Insight

Securing Comprehensive Privacy Reform: The Federal Fix to the Patchwork Problem

NICK KROSSE | JUNE 2, 2026

Executive Summary

- The United States is the only major economy without a comprehensive consumer data privacy law; in the absence of such a federal framework, states have enacted a patchwork of data privacy laws that increase compliance costs for businesses both large and small.
- The SECURE Data Act is the latest congressional proposal to create a comprehensive federal data privacy standard for consumers in every state, while preempting the state patchwork of data privacy laws and creating a mechanism to develop industry-specific codes of conduct backed up by Federal Trade Commission and state attorneys general enforcement.
- While critics argue the bill offers insufficient protections relative to the strongest state privacy laws, the existing state patchwork puts businesses in the position of having to focus on navigating minor differences in state laws rather than protecting privacy; a better approach would be to enact a single federal standard with incentives for industries to adopt stronger codes of conduct backed by government enforcement.

Introduction

In the past decade, as technology increasingly mediates our daily lives, demand for data privacy laws has grown across developed economies. The United States is the only G20 economy without a national privacy law covering every industry. In this gap, 21 states have enacted comprehensive privacy laws, leading to a patchwork of laws that are increasingly costly for businesses to coherently comply with.

In the wake of previous failed attempts to pass a national comprehensive data privacy law, the House Energy and Commerce Committee is currently considering the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act). The bill establishes a federal privacy standard based on existing provisions in state privacy laws, creating a baseline set of rights and expectations for all consumers nationwide. It furthermore preempts state privacy laws and contains innovative provisions allowing the creation and registration of voluntary industry-specific codes of conduct that must meet or exceed the act's requirements.

The bill faces opposition from congressional Democrats and consumer groups, which argue that the framework offers insufficient protections for consumers, excessively preempts state privacy laws, and lacks a private right of action. But the existing state patchwork puts businesses in the position of having to focus on navigating minor differences in state laws rather than protecting privacy. A better approach would be to enact a single federal standard with incentives for industries to adopt stronger codes of conduct backed by government enforcement.

Background

With the growth of the internet and computing in the past few decades, our daily lives have increasingly been mediated through technology. From 2000 to 2025, the percentage of Americans adults reporting that they use the internet grew from 52 percent to 96 percent. In 2025, 91 percent of American adults reported owning a smartphone, up from 35 percent in 2011. The "Internet of Things" (IoT) has connected many everyday household items to the internet as well: In 2024, households and businesses were using 18.5 billion IoT devices worldwide, more than double the 7 billion in use in 2018.

This increase in internet usage and connected devices has also necessitated and allowed for the generation and collection of more consumer data. Often, this data generation and collection benefits consumers. For example, consumer data can reduce search and matching costs for consumers and businesses through targeted advertising. It can also help to prevent fraud, enable faster product innovation, and make goods and services lower-cost, free, or even just available to begin with. But consumers face risks as well, particularly from data breaches, or even data being misused after being acquired legally.

In the wake of a spate of data breaches in the latter part of the past decade, demand for comprehensive privacy laws swept developed economies, starting with the European Union's General Data Protection Regulation (GDPR) internationally and the California Consumer Privacy Act (CCPA) in the United States. At the federal level, several, mostly industry-specific, privacy laws exist that predate the recent push for general privacy laws

covering the entire economy. The most industry-agnostic federal law concerning privacy is the Federal Trade Commission (FTC) Act, which merely forbids companies from engaging in "unfair and deceptive practices" as a general matter. While Congress has considered several proposals for a comprehensive federal privacy law since 2018, no proposal has yet been voted on by either chamber, much less passed.

The Patchwork Problem

In the vacuum created by Congress' inaction, 21 states have enacted comprehensive privacy laws. The first, as mentioned above, was California's CCPA, passed by voters through a ballot initiative in 2018, and subsequently amended by a second ballot initiative in 2020. The CCPA was the first law at the state or federal level to establish general consumer data access, deletion, correction, and collection opt-out rights, alongside a web of data transparency, minimization, security, and monitoring requirements on businesses large and small. The California Consumer Privacy Rights Act, which amended the CCPA, also established a new agency, the California Privacy Protection Agency (CPPA), to enforce the CCPA. The CCPA granted that agency (and before it, the state attorney general) broad rulemaking authority, which has allowed the CPPA to expand the reach of the CCPA even further. Unlike any of its subsequent counterparts in other states, the CCPA also governs employee and business-to-business data and gives consumers a narrow private right-of-action over data breaches.

Beginning with Virginia and Colorado in 2021, several states began passing comprehensive privacy laws based on the "Washington Privacy Act" model. This model abstractly provides the same kinds of rights to consumers and imposes similar obligations on businesses as the CCPA, albeit with important practical differences in these core rights and obligations. No state law based on the Washington Privacy Act model provides a private right of action for consumers, instead relying on enforcement by the respective state's attorney general, and only a few authorize any rulemaking by state agencies. Twenty states ultimately adopted this model, although each state has passed this model with its own variations on the underlying definitions, rights, and obligations.

Two recent state laws based on the Washington Privacy Act model are illustrative of the patchwork problem. Maryland's Online Data and Privacy Act introduces a new data minimization standard that is even stricter than California's and bans the sale of sensitive data even with customer consent. Minnesota's Consumer Data Privacy Act requires that businesses maintain an inventory of data that has been collected and processed. Both laws demonstrate that even while 20 of the 21 states with a comprehensive privacy law has modeled it on similar rights, obligations, and definitions, the insertion or alteration of one provision by a state can dramatically increase compliance costs in terms of money, time, and

risks. Furthermore, it shows that interstate companies can no longer simply comply with the strictest state regime, as different states may have stricter requirements on different margins.

The Federal Fix

Following two failed attempts to pass a comprehensive federal privacy framework over the past two congresses, the House Energy and Commerce Committee is now examining the SECURE Data Act as a potential federal, economy-wide privacy framework. The SECURE Data Act is based on the Washington Privacy Act model used by all but one state with a comprehensive privacy law. It contains provisions covering consumer rights and business obligations that align with provisions enacted by states controlled by both Democrats and Republicans. While it does not contain some of the stricter provisions from versions such as Maryland's or Minnesota's, it goes further than most state laws in other ways. For example, it creates the first registry of "data brokers" (companies that collect personal information from third parties rather than directly from consumers) to make it easier for consumers to exercise rights created under the law. It also raises the age required for obtaining parental consent for processing sensitive data to 16 from the current 13 in the federal Children's Online Privacy Protection Act (COPPA).

The SECURE Data Act also preempts all state comprehensive privacy laws, ensuring one national baseline for all sectors of the economy. Having a single national standard to comply with reduces costs associated with duplication of compliance efforts where state laws vary. This is particularly true for small businesses, which, due to varying applicability thresholds at the state level, may have to comply with privacy laws in states where they do not regularly operate but may have few customers. While critics object that this will leave states without a role in regulating privacy, it empowers attorneys general to enforce the law alongside the FTC, still giving states a critical role in protecting their residents. Furthermore, nearly 30 states covering more than 40 percent of the U.S. population have no comprehensive privacy law; The legislation would give those state attorneys general new tools to protect their citizens.

Additionally, the SECURE Data Act offers an innovative mechanism by which industries can develop their own voluntary codes of conduct to be overseen by independent third parties and submit them to be enforced by the FTC. Companies that adhere to these guidelines will be given a rebuttable presumption that they are not violating the law. But if companies fail to adhere to the guidelines they agreed to, the FTC and state attorneys general can use their enforcement powers under the Act to ensure compliance and obtain relief for consumers.

What constitutes good practices for data collection, security, and privacy is dependent on the context in which the data will be used, which is more likely to vary based on industry-specific use cases rather than geography. For example, the automotive and advertising industries have very different use cases for consumer data: The former is concerned with helping customers diagnose mechanical problems or call emergency services, while the latter connects buyers and sellers more efficiently. Both serve different needs for consumers and need to approach issues of collection and minimization differently. U.S. federal privacy law already reflects this with its current sector-based approach to privacy. Furthermore, the legislation's inclusion of independent third-party overseers as well as the backstop of enforcement through FTC and state attorneys general are both critical to ensure the success of this mechanism. Through this innovative provision, the SECURE Data Act would provide consumers with a consistent baseline of privacy expectations to rely on across the economy while also giving flexibility to different industries to adapt to changing technological and social circumstances.

Critics of the legislation also object to the lack of a private right of action for consumers to bring lawsuits against companies they believe are violating or have violated the act themselves. Yet no existing state comprehensive privacy law has a general private right of action for consumers (as noted above, California has a limited private right of action for data breaches). Furthermore, many of the existing industry-specific federal privacy laws also lack general private rights of action, including those that cover health and financial information (except for credit reports). For those that do, because the actual financial damages individuals experience from privacy violations tend to be relatively small (often not exceeding the low thousands), a significant portion of awards end up being paid out in attorney's fees and other court costs, without any of the general enforcement benefits that FTC or state attorney general suits provide.

Legislative Outlook

The SECURE Data Act is being considered by the House Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade. While it has been endorsed by Republican leadership on the committee, objections from Democratic leadership on the committee demonstrate that it may face an uphill battle in garnering enough support to pass both chambers of Congress. Regardless of whether it succeeds where previous attempts have failed, the underlying principles it contains are essential components of any future federal privacy law. Privacy concerns transcend geographic constraints and instead are driven more by the context in which the data will be used. The SECURE Data Act fixes the web of compliance created by the state patchwork and replaces it with a baseline that all consumers can expect across the economy, and gives industries,

small businesses, and federal and state enforcers the tools to develop more robust protections for consumers based in actual data use cases.