed above, the collection, processing, and transfer of sensitive personal information should be subject to heightened protections, including the requirement for explicit, affirmative consent from individuals. Dark patterns, or manipulative design intended to subvert consumer choice, must be prohibited in both the definition of consent and provisions granting consumer rights. Design choices that intentionally discourage consumers from exercising their privacy rights undermine the core purpose of privacy laws, which is to empower individuals. Sensitive information should be handled with additional safeguards, such as explicit consent requirements for its collection, transfer, and processing, as well as prohibitions on sharing this data with data brokers without express consent. There should be strict limitations on data usage, with purpose restrictions that prevent misuse, enhanced security measures like encryption and access controls, and automatic deletion once the purpose for which the data was collected is fulfilled. Additionally, there should be a ban on targeted advertising directed at children, ensuring that minors are not exposed to personalized ads that take advantage of deceptive data collection practices.

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.

Maryland's Online Data Privacy Act provides the strongest model for federal legislation due to its emphasis on data minimization over the flawed notice-and-consent approach, which allows businesses to list any purpose they choose in privacy policies, knowing that few consumers will read them. The act includes several critical protections, such as heightened safeguards for sensitive data, a ban on the sale of sensitive data, a prohibition on targeted advertising to minors under 18, and a restriction preventing controllers from requiring consumers to consent to the sale of their personal data as a condition of participating in loyalty programs. Additionally, it grants consumers the right to obtain a specific list of third parties to whom the controller has disclosed either their personal data or personal data more broadly and notably does not exempt pseudonymous data. In contrast, while the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) offer certain protections, they place an excessive burden on consumers to navigate complex opt-out mechanisms across numerous entities. Maryland's approach, by comparison, correctly imposes affirmative obligations on companies to limit data collection.

The Texas Data Privacy and Security Act also contains a number of strong provisions, particularly through its empowerment of the AG and its use of a universal opt-out signal provision, which requires controllers to honor authenticated consumer requests to opt out of targeted advertising, personal data sales, or profiling that leads to legal or similarly significant effects. Additionally, several states—including Texas, Virginia, Kentucky, Iowa, Utah, Tennessee, Nebraska, and Montana—have enacted transparency provisions and data protection impact assessments. These measures require documentation on what personal data is collected, why it is collected, how it is used, transferred, or sold, and what risks and benefits the collection presents to consumers. Further, they mandate an explanation of why the benefits outweigh the risks, how those risks are mitigated, and an evaluation of alternatives to profiling, including why the controller rejected those alternatives. However, as mentioned previously, we strongly recommend that these requirements only apply to larger or high-risk companies.

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.

U.S. privacy protections remain highly fragmented at the state level. As of 2025, twenty states have enacted comprehensive privacy laws, each offering varying levels of consumer protection. This patchwork of regulations creates significant compliance challenges for companies operating nationally or globally, forcing them to navigate inconsistent requirements across jurisdictions. These administrative burdens increase costs, discourage innovation, and heighten the risk of inadvertent violations. A federal standard would establish uniform protections for all Americans, ensuring that privacy rights are not determined by geography. While some states have enacted strong privacy laws, residents in up to thirty states remain largely unprotected. Additionally, the complexity of complying with multiple state laws places a disproportionate burden on small and medium-sized businesses, which often lack the resources to manage compliance, while large tech companies can afford to spend millions annually on regulatory navigation. A unified strong federal privacy standard would reduce compliance costs, encourage innovation and small business growth, and strengthen privacy protections nationwide.

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?

Every American deserves a strong, baseline standard of data privacy to protect their rights as both consumers and citizens. Issue One supports a strong comprehensive federal standard—rooted in data minimization principles—that would set a national ceiling while allowing states to enact additional protections in specific areas such as student privacy and biometric data. A uniform standard would prevent the burden of navigating fifty different state laws, which primarily benefits large technology companies like Google, Amazon, and Meta that can afford the high compliance costs of a fragmented regulatory landscape.

However, we recognize that achieving a strong national ceiling may be challenging. Therefore, we would also consider supporting a floor preemption approach, which would establish baseline protections for all Americans while allowing states to introduce additional consumer safeguards. Regardless of the approach, if a federal data privacy law includes preemption, it must be stronger than existing state laws to justify overriding them.

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

While this is somewhat outside our direct focus, it is critical that any federal framework maintains consistency in definitions and protections across various privacy statutes, preventing loopholes and unnecessary fragmentation. Existing laws like HIPAA, FCRA, GLBA, and COPPA each serve distinct purposes, but they lack comprehensive measures that are applicable to all consumers. Any federal law must establish clear regulatory coordination requirements between the FTC and other agencies with privacy jurisdiction to prevent enforcement gaps and ensure effective oversight across industries.

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?

Although this is generally outside the scope of Issue One's work, a federal data privacy law should enhance consumer data security by requiring encryption for sensitive data, access controls, regular security assessments, and incident response planning. It should mandate security-by-design principles, breach notifications within standardized timelines (e.g., 72 hours to regulators, seven days to individuals), and third-party security audits for entities handling sensitive information. Incorporating adaptable standards like the NIST Cybersecurity Framework could help ensure compliance, while recognizing data minimization as a fundamental security measure will reduce the risk of breaches by limiting unnecessary data collection and retention.

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?

Issue One has not traditionally focused on state-level AI frameworks. Still, it is possible to both have transparency in decision-making and data collection. Techniques like pseudonymization and synthetic data can help mitigate risks by enabling system-level testing for biases and vulnerabilities without exposing real personal data. However, the use of sensitive data in automated decision-making systems presents significant risks—both in terms of privacy and security. Any federal framework should acknowledge these risks and ensure that sensitive data is handled with the highest level of protection to prevent misuse, discrimination, and breaches.

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.

Expert agency enforcement provides benefits including technical expertise, ability to issue evolving guidance, consistent enforcement across jurisdictions, and resources for technical investigations. However, potential costs include the risk of regulatory capture, shifting enforcement priorities between administrations, resource constraints, and delayed justice for consumers.

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 receive APA rulemaking authority for privacy and data security standards, first-instance civil penalty authority without requiring prior consent orders, a dedicated privacy and security division with technical experts, increased funding for privacy enforcement, and algorithmic auditing capabilities to evaluate the use of data in automated systems.

Importantly, state AGs should have parallel enforcement authority, allowing them to take action against data privacy violations in their respective states. These AGs should also receive technical assistance from the FTC to tackle complex investigations, ensuring that smaller offices are equipped with the expertise needed to address cutting-edge privacy concerns. Moreover, multistate coordination mechanisms should be established to allow states to work together efficiently, sharing resources and strategies to address national violations of privacy laws. The work of AGs, such as Texas Attorney General Ken Paxton, exemplifies how state-level enforcement can be highly effective. Paxton's office has demonstrated a proactive and impactful approach, often outpacing broader frameworks like the California Consumer Privacy Act (CCPA) in addressing violations.

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

A safe harbor can be beneficial by providing clear guidelines for compliance and reducing uncertainty for businesses, encouraging proactive data privacy and security practices. However, it can also be harmful if it is filled with loopholes, too slow to adapt to emerging technologies, or creates a false sense of security for consumers. Additionally, safe harbors may limit accountability and face regulatory challenges, potentially undermining the effectiveness of data protection efforts.

VII. ADDITIONAL INFORMATION: NATIONAL SECURITY AND DEMOCRATIC INTEGRITY CONSIDERATIONS

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

For too long, technology giants have dominated the digital marketplace, limiting consumer choice and stifling competition from small businesses. Dominant platforms trap valuable consumer data within "walled gardens," preventing startups from building innovative products and ultimately hindering consumer choice. The biggest companies have the widest market share – their extensive reach allows them to collect and aggregate data across multiple platforms, leaving business owners at a disadvantage. Crucially, these data monopolies can push lower quality products with fewer privacy protections, while advertising their products are safe and trustworthy. Data privacy provisions would limit powerful companies' overwhelming control over the market by allowing users to take their personal data and transfer it between platforms, empowering consumers through choice. Unfortunately, data companies argue that user data is proprietary or too cumbersome to individualize. As a result, they advocate for the status quo: notice and consent. However, notice and consent regimes encourage the biggest companies to continue to hoard personal data, promoting a race to the bottom, where consumers are left with no choice but to use the platforms with the weakest privacy protections. The largest data holders have demonstrated a systemic inability to prioritize data safety and privacy over profit, with little transparency over how data is used and where it is stored.

Still, through innocuous internet activity such as social media or gaming, Americans are unwittingly revealing sensitive information about themselves to malicious actors. Mindless games like Candy Crush use behavioral data on users' habits, friends, and interests to create eerily detailed user profiles, such as fitness level or location, used for targeting advertisements or enhancing user engagement. Additionally, the popular fitness app Strava was found to inadvertently reveal the locations of President Trump, former President Biden, and other world leaders through tracking the habits of their bodyguards in a simple user heat map. Foreign adversaries have a demonstrated interest in collecting American data. China, Russia, and Iran have all carried out widespread attacks on our cyberspace, both covert and overt, in the interest of acquiring as much data as possible. While there are restrictions on foreign adversary-affiliated companies acquiring and selling American user data, there is no restriction on regular firms selling to foreign adversaries — a critical shortcoming. Effective data privacy legislation needs to include data minimization provisions and explicit protections for sensitive data to ensure American identities are protected from theft, fraud, or manipulation. Companies need to be held to higher standards when holding sensitive information, this means limiting how much and for how long personally identifiable data can be retained, and implementing strong security measures for information like social security numbers, health records, and biometric identifiers. The industry as a whole is the culprit, leveraging their economic and political might to evade proper responsibility for failing to protect users.