Comments of the Software & Information Industry Association

House Committee on Energy & Commerce
Privacy Working Group Request for Information

April 7th, 2025

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments to the Privacy Working Group's request for information on federal privacy legislation. SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 380 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, and one essential to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of data privacy practices. For many years, we have engaged extensively with Congress to provide stakeholder input on past legislative efforts, including the *American Data Privacy Protection Act* (ADPPA) and the *American Privacy Rights Act* (APRA). We are hopeful about the potential of the Working Group to generate a draft that can realize the goal of a national consumer privacy law.

We appreciate the goals of the Working Group and the Committee's careful attention to the efficacy and potential unintended consequences of overly prescriptive requirements. In this submission, we emphasize the need for a preemptive federal privacy law to promote consistency for consumers, uniformity and efficiency for U.S. companies, and clarity for both American citizens and businesses. Regulation must balance the interests of guaranteeing that Americans' consumer data is protected, while maintaining thoughtful rules of the road that continue to promote innovation and competitiveness for domestic companies endeavoring to comply in good faith.

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?

It is important for a comprehensive privacy framework to clearly define and separate the roles and requirements for data "controllers" and data "processors" (the latter are also sometimes referred to as "service providers"). The Virginia privacy law defines controllers as entities that determine the purposes and means of processing.[1] It defines processors (or service providers) as entities that process data on behalf of these controllers, but do not determine such purposes and means.[2]

From a consumer protection standpoint, therefore, processors need not retain the same direct obligations to data subjects (*i.e.*, access, correction, and deletion). Further, from a technical perspective, processors are often unable to assess a controller's purposes of processing – at least not without that controller counterproductively sharing with them even more data.

Despite this caveat, both controllers and processors can and should be responsible for their own internal cybersecurity measures designed to secure consumers' personal data.

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

A comprehensive federal consumer privacy law must exist alongside existing federal privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley Act (GLBA), and the Family Educational Rights and Privacy Act (FERPA), and the Fair Credit Reporting Act (FCRA). As discussed in more detail below, entities subject to these laws may require entity-level or data-level carveouts in the interest of operational feasibility while complying with a federal privacy framework.

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

[1] *See* Va. Code Ann. § 59.1-575.
[2] *See Id.*

In line with how U.S. privacy laws are typically scoped at the state level, we would recommend that to be subject to a federal privacy framework, controllers or processors should control or process 1) the personal data of at least 100,000 consumers in a calendar year, or 2) the personal data of at least 25,000 consumers. These entities should also derive over 50 percent of gross revenue from the sale of that data.[3] In drafting their own privacy laws, most states have recognized correctly that covering smaller entities within the scope of the law risks burdening startups and innovators with a proportionally overbearing compliance burden. Rather than protecting consumer data, this risks simply locking in larger entities that can afford the cost of compliance, while restricting the domestic development of innovative data-driven technologies at an early stage.

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."

Publicly available information (PAI). It is imperative that a federal privacy framework respects the bounds of the First Amendment. To that end, it should exempt publicly available information, as well as inferences derived solely from PAI. Within this exemption, a federal law should further clarify that such inferences from PAI remain protected under the First Amendment even if they happen to reveal data that could be defined as "sensitive data" in other contexts (*i.e.*, a public official's health condition). Lastly, it is important to specify that temporarily combining PAI with personal data, or even sensitive data, does not remove the PAI's subsequent protections when it is no longer included in this combined dataset.[4]

Personal information. At a high level, a federal privacy law should be scoped based on a risk-based approach. Therefore, the framework should focus on protecting the personal data of "consumers." This should not include individuals acting in an employment or a commercial context. Data collected in employment and commercial contexts are distinct and the risks of misuse dramatically lower than those faced by consumers who are potentially exposed to unscrupulous actors online. Further, collection in these contexts is often necessary as a matter of course, and imposing equivalent compliance requirements as exists for consumers would be incredibly burdensome to businesses and employees alike. As such, a federal consumer privacy law should make clear that these contexts are specifically excluded from the scope of the law.

[3] *See Id.* at § 59.1-576.

[4] *See* SIIA, *SIIA Releases Memo on First Amendment Protections for Publicly Available Information* (Apr. 4, 2025), https://www.siia.net/siia-releases-memo-on-first-amendment-protections-for-publicly-available-information/.

Sensitive personal information. In general, a federal privacy law should define sensitive data to include 1) consumer health data, 2) precise geolocation data, 3) biometric data, and 4) kids' data. The scope of these definitions should map to emerging norms in U.S. state privacy law, which are in turn focused on the risk of misuse and consumer harm within these data categories.

Consumer health data. This should be treated as a single definition and scoped to any data that the controller uses to identify a health condition.[5] This is the data set that presents a unique risk to consumers if misused. Note that this is distinct from a carveout for the HIPAA data, as discussed later in this submission.

Precise geolocation data. Because the heightened risk to consumers of processing this data occurs in the context of real time identification of a consumer's location, a federal privacy law should scope this definition accordingly. Emerging norms in U.S. state privacy laws typically restrict this definition to data that is derived from a technology, such as GPS, that directly identifies the specific location of an individual within 1,750 feet.[6]

Biometric data. Due to heightened risk, biometric data should be scoped, as it is typically defined at the state level, to automated measurements of an individual's biological characteristics that are used to identify a specific individual, or used to reveal something sensitive about the individual. The definition should also include two additional caveats to render it workable, which are also present in state law. First, the definition should include an exemption for physical or digital photographs, video or audio recordings or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.[7] Second, the definition should address that opt-in consent in the context of biometric data can, in certain cases, be implied *if* the consumer provides biometric data to a controller in the course of using a product, service or feature. However, implied consent should only exist where the processing of this data is consistent with the consumer's reasonable expectations in using the application.

Kids' data. A federal privacy law should provide a single preemptive standard for children's privacy throughout the nation. This standard should be guided by prevailing approaches in the states. This includes the scope of "kids' data" considered sensitive, which should be defined as

[5] *See* Va. Code Ann. § 59.1-575.
[6] *See Id.*
[7] *See Id.*

personal data collected from a known child.[8] For consistency, a "child" should be defined as a person under the age of 13, and "known" in this case should be defined as actual knowledge.[9]

At the same time, a federal privacy framework should avoid incorporating elements of state laws currently being challenged in the courts. In addition to addressing topics fundamentally outside the remit of consumer privacy, these content-based restrictions do not represent the consensus of kids' protections at the state level, and implicate several significant constitutional infirmities. Chief among these is a First Amendment challenge, as these laws restrict kids from receiving speech online. As a policy matter, these laws also paradoxically prevent online platforms from offering age-appropriate content to children by restricting the collection and protection of children's data, and thus the tailoring of kids' content to children's profiles. In fact, they would impact products and services available online even to adults by effectively forcing the takedown of "harmful content," while leaving the interpretation of what constitutes "harm" to regulators.

We encourage the Working Group to engage with the Committee on Education and Workforce to understand the existing protections and guardrails established by FERPA for the use of student data.

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

As is consistent with emerging norms in U.S. state general consumer privacy laws, a federal privacy framework should require U.S. businesses to disclose 1) the categories of personal data collected by a company, 2) the purposes for which such data is used, 3) the categories of personal data shared with third parties, and 4) the categories of third parties with whom that data is shared, and how consumers may exercise their rights under the law be made in a "reasonably accessible" and "clear" privacy notice.

However, federal privacy legislation should avoid unduly specific mandates beyond these requirements. Overly granular requirements risk rapidly becoming irrelevant or obsolete, and restrict businesses' — especially small businesses' — flexibility to leverage new technologies to increase transparency. Further, specific requirements rarely provide additional transparency due to consumer confusion and "notice fatigue." For example, Washington state's *My Health, My Data Act* (MHMDA) implemented a requirement for businesses to provide multiple types of

[8] *See Id.*

[9] *See Id.* at § 59.1-580.

privacy notices.[10] Rather than increasing transparency, this has resulted in widespread consumer confusion and even required several clarifications to be issued by the Attorney General's Office in that state.[11]

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?

In general, SIIA recommends that the Working Group consider two categories of consumer protections to include in a comprehensive data privacy and security law. First, the law should include procedural data minimization requirements while avoiding substantive minimization requirements. Second, the law should give U.S. consumers clear and consistent consumer rights to their personal information.

Data minimization. Data minimization is the principle that data collection should be limited to only what is required to fulfill a specific purpose, and has both procedural and substantive components. Procedural data minimization, which is a hallmark of both European Union and United States privacy law, focuses on disclosure and consumer consent. Virginia's Consumer Data Protection Act, for example, requires data collected and processed to be "adequate, relevant, and reasonably necessary" for its purposes as disclosed to the consumer.[12] Privacy statutes modeled on procedural data minimization might make it difficult to process certain kinds of personal information, but ultimately with sufficient evidence of disclosure, they tend to remain agnostic about the data's ultimate use.

Substantive data minimization goes further by limiting the ability of controllers to use consumer data for purposes beyond those expressly permitted under the law. Maryland's Online Data Privacy Act, enacted earlier this year, is an example of this. The Maryland law permits covered businesses to collect, process or share sensitive data when it is "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer."[13] Although Maryland permits consumers to consent to additional uses, practices that are by default legal under Virginia's and similar statutes would generally not be permissible in Maryland.

---

[10] *See* Washington My Health My Data Act, 2023 Wash. Laws 191, § 19.373.020.

[11] *See* Washington State Office of the Attorney General, *Protecting Washingtonians' Personal Health Data and Privacy*, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

[12] Va. Code Ann. § 59.1-578.

[13] Maryland Online Data Privacy Act of 2024 (MODPA), § 14–4601.

A federal privacy law should lay out clear procedural data minimization principles. It should limit data collection and processing to what is reasonably necessary for the purposes of the business, which themselves must be disclosed to the consumer. This is the most effective standard for implementing the minimization principle, and avoids otherwise broad standards that would, in practice, create disparities in how varying businesses apply it from a compliance perspective.

However, a federal framework should avoid substantive data minimization, which has already been shown to create significant barriers to innovation. For example, even with the permission to use data pursuant to consumer consent, the GDPR's restrictions on data use have already slowed the pace of European AI development compared to the United States and China. Enforcement actions by EU regulators, as well as general uncertainty over the legality of training multimodal AI under the GDPR, have already forced even large companies operating in the EU to altogether stop offering their consumer AI applications within the jurisdiction.[14] A federal privacy law should similarly avoid Maryland's vague substantive data minimization standard that limits collection to what is "reasonably necessary and proportionate" — or "strictly necessary" in context of sensitive data — to provide and maintain a product or service requested by the consumer.

Lastly, data minimization in the context of kids' data is unique. As we outline in SIIA's *Child and Teen Privacy and Safety Principles*, we believe that in addition to standard procedural data minimization protections enjoyed by all consumers, businesses should limit the collection of children and teens' personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed. Furthermore, this personal data should not be used for reasons that are neither reasonably necessary for nor compatible with the disclosed purposes, unless the business obtains consent. However, kids' data may still be used to provide access to high-quality content, as well as safety-enhancing and privacy-protective algorithm-based features that are in the interest of children and parents.[15]

Clear and consistent consumer rights. In addition to procedural data minimization safeguards, a federal privacy law, like U.S. state privacy laws, should emphasize clear and consistent consumer rights. These include access, correction, and deletion rights, subject to a series of practical exemptions also present in state laws that address trade secrets, technical feasibility, and practicable processes and timelines for administering these rights.

---

[14] Axios, *Meta Won't Offer Future Multimodal AI Models in EU* (Jul. 17, 2024), https://www.axios.com/2024/07/17/meta-future-multimodal-ai-models-eu.

[15] *See* SIIA, *Child Privacy and Safety Principles*, https://www.siia.net/wp-content/uploads/2024/03/SIIA-Child-Privacy-and-Safety-Principles-.pdf.

Frameworks such as the *Texas Data Privacy and Security Act* (TDPSA) and the *Virginia Consumer Data Protection Act* (VCDPA) provide a good balance of pragmatic and risk-based consumer rights provisions. These laws also include clearly defined opt-out rights focused on processing that implicates a heightened risk of data misuse and consumer harm. Finally, incorporating language from these laws as a framework for baseline protections will better enable U.S. companies to more efficiently come into good faith compliance with a federal framework, as these entities have already been required to invest substantial resources into their existing compliance programs derived from the state frameworks.

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

In general, heightened protections for sensitive data should be tailored to the risk that this data is misused in ways likely to harm their data subjects. To enable good faith compliance and consistency with emerging norms in U.S. privacy law, heightened protections should also be generally consistent with existing state law requirements. These include 1) consumer consent prior to collection and processing, or opt-in consent, and 2) mandatory data protection assessments (DPAs).

The Committee should, however, take care to avoid imposing restrictions likely to needlessly curtail innovation without a meaningfully corresponding reduction in risk to consumers. It should also ensure that the new requirements do not add to consumer confusion about their rights to control the collection, use and dissemination of sensitive data. Examples of frameworks to avoid include 1) multiple standalone disclosures that must be surfaced on websites, 2) prohibiting sharing of data with service providers, and 3) a restrictive substantive data minimization standard for sensitive data that already retains heightened protections (as discussed above).

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-driven innovation and small businesses.

Targeted advertising, although frequently maligned as a threat to consumer privacy, plays an integral role in data-driven innovation and small businesses. In fact, it largely serves as the foundation that funds the operations of online platforms where U.S. consumers can connect, access news, and consume information and entertainment largely for free. Furthermore,

targeted advertising serves as a boon to small businesses. Efficient and effective advertising based on business's responsible collection and processing of consumers' personal information enables small businesses to compete with their larger competitors, and aids consumers in discovering their products.

It would be a mistake to pull out the rug from the online ecosystem that is responsible for this explosion in informative content and entrepreneurship. This would decrease the quality, while increasing the cost, of consumers' online experiences. As such, targeted advertising opt-in requirements for overbroad categories of "sensitive" data, as existed in the APRA, is ill-advised. This would unnecessarily harm the viability of many ad-supported services offered for free or at reduced costs that offer significant consumer benefits.

Instead, a federal privacy law should target specific privacy risks in connection with targeted advertising. Because these privacy risks flow from personal data processed via third parties, targeted advertising in this context should be subject to a consumer opt-out right. However, a targeted advertising opt-out that covers first party data is unnecessary and would simply harm small businesses that consumers have already chosen to trust with their personal data. In fact, including first party data in the opt-out right would paradoxically reduce consumers' control over their own data. It would force consumers into the all-or-nothing choice between permitting third party advertisers' access to their data, and interacting with trusted businesses of which they are already customers.

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 patchwork of U.S. privacy laws has caused three primary harms. These include 1) consumer confusion, 2) conflicting or uncertain mandates, and 3) complicating compliance.

Consumer confusion. Consumers are likely to be confused by rights granted them by various states that are described using the same name yet whose scope or processes vary significantly. Different requirements around how consumers may exercise their access, correction and deletion rights, processes for disclosing privacy policies, and even definitions of the "sale" of consumer information across states create confusion among even tech-savvy consumers.

As just one detailed example, under most privacy laws, the consumer right to opt out of targeted advertising includes a right to opt out of third party advertising. However, in California and Florida, third parties may include affiliated sites, or "cross-context" behavioral advertising,

which is treated as "targeting" for purposes of the opt out right.[16] Furthermore, in California, even data collected from "distinctly-branded" services and shared among them is considered "cross-context" behavioral advertising, and thus "targeted advertising" subject to the opt-out.[17] The varying scope of the right is almost certain to bewilder consumers, who despite opting out of third party targeted advertising, may wish to receive advertising from a site affiliated, or even branded, with the identity of a business of which they are already customers.

Conflicting or uncertain mandates. The state privacy patchwork has inevitably created conflicts between various state laws. Beyond the inefficiencies and uncertainty this creates, it makes it significantly harder, if not impossible, to choose between implementing the conflicting requirements.

For example, Colorado mandates that a universal opt-out mechanism on a device or browser cannot be turned on by default.[18] California, meanwhile, requires businesses to respect any commonly used signals, including universal opt-out signals, without this default limitation.[19] It is not possible to opt a single consumer both in and out at the same time. Similarly, most states require consent prior to the collection of sensitive consumer data. However, California requires businesses to offer consumers the ability to *limit* the collection of sensitive data, which operates as an opt-out right.[20] Providing both of these to the same consumer is technically unfeasible.

Even when there is not a direct conflict, the patchwork of state requirements creates widespread uncertainty around how, and when, to implement various compliance protocols. By interpreting the same language differently, courts and state attorneys general may create judicial or enforcement patchworks of their own. Vague phrases within many state privacy laws, such as "*reasonably foreseeable risk* of unfair or deceptive treatment of consumers" or "*capable of revealing* race, religious belief, or health conditions" (emphases added) leave so much to interpretation that they create further downstream uncertainty while implementing compliance programs.[21] A federal privacy framework, even when expressly preemptive, should take care to clarify these terms to limit the potential for derivative patchworks from emerging.

Complicating compliance. Lastly, the incremental timeline of new state requirements — let alone regulations drafted on top of the base text of state privacy laws — adds a "moving target" complication to attempts at good faith compliance. This is especially true when subsequent

[16] Cal. Civ. Code § 1798.100 et seq., § 1798.140; *see* 32 Fla. Stat. Ann. § 501.702.
[17] *Id.*
[18] C.R.S. § 6-1-1301, et seq., § 6-1-1306.
[19] Cal. Civ. Code § 1798.100 et seq., § 1798.185.
[20] *Id.*
[21] C.R.S. § 6-1-1301 et seq., § 6-1-1701.

requirements prove incompatible with previously implemented systems and processes, which themselves were implemented to fulfill requirements imposed as recently as the preceding year.

For example, many state privacy laws give consumers the right to access, correct, and delete their personal data. Businesses naturally complied by providing, altering, and deleting this data upon request. Recent regulations in several states, however, require businesses to provide context about data that was accessed, altered or deleted in cases where other data in that consumer's dataset was left out of the request due to a statutory exemption. In the case of corrected or deleted data, of course, this is often impossible, as the data no longer exists in its previous form, and compliance programs are not capable of resurfacing it due to a subsequent change in policy.

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?

It is critical that any federal privacy framework include broad, strong and carefully-drafted preemption of U.S. state and local laws. Consistency, uniformity and clarity are the purpose and promise of a federal privacy law for both U.S. businesses and consumers. First, businesses attempting to comply with a patchwork of state and local privacy requirements need uniformity and consistency to enable innovation and reduce both upfront and ongoing compliance burdens. For multistate U.S. companies, the nature of data flows effectively requires them to comply with the state with the most draconian requirements, which invariably grants states like California the ability to dictate default privacy standards for the nation.

This problem is compounded when these states grant rulemaking authority to state attorneys general or even independent agencies such as the California Privacy Protection Agency (CPPA). This, in turn, now renders this default national standard also a moving target for all U.S. businesses attempting to comply. It also creates the additional risk that these entities may seek to use their authority under state privacy laws to legislate beyond privacy concerns as they are conventionally understood nationwide. For example, we have recently seen the CPPA attempt to regulate artificial intelligence more broadly and restrict first party advertising – thus risking new effective default national standards in these domains as well.[22]

[22] *See* SIIA, *Comments of the Software & Information Industry Association* (Feb. 19, 2025), https://www.siia.net/wp-content/uploads/2025/02/SIIA-CPPA-Draft-Regulations-Comment-2.19.25-1.pdf.

Second, preemption benefits consumers by providing consistency and uniformity around their rights and expectations regarding their personal and sensitive data. Without broad preemption, American consumers can receive different levels of privacy protections depending on their jurisdiction or that of the data controller. Not only is this nonsensical given the inherently cross-border context of data privacy protections, but it also causes needless consumer confusion around when and where their rights apply, and even more importantly, how to exercise them. In fact, this even applies to consumers learning *how* to exercise these rights. For example, the current patchwork of laws require multiple notices such as under the MHMDA, and state-specific opt-out pages as under the California Consumer Privacy Act (CCPA).

Further, state and local laws imposing requirements on specific categories of data *(i.e.,* biometric data, health data, kids' data, data incorporated into artificial intelligence tools) implicate these same concerns. Because these laws are often structured differently than general privacy laws, they present the additional complication of conflicting protections for sensitive or even personal data. For example, a state may require opt-in consent for a category of data for which the federal law requires only an opt out, in turn creating a technical impossibility for consumers to opt into specific uses. A state may also eschew relevant exemptions for the productive use of data provided for in a federal law, again restricting these uses by default nationwide despite Congress's intent.

Finally, it is important to draft strong preemption using airtight language to avoid subsequent legal challenges and questions about congressional intent. A law should preempt state laws "*related to* data privacy and security" (emphasis added) with limited exceptions. Alternatively, a federal law could expressly preempt state laws "with respect to the collection, transfer, processing, retention, and sharing of personal information," again with limited exceptions. Preempting only state laws "covered by the provisions of the Act," as the *American Privacy Rights Act* (APRA) was drafted, is insufficient for this purpose. This is because the Congressional Research Service has recommended that the phrase "covered by" is limited in its ability to preempt.[23] Courts following this recommendation will only preempt state bills with the same requirements as the federal law – leaving open the possibility of passing even more restrictive requirements.

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

[23] Congressional Research Service, *Federal Preemption: A Legal Primer* (Mar. 18, 2023), https://www.congress.gov/crs-product/R45825.

A federal privacy law can exist alongside existing federal privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA). However, this must be subject to certain data-level and entity-level carveouts.

HIPAA. Like in the state laws, a federal privacy framework requires a HIPAA carveout. In this case, the carveout should apply to the entire law to avoid conflict, and apply at the entity level. Thus, an entity should be exempt when it is acting as a "covered entity" or a "business associate" under HIPAA.[24]

COPPA. A federal privacy law can and should exist alongside COPPA. COPPA provides protections for minors under the age of 13. COPPA's protections are distinct from sensitive protections for kids' data because they specifically implement parental consent protections.

FERPA. It would also be helpful for a federal privacy law to clarify the intersection of COPPA and FERPA. Specifically, it is critical that schools are permitted to provide consent to student data collection and processing on behalf of parents. Restricting schools from providing consent *in loco parentis* would hamstring teachers and their use of educational tools, as well as burdening parents with a stream of consent requests. We support the language in the recently introduced COPPA 2.0 bill that would clarify the validity of schools' consents.[25] We recommend that a federal privacy law provide a similar clarification. Any work done in this area should be done in partnership with the Committee on Education and Workforce.

IV. Data Security

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

In general, a federal privacy law should emphasize cybersecurity protections for consumers that are consistent, aligned with existing best practices, and antifragile to technological change by emphasizing ongoing flexibility and adaptability.

First, cybersecurity protections are an area ripe for strong federal preemption to avoid a counterproductive patchwork of state security requirements. Currently, states seek to advance their own cybersecurity requirements, such as the CPPA's draft regulations that purport to regulate the scope and content of cybersecurity audits. Localized requirements like this are

[24] *See* 42 U.S.C. § 1320d et al., § 1320d.
[25] *Children and Teens' Online Privacy Protection Act* (COPPA 2.0) (S.1418), § 2.

fundamentally at odds with establishing consistent best practices in cybersecurity and cross-border data protection. Federal preemption is both logical and practical, and would free U.S. companies' cybersecurity teams to spend less time on compliance and more time securing data.

Second, regulations should recognize and align with existing standards and frameworks. These include those promulgated by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). Businesses are already using these frameworks in their existing security measures, and these frameworks serve as reference points for comprehensive best practices. A federal privacy law should seek to align its requirements with those that are already widely accepted as industry best practices.

Consumer cybersecurity protections should lastly emphasize adaptability and an ongoing flexibility to adapt to new technologies. Conversely, a federal law should avoid rigid or prescriptive requirements that are likely to be contextually suboptimal for many entities, or even irrelevant in the face of continued technological development in the long run. This will ultimately lead to better data security for consumers, even as threats and technologies evolve.

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?

Despite the substantial intersection between equities in data privacy and AI development, a federal privacy framework need not define or directly address AI. Privacy protections should be technology-neutral as they apply upstream of data processing, and this processing includes AI. Of course, AI may be unique among the methods of data processing in the degree of risk it presents to consumers and the scale of potential misuse of consumer data. Furthermore, we support the creation of a separate, federal preemptive framework for governing the unique opportunities and risks posed by AI technology. Many of these risks, however, can also be addressed at scale in a technology-neutral way via the consumer protections discussed above — including procedural data minimization and consumer data subject rights — that are native to the consumer privacy space.

At the same time, Congress must be cognizant of an emerging state patchwork specifically around AI. This is relevant to a federal privacy framework because states can attempt to skirt federal privacy preemption by cloaking what are, at their core, data privacy regulations as "rules of the road" for AI or automated decision-making (ADMT). For example, the CPPA's proposed regulations around ADMT include severe restrictions around how and what data can be used in

these automated processes.[26] Similarly, states have considered "data digester" legislation specifically imposing burdens on entities that use datasets to train AI, above and beyond what those states' consumer privacy laws would otherwise require.[27]

These are, at their core, data privacy regulations – *they are simply not technology-neutral since they apply only to AI*. It is important for a federal law to indicate clearly that these laws, no less than technology-neutral privacy laws at the state level, are preempted by a federal privacy framework. Otherwise, Congress risks replicating the data privacy patchwork specifically in the context of this critical technology.

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.

Enforcement. In general, a federal privacy framework should be enforced exclusively through a single federal regulator. The FTC is the appropriate enforcement agency for a general consumer privacy law. Further, because privacy laws are still relatively new and even basic provisions in the EU and U.S. states have been interpreted differently even among judges, the role of a regulator is to set consistent policy through enforcement in a thoughtful and systemic way, including through penalties or injunctive relief for consumers if and when necessary.

Private Right of Action (PRA). Rather than protecting individual consumers, PRAs in state privacy laws have been routinely weaponized by the plaintiff's bar. In California, for example, even a limited PRA that applied to cybersecurity breaches gave rise to plaintiffs' lawyers leveraging the threat of injunctions, fees, and reputational harm to force settlements for claimed but often nonexistent infractions.[28] Rather than protecting consumers, these efforts routinely disrupted services to consumers and drove up costs, especially for smaller businesses unable to absorb the costs of litigation.

Studies have revealed that private rights of action fail to compensate consumers *even when a violation has been shown*, and instead primarily benefit the plaintiff's bar by creating a "sue and

[26] California Privacy Protection Agency, *Proposed Text (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)*, cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.
[27] California AB 3204 (2024), https://legiscan.com/CA/text/AB3204/id/2984208.
[28] *See* WilmerHale, *Year in Review: CCPA Litigation Trends from 2023* (Mar. 1, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240226-year-in-review-ccpa-litigation-trends-from-2023.

settle" environment.[29] Furthermore, although we appreciate the intent behind ideas designed to restrict a federal PRA, such as by specifying damages "up to" a statutory minimum, this is unlikely to solve the problem of frivolous lawsuits. This is because plaintiff's lawyers' legal strategy to extract settlements does not rest on the outcome of the case, but instead on the opportunity to inflict asymmetrical eDiscovery costs on businesses. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal eDiscovery costs, huge negotiating leverage for nuisance settlements even if the defendant is compliant.

Rulemaking. As discussed above, we urge the Committee to avoid the uncertainty that ongoing rulemaking authority would create. Creating a presumptively permissive federal privacy framework — rather than one that relies on substantive data minimization and "permitted purposes" — should render a federal privacy framework resilient to changes in technology.

Affirmative defenses. A federal law should also incentivize organizational accountability by including an affirmative defense for businesses to demonstrate compliance through the adoption of a privacy program and compliance with established privacy frameworks, as established by NIST.[30]

* * *

SIIA looks forward to continuing to work with the Energy & Commerce Committee and the Privacy Working Group to advance a comprehensive federal consumer privacy bill that will provide a nationwide standard for consumer privacy. Please direct inquiries to Anton van Seventer, Counsel for Privacy and Data Policy (avanseventer@siia.net) and Paul Lekas, Senior Vice President for Global Public Policy & Government Affairs (plekas@siia.net).

[29] *See* Institute for Legal Reform, *Ill-Suited: Private Rights of Action and Privacy Claims* (Jul. 11, 2019), https://instituteforlegalreform.com/research/ill-suited-private-rights-of-action-and-privacy-claims/.
[30] *See* NIST, *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0*, (Jan. 16, 2020), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.