ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

Data Privacy Working Group

House Committee on Energy and Commerce

Washington, DC

	)
	)
In the Matter of:	)
	)
Data Privacy Working Group	)
Request for Information	)
	)
	)

April 7, 2025

CONTENTS

Comments of ITIF 1
Introduction and Summary 2
I. Roles and Responsibilities 3
II. Personal Information, Transparency, and Consumer Rights 3
III. Existing Privacy Frameworks & Protections 5
IV. Data Security 6
V. Artificial Intelligence 6
VI. Accountability & Enforcement 7
Conclusion 7

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the request for public information concerning the Privacy Working Group formed by House Committee on Energy and Commerce Chairman Brett Guthrie (KY-02) and Vice Chairman John Joyce, M.D. (PA-13).[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress.

Comprehensive data privacy legislation has been on the congressional to-do list for years. In the meantime, several states have passed their own laws, with many more likely to follow. This trend has created a state of play wherein organizations that handle personal data must comply with a patchwork of legislation, driving up costs and creating confusion among consumers. The longer this trend continues, the more difficult it will be to reach a compromise on data privacy. Therefore, it is imperative that Congress establish a unified national approach to privacy by preempting state laws.

ITIF strongly supports Congressional efforts to develop a reasonable compromise on federal data privacy legislation. Such legislation should protect and promote innovation by minimizing compliance costs and restrictions on data use. It also should address concrete privacy harms, not hypothetical ones, improve transparency requirements, and strengthen oversight and enforcement. Congress should not include data-minimization requirements, universal opt-in rules, purpose-specification requirements, limitations on data retention, a right to deletion, a private right of action, or privacy-by-design requirements.

[1] "Privacy Working Group Request for Information," House Committee on Energy and Commerce, February 21, 2025, https://d1dth6e84htgma.cloudfront.net/02_21_2025_PWG_Request_for_Info_2_e1753e1356.pdf.

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?

Data controllers warrant heightened regulatory scrutiny due to their decision-making authority, whereas data processors have contractual obligations to data controllers. Thus, the ultimate responsibility should fall onto data controllers to ensure they and their contracted data processors follow the relevant privacy regulations.

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

Data controllers' obligations should include transparent data practices, consent mechanisms, security safeguards, and consumer access rights. Data processors, conversely, require more focused obligations centered on implementing appropriate security measures, processing data according to controller instructions, and reporting security incidents promptly. Due to data controllers' ability to determine the purpose and means for how it processes personal data, liability for failures, such as data breaches, from the data processors should fall on the data controller.

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

No. A size-based approach ignores that firms of all sizes collect and use data and that consumer privacy harms do not depend on the size of the data controller. Entities of any size can cause harm to consumers through privacy violations, making regulation equally important for a smaller or emerging business or a nonprofit organization with limited resources as it is for a larger, established company.

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."

Federal privacy legislation should scope its rules to apply to all data and should not treat digital data in a different way from other forms of data. If privacy protection is the goal, a broad scope is important because privacy risks are not confined to data that is entered digitally. Moreover, having a standard for digitally collected data that is different for data collected in other ways (i.e., over the telephone, collected on a paper form, scanned from a driver's license, etc.) is unfair and discriminatory. However, policymakers should be aware that extending privacy regulations to all kinds of data will significantly increase compliance costs and complexity, in part because the scope of offline data collection is massive and the costs of providing notice, choice, redress, and other consumer measures is much higher for offline than online applications. The only way to square the circle between broad-based coverage and limited economic cost is to ensure privacy regulations are designed to limit the compliance burden.

With this in mind, the definition of personal information should include information that can be used to distinguish or identify an individual or can be linked or are reasonably linkable to that individual. This definition should explicitly exclude de-identified data, including anonymized, pseudonymized, or aggregated data, which would ensure firms have access to data while providing strong privacy protection to individuals.

Meanwhile, the definition of sensitive personal information should include personally identifiable information that likely presents a high risk to individuals if made public. Examples include health-related data, genetic and biometric data, data regarding children under the age of 13, and precise geolocation information.[2]

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

In most cases, opt-out rules for data collection and sharing are better for innovation and productivity while still protecting privacy. Opt-in consent requirements lead fewer users to share their data because most users select the default option of not giving consent, often for irrational reasons. Additionally, obtaining opt-in consent costs significantly more than an opt-out system, wherein users can revoke consent to have their data collected. Given the thin margins involved in data-related transactions such as targeted advertising, companies could end up passing these costs onto consumers. In cases of sensitive personal information, such as health or financial data, opt-in should be the default to ensure the highest levels of privacy align with consumer expectations. However, opt-in requirements are less efficient and costlier than opt-out requirements, so opt-out should be prioritized in all other instances because they benefit consumers, businesses, and the overall economy while protecting consumer choice.[3]

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?

Prescriptive operational requirements—specifically data retention limitations, data minimization mandates, purpose specification limitations, and privacy-by-design requirements—impose excessive compliance burdens and result in lower productivity and higher opportunity costs by reducing access to data, limiting data sharing, and constraining its use. It is important to avoid restrictions on companies' ability to explore and use new data sets to improve products or services. Instead, a federal data privacy law should provide consumers with the right to access, port, delete, and rectify their personal data.[4]

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

Sensitive personal information should require opt-in consent, as opposed to non-sensitive personal information, which should instead utilize an opt-out consent mechanism.

---

[2] Alan McQuinn and Daniel Castro, "A Grand Bargain on Data Privacy Legislation for America" (ITIF, January 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf.

[3] Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules," ITIF, October 6, 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/.

[4] Ash Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (ITIF, August 2022), https://www2.itif.org/2022-light-touch-data-protection.pdf.

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.

The European Union passed its General Data Protection Regulation (GDPR) in 2016, taking a strict approach to privacy that has proven both costly and overly broad. While the EU was right to streamline data privacy regulations across borders—an approach the United States should follow with its own comprehensive data privacy law—passing a GDPR-like law here in America would come with significant costs and may also fail to produce its intended outcomes.[5] After the first year of GDPR enforcement, ITIF's Center for Data Innovation found that the GDPR negatively affects the European economy and businesses while failing to increase trust among users, negatively impacting users' online access, and straining regulatory resources.[6]

Some states have taken inspiration from the GDPR, most notably California, which became the first state to pass a comprehensive data privacy law with its California Consumer Privacy Act (CCPA) in 2018. ITIF estimated that the CCPA would cost $78 billion annually, with California's economy bearing $46 billion and the rest of the country bearing the other $32 billion.[7] California's own study estimated costs of up to $55 billion.[8] Following in Europe or California's footsteps would impose high costs on the American economy compared to more targeted legislation: $122 billion per year compared to $6 billion, 95 percent less.[9]

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.

As of March 2025, 19 states have passed comprehensive data privacy laws, with many more states considering their own legislation.[10] ITIF estimates that if all 50 states passed their own privacy laws, out-of-state enforcement costs could exceed $1 trillion over 10 years, with at least $200 billion hitting small businesses.[11]

In the meantime, while consumers in the 19 states with existing privacy laws benefit from certain rights and protections, consumers in the remaining 31 states are left behind. It makes little sense for two consumers in two different states using the same online service to have different data protections available to them.

---

[5] Johnson and Castro, "Maintaining a Light-Touch Approach."

[6] Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (Center for Data Innovation, June 2019), https://www2.datainnovation.org/2019-gdpr-one-year.pdf.

[7] Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws" (ITIF, January 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[8] Berkeley Economic Advising and Research, LLC, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018," September 2019, https://iapporg/media/pdf/resource_center/standardized_regulatory_impact_assessment_CCPA.pdf.

[9] Johnson and Castro, "Maintaining a Light-Touch Approach."

[10] C. Kibby, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, updated March 17, 2025, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[11] Castro, Dascoli, and Diebold, "The Looming Cost."

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?

Federal privacy legislation should create a single set of data privacy rules for the United States. Consumers should have the same rights and protections regardless of which state they live in, and companies should not be faced with 50 different state laws. This will require federal privacy legislation to preempt state and local government privacy rules, including preempting their ability to add additional protections on top of federal rules for general data processing. This principle does not mean states should completely sit out of the process. States can exercise their authority by providing additional oversight and enforcement through state attorneys general.

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

Wherever possible, a federal data privacy law should prioritize harmonizing key definitions—such as definitions of "personal information" and "sensitive personal information"—with existing sectoral frameworks (i.e., HIPAA, GLBA, FCRA, COPPA) to minimize regulatory fragmentation and avoid overcomplicating compliance. However, a comprehensive law should avoid changes that would do the reverse by complicating compliance for covered entities within those sectors that comply with existing laws as written.

IV. DATA SECURITY

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

Similar to the patchwork of state privacy laws, there is also a patchwork of state data breach notification requirements.[12] This complicates compliance for covered entities that operate in multiple states and creates duplicative enforcement costs, just as the privacy patchwork does. Thus, a comprehensive federal privacy law should include data breach notification requirements that preempt state requirements and set a single standard for all organizations that operate anywhere in the United States.

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?

Congress should avoid conflating data protection with policies on AI or automated decision-making. These are separate issues that each require a different approach. A federal privacy law would address many concerns related to AI's use of consumers' personal data, but other AI-related concerns are outside the scope of a federal privacy law.[13]

---

[12] "Security Breach Notification Laws," National Conference of State Legislatures, updated January 17, 2022, https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

[13] Hodan Omaar and Daniel Castro, "Picking the Right Policy Solutions for AI Concerns" (Center for Data Innovation, May 2024), https://www2.datainnovation.org/2024-ai-policy-solutions.pdf.

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.

Authority should be split between the FTC and state attorneys general, instead of allowing a private right of action that would significantly drive up the cost of duplicative enforcement. By allowing both federal and state regulators to take action on violations of federal privacy law, there would be some duplicative enforcement, costing organizations roughly $210 million per year, but this is a fraction of the projected costs associated with a private right of action, up to $2.7 billion per year.[14]

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?

Given the FTC's established expertise in consumer protection and the efficiency advantages of centralized enforcement, it should maintain its status as the primary regulator for consumer privacy enforcement. State attorneys general, on the other hand, should have secondary enforcement powers as they can address localized privacy violations. For highly sensitive sectors, such as health care and financial services, regulators within those specific sectors can provide specialized expertise.

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

The purpose of a federal data privacy law should be to encourage compliance, not to seek opportunities to punish covered entities. A 30-to-90-day "right to cure" would give covered entities the chance to remedy privacy violations within 30, 60, or 90 days in order to avoid facing penalties. This would encourage compliance, especially by covered entities acting in good faith to comply with the law.

CONCLUSION

Overly broad privacy legislation would come with both significant compliance costs and enormous hidden costs, whereas a more targeted law that still protects consumer privacy would be far less burdensome on organizations, consumers, and the economy. In order to minimize the economic impact of privacy legislation, Congress should pass a comprehensive law that preempts state and local laws and minimizes the costs of data protection while still addressing actual privacy harms and protecting consumer privacy.

Thank you for your consideration.

Ash Johnson
Senior Policy Manager

Alex Ambrose
Policy Analyst

Daniel Castro
Vice President

[14] Johnson and Castro, "Maintaining a Light-Touch Approach."