The Fragmented Privacy Landscape

Submission to the House Committee on Energy and Commerce's Request for Information on a Data Privacy and Security Framework[1]

The Current State of Privacy Regulation

The United States is experiencing a rapid proliferation of state-level privacy laws, creating an increasingly complex regulatory landscape. Since California pioneered comprehensive privacy legislation with the California Consumer Privacy Act (CCPA) in 2018, the trend has accelerated dramatically. Currently, 19 states have enacted their own privacy legislation, each with unique requirements, enforcement mechanisms, and compliance frameworks.

The layered approach that has emerged, with states each protecting their citizens, is creating problems. The internet's inherently borderless nature means that companies must simultaneously comply with numerous, at times conflicting, regulatory regimes. This leads to substantial duplication of effort, bespoke legal reviews, and customized technical architectures, all of which drive up compliance costs. For large companies, this means building out expansive legal and engineering teams to keep up. For smaller firms, it often means pulling back from certain states entirely, simply because the cost of compliance outweighs the potential revenue.

The result is a regulatory environment where cost—not conduct—determines who can afford to participate. This, in turn, raises the barrier to entry, distorts competition, and undermines the original consumer protection goals of privacy legislation.

The House Energy and Commerce Committee deserves credit for reengaging federal privacy legislation. In a policy space that has long been stalled by jurisdictional turf wars and ideological standoffs, the Committee's willingness to put forward a serious, bipartisan proposal represents a step forward. But this momentum should not obscure a hard truth: there are real costs to privacy regulation, no matter how well-designed. Any national standard, especially one that includes private rights of action, new enforcement authorities, and mandatory technical requirements, will carry financial and operational burdens, particularly for smaller firms. Lawmakers should proceed with humility, recognizing that even the best-intentioned privacy frameworks must be crafted with an eye toward economic sustainability and proportionality.

The Two-Path Dilemma: Congress v. States

The current trajectory presents two distinct paths forward: Option A and Option B.

[1] The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

In Option A, privacy bills are passed in each state legislature, expanding from the current 19 states to all 50 states. Option A is the baseline. It is what is being chosen in the absence of choosing Option B, which is a federal privacy bill. There is precedent for Option A in the development of data breach notification laws in the United States. In 2002, there were no data breach laws, which force companies to announce when they have been breached. One by one, states started adopting data breach notification laws. Now, every state has one.

Option B is a negotiated agreement in Congress: a federal privacy bill. The drive to harmonize privacy law and create one set of rules has made a federal privacy bill a live issue for over a decade. However, federal online privacy legislation has never successfully crossed the finish line. The fact that Congress hasn't passed anything underscores how much political capital would have to be spent to achieve a consensus.

The drawbacks of Option A:

1. Compliance Complexity: Companies face enormous challenges in managing compliance across multiple jurisdictions, leading to increased operational costs and legal uncertainty.
2. Technical Compliance Challenges: As noted by one Big Tech legal team member, "We will be defensible, but I am not sure we could ever be technically compliant." This highlights the fundamental difficulty of achieving perfect compliance with numerous overlapping regulations.
3. Competitive Disadvantages: Small and medium-sized businesses would be disproportionately impacted, as they lack the resources to navigate complex multi-state compliance requirements, potentially creating market concentration effects similar to those observed after the General Data Protection Regulation (GDPR) was implemented in Europe.
4. Inconsistent Consumer Protections: American consumers would receive varying levels of privacy protection based solely on their state of residence, creating an uneven protection landscape.

The drawbacks of Option B:

1. Preemption Concerns: Democratic lawmakers, particularly from states with robust privacy laws such as California and Illinois, have resisted broad preemption provisions that would supersede their existing state protections.
2. Private Right of Action (PRA): There remains disagreement about the scope and timing of individuals' right to sue companies for privacy violations. The American Data Privacy and Protection Act (ADPPA) proposed a four-year delay before PRA implementation, while the American Privacy Rights Act (APRA) reduced this to 180 days.
3. Enforcement Mechanisms: Some have pushed for stronger enforcement measures, including limits on forced arbitration and a broad right for individuals to sue companies that violate the law.
4. Cure Periods: The appropriate grace period for companies to address violations after notification remains contentious, with ADPPA proposing 45 days and APRA suggesting 30 days.

Economic Impact Assessment

There is no denying that privacy bills are expensive.[2] When California ran the numbers for its 2018

[2] Rinehart, Will. (2022). What is the cost of privacy legislation? A Collection of Estimates. https://www.thecgo.org/benchmark/what-is-the-cost-of-privacy-legislation/

California Consumer Privacy Act, it estimated the initial compliance costs would land at $55 billion, about 1.8 percent of the gross state product (GSP).[3] As for the upper bound, estimates suggested the bill could have cost as much as 4.6 percent of GSP.

Privacy bills shift the power relations between internet players. While research on US privacy laws is limited, studies on the impact of Europe's GDPR give us a sense of what to expect. After it went into effect, smaller vendors were more commonly dropped by the bigger players, which increased the relative concentration of the vendor market by 17 percent. [4] Users spent less time on European websites and the number of deals in the EU backed by venture capital dropped by 26.1 percent compared to their American counterparts.[5] In other words, policymakers should expect market concentration effects, consumer engagement decline, an investment chilling effect, and competitive disadvantages after passing privacy laws.

Toward a Minimum Viable Regulation Approach

Policymakers should be approaching privacy law through the lens of a minimal viable product—an MVP. MVPs are products designed with sufficient features to draw in early adopters and confirm the viability of a product concept. Why not apply this idea to regulation? A minimum viable regulation would focus on creating a targeted regulatory framework with sufficient scope to address core privacy concerns while remaining adaptable and minimizing compliance burdens. It would be limited in scope and would produce information about the viability of enforcement.

A privacy MVP could be built around compliance with the NIST Privacy Framework.[6] The Ohio Personal Privacy Act (OPPA) encourages businesses to adopt the NIST Privacy Framework as a standard for developing privacy policies, granting them an affirmative defense against legal claims if they adhere to it. Congress can do the same at the federal level. If you adhere to the NIST privacy framework, then certain legal protections would apply, creating a safe harbor that incentivizes adoption without imposing excessive compliance burdens. In a policy environment increasingly defined by gridlock, complexity, and unintended consequences, a minimum viable regulation may be the only viable regulation.

Conclusion

As discussions in Congress continue to evolve toward a potential federal privacy framework, stakeholders would be well-advised to advocate for thoughtful, targeted approaches that recognize the complex trade-offs inherent in privacy regulation and seek to maximize benefits while minimizing economic and competitive disruption.

A national privacy framework will inevitably impose financial and operational burdens that

---

[3] Roland-Holst, D., Evans, S., Behnke, D., Neal, S., Frolund, L., & Xiao, Y. (2019). Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations. https://web.archive.org/web/20190830173026/http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf

[4] Johnson, G., Shriver, S., & Goldberg, S. (2019). Privacy & Market Concentration: Intended & unintended consequences of the GDPR. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3477686

[5] Jia, J., Jin, G. Z., & Wagman, L. (2019). The short-run effects of GDPR on Technology Venture Investment. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912

[6] *Privacy framework*. NIST. (2025). https://www.nist.gov/privacy-framework

disproportionately impact smaller businesses. Moving forward requires balancing bold ambition with prudent restraint—crafting privacy protections that serve consumers while maintaining economic viability through proportional requirements and implementation timelines. The path to effective privacy legislation lies not in regulatory maximalism, but in thoughtful frameworks that protect both individual rights and market innovation.