Comments of Reason Foundation on a Federal Comprehensive Data Privacy and Security Framework

Privacy Working Group
Committee on Energy and Commerce
U.S. House of Representatives

April 7, 2025

Prepared by:

Jen Sidorova
Policy Analyst
Reason Foundation
jen.sidorova@reason.org

Nicole Shekhovtsova
Technology Policy Analyst
Reason Foundation
nicole.shekhovtsova@reason.org

Chair Guthrie, Vice Chair Joyce, and members of the Privacy Working Group,

On behalf of Reason Foundation, we respectfully submit these responses to the prompts contained in the February 21 request for information on the parameters of a federal comprehensive data privacy and security framework. Reason Foundation is a national 501(c)(3) public policy and education organization with expertise across a range of policy areas, including technology policy.[1] Our responses below are numbered to correspond to the individual prompts.

[1] *See* "About Reason Foundation," Reason Foundation website, https://reason.org/about-reason-foundation/.

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.

Efficacy at Protecting Consumers

Comprehensive privacy laws such as the European Union's General Data Protection Regulation of 2016 (GDPR) and the California Consumer Privacy Act of 2018 (CCPA) were enacted with the intent to give consumers more control over their data and set clearer expectations about how that data would be used.[2] However, economic and social science research has not yet determined whether these laws provide meaningful additional protection for consumers. Moreover, these regulations appear to have had unintended negative effects on consumer behavior and business activity.

With respect to Europe's GDPR, our own analysis of the Survey on Internet Trust (Ipsos) found that consumer trust did not change before (2017) or after the introduction of GDPR (2019).[3] Another group of researchers, using the same data, looked at the interval between 2019 and 2022 and found that Internet users' trust in the Internet has actually dropped.[4] We have also previously warned that overbroad privacy regulations could make the Internet less user-friendly.[5]

These concerns have been validated by the findings of a recent study funded by the European Research Council. The authors examined how GDPR affected online user behavior and found it had a negative impact on website traffic.[6] After GDPR took effect, weekly website visits dropped by approximately 5% within three months and by about 10% after 18 months.

These traffic declines caused significant revenue losses—averaging $7 million for e-commerce websites and nearly $2.5 million for ad-supported websites after 18 months.

---

[2] "General Data Protection Regulation," Regulation (EU) 2016/679, European Union, April 2016; California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq.
[3] Jen Sidorova, "Impact of General Data Protection Regulation on Online Behavior," APPAM Fall Research Conference, November 19 2022, https://rb.gy/a6u0k6.
[4] Fen Osler Hampson and Sean Simpson, "Internet users' trust in the Internet has dropped significantly since 2019," Ipsos, November 2022, https://www.ipsos.com/en-us/news-polls/trust-in-the-internet-2022.
[5] Jen Sidorova, "Data analysis suggests privacy legislation may make the internet less user-friendly," Reason Foundation, October 2022, https://reason.org/commentary/data-analysis-suggests-privacy-legislation-may-make-the-internet-less-user-friendly/.
[6] Klaus M. Miller, Julia Schmitt, and Bernd Skiera, " The Impact of the General Data Protection Regulation (GDPR) on Online Usage Behavior," arXiv Working Paper, November 2024, https://arxiv.org/abs/2411.11589.

However, the impact varied depending on website size, industry, and user location. Larger websites suffered less, suggesting that GDPR may have unintentionally favored large websites and increased market concentration by harming smaller competitors.

In an analysis of the California Consumer Privacy Act (CCPA), scholars from the University of California, Irvine, and New York University found significant correlations between the regulation and shifts in consumer behavior on commercial websites. Specifically, Californians decreased their purchases by approximately 4.3% and increased their product returns by 3.0%, resulting in an average reduction of $96 in discretionary spending per consumer within one year of the CCPA's introduction. Browsing behavior data from commercial websites indicates that Californians spent more time online and visited more pages per website, suggesting that increased privacy restrictions may have compelled consumers to expend greater effort to locate suitable products or services.

Impact on Data-Driven Innovation

Europe's GDPR requires businesses to obtain explicit consent before collecting consumer data. This has greatly impacted entrepreneurs, particularly AI startups that rely heavily on large datasets for advanced algorithms like neural networks. Compliance with GDPR significantly limits data access and retention, constraining algorithm training. This may hinder the development of AI products that optimize processes, boost productivity, and deliver economic benefits across industries.

Researchers from Boston University and New York University documented several negative impacts that occurred after GDPR was introduced.[7] They found that GDPR forced AI startups to divert limited resources and create new roles dedicated to compliance—70% of surveyed firms explicitly hired to comply with GDPR, while 63% reallocated resources and about 75% had to delete data. Smaller startups were particularly affected by the large compliance burden. Even firms exempted by having revenue below $1 million faced pressure from investors anticipating future compliance requirements, further disadvantageing smaller AI companies.

Impact on Small Businesses

Empirical evidence from the scholarly economics and management literature finds that comprehensive privacy laws, such as the GDPR, tend to favor large companies over small- and medium-sized businesses. GDPR increased market concentration and harmed

[7] James Bessen and Stephen Michael Impink, "GDPR and the Importance of Data to AI Startups GDPR and the Importance of Data to AI Startups," Boston University School of Law, April 2020, https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=2349&context=faculty_scholarship.

competition because compliance is costly and complex, especially mechanisms such as a "one-time consent" approach.

One study found that market concentration among internet service providers increased by 17% in aggregate just a week after the GDPR was introduced.[8] The research indicates that large firms like Google and Facebook, whose expansive web technology offerings naturally foster greater market concentration, became further entrenched. The primary reason for this shift is that websites tended to end contracts with smaller vendors that could not quickly adapt to rigorous compliance demands.

Supporting this finding, another study showed that Google's market share increased after the GDPR was introduced.[9] The authors argue that while GDPR compliance costs were significant for Google, the relative burden was lower than the compliance burden borne by smaller competitors. Consequently, "some firms—and most strikingly Google—lose relatively less such that their market shares increase after the GDPR."

Regarding technical implementation, "one-time consent"— which involves a single interaction where users grant permission to collect and process their data across multiple services offered by a firm — disproportionately benefits larger companies. Larger firms that offer many services and more frequently interact with users can spread compliance costs over more users, placing smaller firms at a competitive disadvantage.

California's CCPA also has similar implications for small and medium-sized businesses. Although the CCPA technically applies exclusively to California residents, its impact extends nationally. Any business collecting personal information from Californians must comply with the law, regardless of the company's geographic location. Consequently, small businesses across the country, often lacking the financial and administrative resources necessary for complex compliance tasks—such as data mapping, inventory management, and data retention—face substantial challenges and a heightened risk of noncompliance.

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.

There are currently 20 U.S. states with comprehensive privacy laws. All state privacy laws apply to companies that conduct business with state residents, regardless of whether the

[8] Garrett A. Johnson and Scott K. Shriver, "Privacy and Market Concentration: Intended and Unintended Consequences of the GDPR," *Management Science*, Vol. 69, No. 10, March 2023, https://rb.gy/xokoj4.
[9] Christian Peukert and Stefan Bechtold, "Regulatory Spillovers and Data Governance: Evidence from the GDPR," *Marketing Science*, Vol. 41, No. 4, February 2022, https://pubsonline.informs.org/doi/10.1287/mksc.2021.1339.

businesses are headquartered within the state. Exceptions to these laws typically include businesses that, for example, process data of fewer than 100,000 consumers per year and do not derive more than 50% of their revenue from selling personal data.

Currently, the laws define sensitive personal data as including information such as racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, genetic or biometric data, and citizenship or immigration status. However, while there is some general agreement on what kinds of data should be included in the definition of sensitive data, there is a lack of consensus on the precise definition, considerable variation between the states, and disagreement on what level of protection or consent is required. As a result, this patchwork provides uneven rights to consumers depending on their state of residence.

Virginia's and Connecticut's privacy laws, for example, classify certain data from *all* individuals as sensitive—such as precise geolocation data—and regard *any* data collected from children as sensitive. This approach is broader than most other state laws, which do not specifically designate children's data as sensitive. Some states—including California, Colorado, Connecticut, and Virginia—require consent and data protection impact assessments for processing sensitive data so that organizations may identify and minimize the data protection risks of a given activity. Other states, such as Utah, merely require notice and the ability to opt out of processing.

Across all these laws, individuals are granted several rights regarding the accessibility and availability of their data. These rights include the ability to access their personal data that an organization holds, to request deletion of personal data, and to obtain and reuse personal data.

At least 11 states allow individuals to request corrections to their data held by organizations. State consumer privacy laws primarily rely on opt-out rights. Four states (California, Colorado, Connecticut, and Virginia) establish a right to opt out of profiling, which allows consumers to prevent businesses from using their data to make certain algorithmic decisions, such as personalized marketing, credit scoring, or even behavioral predictions. In contrast, many states require opt-in to process sensitive data and data about children. However, some states, such as Utah, simply have an opt-out for all activities involving sensitive data. Each law has a timeframe for responding to a consumer rights request. This timeframe ranges from 30 to 60 days. While these rights empower consumers to control their data, they can present problems for businesses due to the complexity and cost of implementing systems that must comply with varying state laws and then responding to requests for access, modification, or deletion within tight timeframes.

State consumer privacy laws impose specific requirements on businesses to protect and properly handle personal data. These requirements include publishing a privacy notice, implementing "reasonable" data security practices, and collecting and using only the data reasonably necessary for the identified purposes (i.e., data minimization). Data minimization mandates that personal data not be used for new purposes without explicit consent, while data transfers require stringent processing agreements.

Regulations also protect consumers from penalties when exercising their privacy rights. Colorado, Connecticut, New Jersey, and Virginia require data protection assessments when processing activities involving targeted advertising, certain forms of profiling, sensitive personal data, and the sale of personal data. The California Privacy Rights Act, Colorado Privacy Act, and Connecticut Data Privacy Act all target deceptive practices commonly referred to as "dark patterns," which can be interpreted as tricking consumers into making decisions that they didn't intend to make, such as giving more personal data than they believed they were providing.

State attorneys general are usually responsible for enforcing these regulations. An exception is California, which established the California Privacy Protection Agency. Most laws have no private rights of action, except in California, which has a limited private right of action for violations involving a data breach. A private right of action allows individuals or entities to file lawsuits seeking damages or other remedies directly, without relying solely on government enforcement agencies.

The variation in state approaches necessarily increases compliance complexity, and the burden of this patchwork is disproportionately borne by small- and medium-sized firms. Compliance with potentially 50 different state privacy laws was estimated by the Information Technology and Innovation Foundation (ITIF) to cost $239 billion annually, with small businesses bearing approximately $50 billion of these expenses.[10] Additional costs stem from litigation risks in states with private rights of action and market inefficiencies resulting from restricted data use.

While adopting a uniform federal privacy framework would not be costless, it could significantly reduce the burden on small businesses. Ultimately, consumers will bear the burden of higher prices and reduced choices in the marketplace. Furthermore, a patchwork of state privacy laws has already created a confusing and uncertain environment for consumers, as privacy rights can differ dramatically depending on where one lives.

[10] Daniel Castro and Luke Dascoli, "The Looming Cost of a Patchwork of State Privacy Laws," Information Technology and Innovation Foundation, January 2022, https://www2.itif.org/2022-state-privacy-laws.pdf.

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?

Regarding comprehensive data privacy laws and degree of preemption, one approach favors uniform rules for simplicity and consistent consumer protections, while another respects states as policy laboratories that can tailor rules locally. "Floor preemption" establishes federal minimums but allows states to adopt stricter rules, preserving state autonomy but potentially creating a complex patchwork of standards. By contrast, "ceiling preemption" enforces a uniform maximum standard, reducing compliance challenges but potentially stifling state innovation and lowering protections where more robust laws exist.

Privacy bills introduced in previous Congresses proposed what some might call "ceiling preemption" but still preserve portions of state law. For example, the American Data Privacy and Protection Act explicitly carved out categories of policies that would remain within state control, such as consumer protection laws of general applicability, civil fraud statutes, children's data protections, and certain biometric data regulations.[11] The American Privacy Rights Act similarly adopted a broad approach to preempting state privacy laws while still exempting certain areas such as consumer protection and civil rights laws.[12] Critics, particularly those in California, worry that these bills might erode stronger state laws over time or block them from adopting new rules in emerging areas like AI or targeted advertising.

Federal privacy statutes have evolved over time in the types of preemption they apply. Early federal laws such as HIPAA, the Gramm-Leach-Bliley Act, and the Electronic Communications Privacy Act largely relied on floor preemption, allowing states to enact stricter rules. More recent federal legislation—such as the Children's Online Privacy Protection Act (COPPA), the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM Act), and updates to the Fair Credit Reporting Act—has introduced stronger preemption provisions, signaling a trend towards greater uniformity and predictability.

The lack of strong preemption leads to multiple overlapping or contradictory laws that can confuse consumers and demand extensive business compliance efforts. A single federal standard would simplify that landscape and potentially make educating the public about their rights easier. Yet, from the perspective of states like California—where the landmark California Consumer Privacy Act (CCPA) has set one of the highest bars for privacy

[11] American Data Privacy and Protection Act, H.R. 8152, 117th Congress, § 404(b).
[12] American Privacy Rights Act of 2024, H.R. 8818, 118th Congress.

protections—there is little incentive to accept any federal law that diminishes existing safeguards or restricts the capacity to legislate further.[13]

Past comprehensive privacy proposals from Congress have favored a hybrid approach to preemption: offering broad, uniform national requirements while carving out space for states to maintain certain laws—especially those dealing with emerging technologies or local concerns. Yet, these exemptions did not satisfy state critics.

Finding the "right" degree of preemption likely involves:

1. Setting a Strong Federal Baseline: Outline core principles for handling personal data—such as clear consent requirements, data minimization standards, robust transparency, and breach notification—and ensure every state meets these minimum requirements.

2. Allowing Carefully Targeted Carveouts: Preserve specific state laws that address unique local issues, protect more sensitive categories of data (e.g., biometric or genetic information).

3. Revisiting Standards Over Time: Mandate regular federal reviews that enable updates to data protection laws, ensuring that the national framework can adapt to technological evolution and that states can request permission to go beyond federal requirements in narrowly defined circumstances.

IV. Data Security

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

Although privacy and security are related, they are distinct concepts that do not necessarily have to be legislated together.

Privacy laws are designed to govern the collection, use, and sharing of personal data, whereas security laws focus on protecting that data from unauthorized access and breaches.

A federal law emphasizing increased security must set clear requirements to ensure that sensitive personal information, or personally identifiable information, is managed to minimize the risk of exposure while preserving its utility for legitimate purposes. By working with industry to set standards for data minimization and ensuring that stored data is either anonymized or securely encrypted, we can reduce data breach risks while fostering innovation.

[13] California Consumer Privacy Act of 2018, AB 375.

The U.S. regulatory environment for cybersecurity is currently a patchwork of overlapping state and federal guidelines. Between 2014 and 2023 alone, according to data collected by the National Conference of State Legislatures, over 550 bills addressing various aspects of cybersecurity—from incident response to election security—have been introduced.[14] This fragmented approach has often pushed organizations to adopt a compliance-first mindset rather than a proactive security strategy as they grapple with conflicting requirements from multiple jurisdictions. Unified cybersecurity standards may help reduce this regulatory confusion. By harmonizing requirements across states, companies can focus on genuine threat mitigation rather than merely checking off compliance boxes.

Any sound approach to a national data security policy requires three elements. First, regulatory coherence must be achieved. By setting unified standards and facilitating voluntary coordination among federal agencies—such as CISA, FCC, and SEC—policymakers can simplify the regulatory landscape. Second, public-private partnerships should be deepened. Effective cybersecurity relies on collaboration between industry and government, where information sharing and joint innovation can address emerging threats. Third and finally, leveraging advanced technologies. The use of artificial intelligence in security operations can automate threat detection and response, thereby bolstering defenses against sophisticated adversaries.

In summary, increasing the security of Americans' personal information through federal comprehensive privacy legislation involves setting unified standards that require data to be both protected and responsibly managed.

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?

State governments have recently pursued independent automated decision-making (ADM) frameworks. Colorado's comprehensive AI law mandates annual impact assessments for high-risk AI systems to prevent algorithmic discrimination, applying stringent obligations to both private and government entities.[15] Illinois amended its Human Rights Act to explicitly prevent employment discrimination through ADM, requiring transparency and notice.[16] New York City's Local Law 144 similarly necessitates bias audits for automated employment tools, ensuring transparency and granting candidates opt-out rights.[17]

---

[14] National Conference of State Legislatures, "Cybersecurity 2023 Legislation Summary," January 2024, https://rb.gy/tw46pe.
[15] Colorado Artificial Intelligence Act, SB 24-205 (effective February 1, 2026).
[16] Illinois Human Rights Act Amendments, HB 3773 (effective January 1, 2026).
[17] New York City Local Law 144 of 2021, "Automated Employment Decision Tools (AEDTs)."

APRA similarly addresses ADM, emphasizing transparency and accountability through mandatory impact assessments, notices, and opt-out opportunities for decisions significantly affecting individuals (e.g., employment, housing, credit).[18] While aiming to safeguard privacy, its data minimization principle poses potential limitations on the breadth of data available for training innovative AI systems.

AI systems frequently assist in making decisions in areas like employment, finance, health care, housing, and insurance—often using personally identifiable information as part of their operations. Some legislative proposals, such as the Colorado Artificial Intelligence Act (CAIA) and the Texas Responsible AI Governance Act (TRAIGA), would subject these AI tools to rigorous and potentially expensive compliance measures, regardless of the actual extent of their influence on final decision-making.

Federal laws like ADPPA and APRA could unify the fragmented state landscape, simplifying compliance for businesses operating nationally, as demonstrated by a 2021 American Action Forum report revealing that California's privacy law alone imposed $55 billion in initial compliance costs on businesses.[19] However, broad federal preemption could inadvertently undermine state-driven innovations or stronger local protections. States have actively filled gaps left by federal inaction, offering tailored protections against algorithmic discrimination, particularly in sensitive sectors such as employment and credit. Comprehensive federal preemption risks eliminating state experimentation and nuanced local solutions unless carefully limited. The Electronic Privacy Information Center (EPIC) and the United States Public Interest Research Group's (U.S. PIRG) 2024 assessment of state privacy laws suggests that comprehensive federal legislation could offer uniform minimum standards without restricting states' ability to implement targeted higher protections.[20]

Inadequate federal preemption may burden businesses with overlapping or conflicting regulatory obligations, increasing costs and deterring innovation. National enterprises face complex compliance challenges with varying state ADM requirements, including differing transparency rules, auditing standards, and consumer opt-out provisions. A carefully structured federal baseline could mitigate this burden, establishing clear and consistent requirements for algorithmic accountability while preserving essential state civil rights protections.

---

[18] American Privacy Rights Act (APRA), H.R. 8818, 118th Congress, § 13.
[19] Jennifer Huddleston, "The Price of Privacy: Analyzing the Economic Impact of California's Privacy Legislation," American Action Forum, June 3, 2021, https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/.
[20] Electronic Privacy Information Center and U.S. PIRG Education Fund, "The State of Privacy: How state 'privacy' laws fail to protect privacy and what they can do better," February 2024, https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf.

To effectively align federal privacy legislation with state AI frameworks, Congress should consider the following recommendations:

- Clear and consistent definitions: Provide explicit definitions for key terms like "automated decision-making," "algorithmic discrimination," and "significant effects," ensuring clarity for businesses and facilitating smoother compliance across jurisdictions. Adopting uniform definitions for terms like "artificial intelligence" and "automated decision-making" would also allow for greater compliance certainty and minimize intra-governmental confusion.
- Strategic and limited preemption: Adopt targeted federal preemption to standardize core requirements, such as impact assessments and transparency audits, without precluding states from maintaining or establishing additional protections in critical areas like civil rights or sector-specific safeguards.
- Flexibility and innovation incentives: Emphasize outcomes-based regulation rather than prescriptive technical mandates, encouraging companies to innovate in compliance methods. Incentivize voluntary adoption of best practices through regulatory safe harbors and federal support for accessible compliance tools, particularly benefiting small and medium-sized enterprises.

Respectfully submitted,

Jen Sidorova
Policy Analyst
Reason Foundation

Nicole Shekhovtsova
Technology Policy Analyst
Reason Foundation