



Perspectives from FSF Scholars
May 7, 2026
Vol. 21, No. 22

The House Builds a Sound Privacy Bill

by

Michael O’Rielly *

The issue of commercial privacy – and in particular the subset of online privacy – has bedeviled federal policymakers for decades. For one reason or another, efforts to craft and advance privacy legislation in Congress have stalled, imploded, or been overtaken by other priorities. Seeking a new approach, the House of Representatives’ Energy and Commerce Committee held listening sessions to hear from interested parties and gather input.

The result of that process is the newly drafted Securing and Ensuring Consumer Uniform Rights and Enforcement over Data Act (“SECURE Data Act”), a comprehensive commercial privacy bill that tackles the hardest topics head-on and lands in relatively favorable territory. If enacted, the bill would establish reasonable national privacy standards with federal preeminence in this critical area of American and global commerce. It would also establish a sensible enforcement structure. At this stage, the bill is a refreshing effort to improve consumers' lives without imperiling important business activities and is worthy of everyone’s support.

New Privacy and Security Requirements

From the outset, the bill lays down firm but seemingly sensible obligations for most companies – online and otherwise – that collect, process, or sell consumer data. It gives consumers seemingly inalienable rights over certain types of information they provide to companies, including the right to control how data about them is collected and used (e.g., access, knowledge, and deletion). Some conservatives may find these rights too generous and inappropriate, especially the right to delete accurate data, but the bill serves as a counterpoint to an overarching,

overreaching baseline established by many state privacy laws. It would also limit data collection to only what companies need to do their jobs, which, hopefully, is meant to be expansive, but would narrow today's universe of unlimited data extracted and used. Consumers would be able to exercise these rights without financial or operational impact or penalties from data collection companies.

Additionally, the bill would require companies to maintain adequate data security to prevent consumers' data from being misused, stolen, or abused. Strengthening data protection and care would help mitigate data breaches and their negative consequences for consumers. This requirement should not be overly burdensome, as most companies are already well aware of the financial risks associated with poor data security practices and already exceed current safety norms by virtue of their investments of time and resources. This requirement should complement the enormous efforts made by the vast majority of private sector firms to protect consumer data.

Strong Preemption and No Individual Private Rights of Action

The tradeoff for this expansive privacy protection regime is strong federal preemption that recognizes the interstate nature of data collection and consumption. That means competing, conflicting, and overaggressive privacy regimes created by states would no longer apply. The bill's drafters properly recognize that instantaneous omni-directional data flows are impervious to the political boundaries of our individual states. The bill gives companies a single privacy framework to work under, rather than expending significant resources to comply with convoluted or unworkable state and local statutes. To argue that preemption should not be included, or shouldn't be absolute, ignores the importance of data in modern commerce, the reality of how data currently flows between networks, and the U.S. Constitution's Commerce Clause. As a key element of privacy legislation, this should remain non-negotiable.

The reestablishment of a national market for consumer data flows is noteworthy. Today, some 20 or more states, depending on how it is counted, have enacted data privacy regimes in some form. This is like trying to wrestle with stray wire hangers, keeping them aligned for transport back to the cleaners. For companies that collect and use data, which is almost every single one, this isn't a case of following the rules of the most stringent state, a regulation-up approach, if you will. Instead, companies have found themselves fighting to remain in compliance, particularly when the obligations in one state conflict with those in another. This has forced companies to pick and choose which U.S. markets in which to compete, thereby avoiding potential compliance issues. Consumers lose out in these circumstances, as state legislators, intentionally or unintentionally, restrict benefits and services, making states and our nation less competitive. It is the exact reason our Founders crafted the Commerce Clause.

Additionally, the bill rightly excludes another flashpoint for privacy advocates: a new private right of action for aggrieved consumers. This is a sound policy choice, as it prevents abusive class-action lawsuits by trial attorneys that have plagued many other sectors of our economy, including telemarketing. Protecting privacy cannot become another cash cow for lawyers crowding state courts and extorting companies trying to comply with the rules. In its place, the bill explicitly authorizes individual state attorneys general to enforce its provisions and empowers the Federal Trade Commission (FTC) to do the same. The bill establishes a thoughtful

notice-and-coordination process to ensure some semblance of order in enforcement. Thus, the bill creates a symbiotic relationship among states, the FTC, and a new federal privacy statute.

The lack of formal FTC rulemaking authority is consistent with the agency's existing mandate and most prior Congressional authorizations. The provisions of the bill, if enacted, are quite clear and reasonable. To the extent they are not, court precedent will resolve any differences, and companies can go about their business, as has been done in the majority of FTC jurisdictional cases. Here, the bill adequately charges the FTC with aggressively enforcing its provisions against bad actors. The last administration showed the dangers of granting the agency rulemaking authority, as the FTC tried to impose itself and create regulatory restrictions that Congress did not authorize. An overaggressive regulatory FTC is not in the privacy interests of American consumers. Too often, agency rulemaking authority has been abused years or decades after the original statute was enacted. It is appropriate for the SECURE Act to recognize and avoid this exact scenario.

In the winding, twisted road of federal data privacy bills, the Energy and Commerce Committee Republicans have seized the moment and narrowly tailored a possible solution that appears to enhance consumer protections without unfairly hindering American data commerce flows. The SECURE Act balances new consumer privacy rights, which are arguably generous, with appropriate preemption of conflicting state laws, the absence of an individual private right of action, and sensible authority for states and the FTC to enforce their provisions.

This carefully crafted bill, which wouldn't be necessary except for state dalliance in federal jurisdiction, may very well provide the certainty and consistent rules that data-engaged companies need to best serve consumers and protect their privacy.

* Michael O'Rielly, a former FCC Commissioner, is an Adjunct Senior Fellow at the Free State Foundation, an independent, nonpartisan free market-oriented think tank located in Potomac, Maryland. He is the host of the "TMT With Mike O'Rielly" videocast. The views expressed in this *Perspectives* do not necessarily reflect the views of others on the staff of the Free State Foundation or those affiliated with it. The author has a long engagement in the issue of commercial privacy that began over 25 years ago, as he was integrally involved in one of the first comprehensive privacy reviews and legislative efforts attempted by Congress, leading to the drafting of the Consumer Privacy Act of 2002, which was the subject of multiple hearings before introduction and afterward, but never received further action. He was also involved in subsequent legislative efforts in the U.S. Senate and directly engaged in regulatory aspects, including authority and enforcement, while at the Federal Communications Commission.