Response by the Centre for Information Policy Leadership[1] (CIPL) to the U.S. House Committee on Energy & Commerce Privacy Working Group Request for Information

April 7, 2025

Word Count: 3,373

I. Roles and Responsibilities

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?

It is important to distinguish between the obligations of "controllers," which collect and determine the uses of personal information, and "processors," which provide a service with respect to personal information on behalf of controllers. This distinction is important because it eliminates confusion among stakeholders and creates certainty around respective statutory obligations. Controllers are responsible for ensuring compliance with most legal requirements pertaining to the processing of data, including requirements related to the exercise of individual rights. Controllers typically have a direct relationship with individuals. Processors process personal information on behalf of controllers, typically to provide a specific service to controllers pursuant to a contract that defines their obligations. If processors use data for their own purposes, however, they may assume the responsibilities of controllers. Statutory requirements for processors typically include reasonable data security measures and compliance with the contractual requirements agreed upon with controllers.

These concepts are important for effective consumer protections because they create certainty regarding the allocation of responsibilities among organizations. Further, these concepts can promote organizational accountability by distributing data privacy and security responsibilities with the entities most responsible for the use of personal information.

That said, the concepts of "controller" and "processor" are sometimes too narrowly interpreted and do not always accurately depict the roles of entities in the digital environment. This is especially the case with innovative data uses enabled by technological developments and the emergence of new business models that may involve more complex

---

[1] The **Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

and dynamic relationships between organizations. For example, the concepts of controller and processor do not easily transpose in the context of blockchain or AI, especially when personal data is used to train an algorithmic model or where many organizations are making decisions concerning processing activities. These concepts must therefore be flexible enough to account for situations where the same parties may have different roles with respect to the same pool of personal data (i.e., they may be controllers for some purposes and processors for others). Therefore, a comprehensive federal data privacy and security law (the Law) should enable flexibility where needed, while striving to distinguish clearly between controllers and processors whenever possible.

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

See our response to Question I(A).

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

In general, the obligations related to processing of personal information should apply to all entities, with appropriate exemptions for defined activities and use cases. While the House Data Privacy Working Group (the Working Group) should consider the differential impacts of compliance according to regulated entities' size, it should keep in mind that small organizations can process the personal data of millions of individuals and this processing may potentially be harmful. If and where the Law allows for any exemptions for small organizations, it should simultaneously create mechanisms and incentives to support and guide them to a path of accountable, secure, and responsible data practices. The Working Group should consider similar principles with respect to the applicability of obligations to nonprofit organizations. Hard thresholds (number of employees, revenue, etc.) can create perverse incentives, where businesses deliberately curtail growth for fear of compliance burdens.

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."

The Law should apply to the processing of personal information (i.e., personally identifiable information or personal data) and exempt the processing of deidentified information. Personal information should be information that can be reasonably linkable to an identified or identifiable individual. Information is deidentified and not reasonably linkable to the extent that an organization: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

The scope of "sensitive personal information" is the subject of widespread debate. On one hand, the categorization of certain information as "sensitive" provides certainty to

organizations and individuals about when a higher level of protection is expected. On the other hand, the actual sensitivity- and risk-level associated with data depends on the use context and cannot always be pre-determined for all contexts. Rigid classification of data as sensitive or not may result in overregulation as well as under-regulation. While the law should recognize that the processing of sensitive personal information may pose high risks, for example, to individuals' civil rights, the law should also recognize that, under the proper technical circumstances (e.g., through the application of privacy-enhancing technologies) and with the proper organizational measures, processing of certain sensitive personal information can provide meaningful benefits to individuals while also presenting low risk. Thus, the question of whether heightened protections apply to certain data should be risk-based and contextual and focus on the use of data, rather than ex-ante strict classification.

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

Transparency, i.e., informing individuals about what happens with their personal information, is essential for building trust in the digital economy. However, individuals are often provided with overly complex and legalistic privacy notices. Transparency can serve its purpose only if it is meaningful, user-centric, and contains relevant information that is necessary or useful for individuals in a particular context to enable them with choice and the exercise of their rights. Concise privacy notices that provide meaningful and actionable information should be the outcome of any transparency requirements.

The Law should require transparency for processing activities related to personal information, offering flexibility regarding the content, timing, and manner of disclosure, and providing for exceptions if there is a compelling reason to limit transparency. For example, transparency should not come at the expense of other important considerations such as safety, security, fraud detection, and trade secrets. Furthermore, the level of detail provided by transparency measures must be proportionate to the risks posed by the processing, and organizations should recognize that greater risks will require greater transparency.

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 protections promote trust and therefore enable the development of reliable technologies based on accurate data sets. The Law should include a robust set of consumer protections with appropriate security safeguards, while taking into account beneficial and low-risk data uses. Consumer protections must be balanced with goals that promote the common good, including policies that promote legitimate innovation, public health, education, national security, and fraud prevention.

The Law should include consumer protections that should be adapted in consideration of other competing rights and interests, such as transparency, access, correction, deletion, security, portability, opt-out, human review of automated decision-making that has legal or similarly significant effect, and complaint-handling by the responsible organization.

In many global and state data privacy laws, "notice and consent" requirements have played a prominent role in attempting to give individuals "control" over their information. However,

this model, while it has a role to play, has significant limitations when it comes to realizing consumer protections and governing the processing of information in a digital society. While consent in many social scenarios is important because it provides individuals with autonomy and control, the "notice and consent" model for many personal information processing activities is not scalable. The "notice and consent" model places a high burden on individuals to read and digest information governing the processing of their data and make informed choices to protect their rights and interests. Hence, "notice and consent" should not be the sole arbiter of consumer protections in the Law, although it may appropriately play a role for many processing activities.

Real empowerment and protection for consumers that balances other public policy goals can be delivered through organizational accountability requirements (see Section VII), such as risk-based protections, demonstrable accountability measures, anonymization or de-identification of personal information, transparency, redress mechanisms, as well as by individuals' rights of access, correction, objection, and deletion, where appropriate. These consumer protections must be meaningful while also ensuring that they do not overburden organizations.

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

As discussed in response to question II(A), the Law should attach heightened protections to the collection, processing, and transfer of sensitive personal information in a context- and risk-based manner. In many circumstances, providing heightened protections, such as consent or opt-out rights, for the collection, processing, and transfer of sensitive information will make sense to drive trust and provide organizations and individuals with necessary certainty. However, the law should enable beneficial uses of sensitive personal information, which may include the ability to (i) provide consumers the products or services they requested; (ii) comply with legal obligations; (iii) promote and enable security; (iv) prevent, detect, protect against, and respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or illegal activity; (v) improve products and services; or (vi) conduct medical or scientific research. Sensitive personal data should generally be subject to heightened data security requirements, keeping in mind that "sensitivity" may be contextual and mitigated through appropriate controls.

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.

Without a doubt, the EU GDPR has triggered the proliferation of data privacy and security laws, both internationally and at the U.S. state level. With the benefit of hindsight, CIPL has taken a candid look at the GDPR's successes and failures in a 2024 report (see endnotes).[i] Our

report contains several recommendations that would be useful for the Working Group's consideration:

- Apply consistency and certainty to the interpretation of data privacy and security principles.
- Balance consumer privacy expectations against other rights and interests with the use of a risk-based approach that prioritizes compliance measures, mitigations, and controls in a way that is proportionate to the risks at hand and while taking into account the benefits of the uses of data as well as the risk of loss of opportunity from not using the data.
- Adopt principles- and outcomes-based, risk-based, technology-neutral, and future-proof standards to promote beneficial emerging technologies.
- Issue timely, pragmatic guidance informed by input from key stakeholders; promote discussion of new issues and emerging technologies; advance technical expertise within government and enforcement bodies; and support innovative regulatory tools such as sandboxes.
- Promote the protection of consumer rights and reduce the need for enforcement by incentivizing best practices and organizational accountability.
- Facilitate alignment with relevant and overlapping legal obligations stemming from other laws and regulations.
- Support small businesses with mechanisms and tools that render compliance manageable, such as with voluntary and affordable certifications and codes of conduct and innovation hubs and sandboxes.
- Establish a regulatory oversight and enforcement model that is itself risk-based, incentivizing organizations to prioritize and focus resources on matters that present significant harm to consumers, coupled with ex-ante engagement and transparent and strategic prioritization and innovative tools, such as regulatory sandboxes that allow for experimentation and innovation.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

Currently, there are approximately 20 state-level comprehensive data privacy laws in the U.S. (depending on which laws one counts as "comprehensive"). While this patchwork of laws is workable for some organizations, this is more true for large businesses that have the resources to adapt their processing activities to the various emerging state-level standards on a variety of key issues such as data minimization, age assurance, automated decision-making, and data protection assessments. Even then, consistent legal rules are essential to enable the effective use and scaling of data necessary for innovation and economic progress. For example, there are emerging inconsistencies related to the scope of sensitive and health-related information that may impact the development and provision of beneficial technologies and services.

The U.S. has always had the advantage of a huge, single market, which has enabled access to consumers, capital, talent, infrastructure, and data—all instrumental for building a successful and competitive U.S. economy. Access to, use, and sharing of diverse and rich data sets, including between the public and private sectors, is essential for the development and

deployment of AI technologies and new products and services. CIPL has long maintained that a comprehensive and harmonized legal framework to data privacy, security, and data use is necessary so as not to burden innovation, hamstring small businesses, and undermine consistent consumer protections.

In a series of papers, CIPL has analyzed the fragmented and inconsistent legal obligations facing organizations in the U.S. at the state level (see endnotes).[ii] Some organizations are struggling to build comprehensive and streamlined data privacy programs and are issuing a variety of amendments to their programs, depending on the state. This work is burdensome and prevents organizations of all sizes from prioritizing data uses that warrant more attention and investment in programs that mitigate potentially greater harms. In some cases, organizations are developing separate data privacy programs for different states because the requirements are difficult to integrate into a single, unified program.

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?

The Law should preempt state law data privacy requirements on issues that it covers.

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

The Law should provide comprehensive privacy protections applicable to all industries and therefore should create consistency with existing federal sectoral laws and regulations, including those specific to domains such as health, clinical research, financial services, and children's data. Where appropriate, the Law should amend or replace inconsistent requirements that fall below the new baseline. It should include appropriate exemptions, as information is increasingly cross-sectoral, and data-driven innovation is premised on the ability to use data sets from different sectors.

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?

The Law should establish a baseline of security requirements for organizations to strengthen the digital ecosystem's resilience to breaches and fraud, promote efficient and effective incident response protocols, and improve the security of consumer data held by companies. To ensure that security requirements are technology-neutral and future-proof, the Law should rely on industry best practices and recognized information security standards. The Law should also create incentives to encourage organizations to implement state-of-the-art technical and organizational data security measures.

To the extent the Law requires consumer consent for certain processing activities, it should ensure that organizations can, where appropriate, rely on data security and fraud prevention exemptions to consent requirements. For example, organizations should not be required to

rely on consent to process necessary personal information for information and system security and fraud prevention and detection purposes. Similarly, where the Law may establish transparency requirements, organizations should be able to rely on the same security and fraud prevention exemptions so that malicious actors do not take advantage of these consumer protections for nefarious purposes.

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?

Not all AI models or systems process personal information, but to the extent they do, the Law should govern the processing of personal information by such models or systems and preempt any overlapping state-level obligations governing the processing of personal information. States are taking various approaches to the scope of opt-out rights in the context of automated decision-making and profiling. Given the complexity and uncertainty associated with these requirements, organizations would benefit from regulatory consistency across the U.S. market.

Also, as demonstrated with GDPR-style laws, there are some important tensions between data protection principles—e.g., purpose limitation, legal basis, data minimization, transparency, and rights of individuals—and the way AI technologies work. An overly narrow interpretation of these principles would hinder the development of AI technologies and the use of data for AI development and deployment. It is important for the U.S. not to follow the same narrow construction in the Law and to promote a degree of flexibility considering new technologies.

CIPL has been tracking how state privacy and AI laws and regulations impact automated decision-making and profiling activities (see endnotes).[iii]

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.

CIPL has long promoted "organizational accountability," which differs from the type of accountability addressed by the Working Group.[iv] Whereas the Working Group's use of accountability focuses on the enforcement context, CIPL views external enforcement as just one of many factors to be considered in an organizational accountability framework. That said, we respond to the Work Group's question regarding accountability in the enforcement context as follows:

A lack of harmonization with regard to regulatory guidance and the interpretation of data privacy requirements, including interaction with other laws, can create complexities and legal uncertainty for all stakeholders. To the extent possible, the Law should place sole enforcement authority in an independent, federal expert agency, such as the Federal Trade Commission, that can develop the proper technical expertise, facilitate ex-ante stakeholder engagement, and issue consistent and timely guidance for the U.S. market. Where an enforcement area may involve more than one agency, the Law should incentivize cross-regulatory cooperation to avoid contradictory interpretations. State Attorneys General should also play a role in enforcing the Law, but subject to FTC leadership, guidance, and coordination to ensure consistency.

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?

While the Law should include sensible and meaningful penalties for violations, it should enable and prioritize incentives for compliance. This should include various forms of constructive ex-ante engagement; collaboration and even co-operation-based regulation between regulators and industry to identify potentially problematic products, services, and business practices (e.g., regulatory sandboxes); and the ability for regulated entities to cure potential violations or non-compliance, with fines being reserved for the most serious violations. Fines and penalties should be proportionate to the harm, taking into account the company size (employees, revenue, profits, etc.); should be mitigated for demonstrated accountability and compliance efforts; and should be used only as a last resort to deal with negligent, wilful, or systematic failures.

Enforcement authorities should be properly resourced to facilitate stakeholder engagement, recruit technical talent, issue timely and risk-based guidance, review and oversee safe harbor frameworks, and foster innovation that protects consumers via regulatory sandboxes and innovation hubs.

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

Formal and trustworthy safe harbor programs based on seals and certifications that are properly resourced can play an important role in promoting compliance and should be enabled by the Law. They can be particularly helpful for small and medium-sized organizations that may not have the resources or expertise to design their own privacy compliance programs. Equally, these frameworks, accompanied by trustmarks, are hugely important in the business-to-business context, as they promote trust and increase speed-to-market by streamlining the procurement and negotiation processes. Indeed, safe harbors based on seals and certifications can play an important role in driving trust among controllers, processors, and users in a data-driven economy.

The Law should also recognize U.S. leadership in the development and advancement of the Global Cross-Border Privacy Rules (Global CBPR) and Global Privacy Recognition for Processors (Global PRP) Systems by expressly endorsing the use of these certified compliance programs in the Law. Global CBPR and Global PRP Systems not only advance trusted data flows with

other jurisdictions but also help facilitate compliance with domestic data privacy and security requirements. Indeed, the free trade agreement between the U.S., Mexico, and Canada (USMCA) recognizes the precursor to the Global CBPR and Global PRP Systems as a valid mechanism to facilitate cross-border information transfers while protecting personal information.[v] The Global CBPR and Global PRP Systems provide a firm foundation for enabling robust, safe, and streamlined cross-border transfers that are essential for the digital economy and society, as well as the development and deployment of AI tools.

VII. Additional Information

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

For more than 20 years, CIPL has been a thought leader on ***organizational accountability*** and risk-based solutions as the foundation for smart data regulation, responsible data governance, and critical innovation, including the development and deployment of AI. Our research shows that organizational accountability is a key building block for effective data privacy and security regulation.[vi] Organizational accountability requires organizations to:

a. Take steps such as implementing a comprehensive data privacy management program (DPMP) to translate data privacy legal requirements into risk-based, concrete, verifiable, and enforceable actions and controls relating to the processing of personal data which are reviewed and adapted over time; and
b. Demonstrate the existence and effectiveness of DPMPs internally (e.g. to the board and senior management) and externally (e.g. to enforcement authorities, individuals, business partners, and shareholders).

CIPL Organizational Accountability Framework

Organizations that implement organizational accountability through DPMPs operate effectively and efficiently in the modern digital economy while also maximizing their innovation potential.[vii] Ultimately, DPMPs allow organizations to realize trust with key stakeholders and maximize their use of data as a competitive edge, enabling broader

innovative and responsible uses of data. Our research on organizational accountability as a facilitator of trust and innovation is referenced in the endnotes of this written response for the Working Group's review and consideration.[viii]

The Law should establish a baseline of organizational accountability measures for regulated entities. Organizational accountability is a well-established architecture for translating data privacy and security legal requirements into risk-based, actionable controls. This architecture allows organizations to be agile in an economy driven by fast, technological advancements and acts as a driver and enabler of responsible innovation and business sustainability. Accountability allows organizations an important degree of flexibility in applying the rules in a context-and risk-based manner, without the prescription and burden of excessive requirements that may stifle innovation. It also enables policy makers to maintain the necessary flexibility in the rules, to ensure they are future-proof and technology-neutral.

---

[i] CIPL Report, "The GDPR's First Six Years Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement" (May 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/gdpr_six_years_on_cipl_may24.pdf.

[ii] *See* CIPL White Paper, "Comparison of U.S. State Privacy Laws: Data Protection Assessments" (Feb. 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comparison_us_state_privacy_laws_dpa_feb14.pdf; *see also* CIPL White Paper, "Automated Decisionmaking and Profiling (ADM) Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations" (May 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/adm_profiling_requirements_us_privacy_law_cipl_may24.pdf; *see also* CIPL White Paper, "Data Minimization in the United States' Emerging Privacy Landscape: Comparative Analysis and Exploration of Potential Effects" (Aug. 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_data_minimization_us_privacy_landscape_aug24.pdf; *and see* CIPL White Paper, "Age Assurance & Age Verification Laws in the United States" (Sept. 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_age_assurance_in_the_us_sept24.pdf.

[iii] CIPL White Paper, "Automated Decisionmaking and Profiling (ADM) Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations" (May 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/adm_profiling_requirements_us_privacy_law_cipl_may24.pdf.

[iv] CIPL White Paper, "Organisational Accountability – Past, Present and Future" (30 Oct. 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf.

[v] CIPL White Paper, "What Does the USMCA Mean for a US Federal Privacy Law?" (17 Jan. 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_what_does_the_usmca_mean_for_a_us_federal_privacy_law__01.17.2020__4_.pdf.

[vi] CIPL Report, "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework" (May 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report_27_may_2020__v2.0.pdf.

[vii] CIPL & Cisco Report, "Business Benefits of Investing in Data Privacy Management Programs" (Jan. 2023), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf.

[viii] *Id.*