Insight

# The Latest on Federal Privacy Legislation

JEFFREY WESTLING | MAY 31, 2022

**Executive Summary**

- Many have called on Congress to develop federal privacy law that would establish baseline rules for the collection and use of consumer data, as well as an enforcement regime to protect consumers.
- Any privacy legislation would need to resolve two key issues that have thus far stalled negotiations between Democrats and Republicans: whether the legislation should include a private right of action (under which an individual harmed by a data security breach can sue) and whether it should preempt state laws governing data privacy.
- A federal private right of action to address privacy violations would increase costs for businesses, but proponents of such a provision worry that without it, overwhelmed federal agencies would not be able to fully address consumer harm; nevertheless, a limited private right of action with a right to cure, limited potential damages, and a strict scienter requirement could garner bipartisan support.
- Preemption of state privacy laws would limit compliance costs for businesses but would require sufficiently robust federal legislation that would adequately protect consumers and perhaps even enforcement from state attorneys general to garner bipartisan support.

**Introduction**

Congress has long discussed a federal privacy framework governing how firms can collect and use data, but thus far a few roadblocks have ultimately prevented bipartisan agreement. While both parties generally agree on the protections that legislation should include, they have not been able to agree on whether individuals should be able to bring an individual claim in response to privacy violations and whether the legislation should preempt state legislation. As a result, lawmakers have made little progress toward a comprehensive privacy framework.

The lack of agreement hasn't dampened all hope, however. Both parties seek to regulate the technology sector, and while there is little agreement between them on potential antitrust and content moderation legislation, many lawmakers see privacy as the preferrable path forward to regulate "Big Tech." Many states have already drafted and passed their own privacy legislation, including California and Virginia. A federal privacy framework could gain bipartisan support, while also protecting consumers from bad practices. Congress may soon take up the issue again, though probably after the midterm elections.

This primer breaks down the key provisions that will be included in any national framework, as well as the major sticking points for potential privacy legislation.

**Major Components of Comprehensive Privacy Legislation**

Federal privacy legislation could take a variety of forms, and multiple provisions already exist for targeted

protections such as health care or children's privacy. A comprehensive framework as currently discussed generally includes some basic provisions.

The first provision is a set of rights for users or restrictions on businesses' use of consumer data, which constitutes the bedrock of a privacy framework. For example, both Senator Wicker's SAFE DATA Act and Senator Cantwell's Consumer Online Privacy Rights Act (COPRA), which was introduced in 2019 but not reintroduced in this Congress, would require businesses to allow consumers to access, correct, or take their data to competing services, though the specific bounds of these requirements vary. Stronger protections generally create additional costs for businesses, and these tradeoffs would require a delicate balancing from Congress to maximize consumer protection without unduly burdening the economy.

The second key aspect of a privacy framework is transparency, which sometimes can be incorporated into the rights section above. Transparency, in this context, refers to a platform making available privacy policies in a comprehensible form so that users can understand what data is collected and how it is used. Often, data collection and use provide significant benefits to users, such as lower prices and better services, but not all users value these benefits the same, nor do they value the risks the same. Transparency allows users to make informed decisions about which products or services to use based on the variety and scale of data these platforms collect. When a firm fails to adhere to the provisions outlined in the privacy policy, the Federal Trade Commission (FTC) can bring action against the firm using its Section 5 deception authority to bring injunctive relief and monetary fines upon violation of a consent decree.

The third and final key aspect of a comprehensive privacy framework is the enforcement regime at the FTC, specifically regarding the agency's rulemaking authority. The FTC acts as the primary privacy enforcer in the United States, and most legislative frameworks rely on the FTC to enforce their provisions. Yet many see the FTC's current authority as somewhat limited in this regard because it cannot impose civil penalties for a first-time offense. This means, in practice, that the FTC must order the firm to stop violating its policy before it can impose fees.

In addition to civil penalty authority, many privacy bills would expand the FTC's authority to issue rules related to privacy. Currently, the FTC is subject to strict rulemaking procedures when issuing unfair or deceptive acts or practices rules, which create high barriers to the FTC issuing enforceable privacy rules. A comprehensive privacy framework often includes a grant of rulemaking authority subject to the Administrative Procedure Act, which in general are much less burdensome for the agency. The scope of this authority varies, but FTC rulemaking would allow the agency to seek civil penalties for first-time violations.

**Private Right of Action**

The first major roadblock to bipartisan agreement on a federal privacy framework is whether individuals, in addition to the FTC and state attorneys general, can also bring suit under this framework. Proponents of a private right of action argue that individuals cannot rely on enforcement agencies to adequately protect their rights: Enforcement agencies have limited resources, they argue, and could face regulatory capture from the targeted industry. Under this standard, when an individual faces harm from a security breach of their data, the individual can bring suit and directly seek redress. This would ensure that any violation of the law would at least be examined by the courts.

At the same time, a private right of action comes with significant costs. First, defending every perceived violation would require significant resources, and smaller companies would face additional burdens as they

often lack the resources and institutional knowledge to navigate the legal system efficiently. Second, a private right of action would also open the door to frivolous lawsuits from professional plaintiffs claiming any minor violation to seek monetary damages.

States are currently split on whether to allow individuals to bring suit. The California Consumer Privacy Act model includes a private right of action, though only for damages following data security breaches that impact specific sensitive categories of information. Even a limited private right of action, however, gives plaintiffs flexibility to test the bounds of the law by bringing a wide range of suits. Virginia, on the other hand, provides no private right of action and instead relies entirely on the state attorney general to enforce its law.

In crafting a federal privacy framework, legislators must decide whether to incorporate a private right of action, and thus far disagreement over this issue has prevented agreement. There may, however, be enough support for a limited private right of action that specifically targets a narrow range of harms. Businesses are primarily concerned with an influx of lawsuits that would drive up costs. To the extent that the framework can limit the ability of bad actors to exploit the provisions by filing frivolous lawsuits, a targeted private right of action may be viable. For example, a private right of action could include limitations such as a right to cure (i.e., giving the offending party time to address the issue), establishing limits on potential damages, or increasing the scienter requirement (i.e., only holding a firm liable for a violation if it knowingly violated the law).

While the boundaries of a private right of action will be fiercely debated, some form of this provision would likely be required to gain bipartisan support. If sufficiently targeted and designed to prevent frivolous lawsuits, the business community may find such a provision acceptable.

**Preemption**

The second major barrier to agreement on a federal privacy framework has been whether it would preempt state laws. The patchwork of state privacy laws presents a significant compliance challenge for businesses. States often require companies to adhere to different privacy standards to comply with the law. Where these requirements conflict, complying simultaneously with every state law becomes nearly impossible. As a result, companies would need to dedicate resources to compliance with a wide variety of state laws.

Many privacy advocates worry, however, that limiting the ability of states to pass their own privacy legislation would leave consumers unprotected. If a national framework proves to be weaker than the average state standards, they argue, firms can continue to engage in privacy violations.

Nevertheless, without a strong preemption of state laws, a national privacy framework would almost certainly not receive support from Republicans or the business community, in general. After all, the onerous patchwork of state laws is what has driven support for a federal privacy law in the first place. At the same time, many on the left and those in support of strong privacy protections would not support any preemption of state laws if the underlying protections in the federal bill do not adequately protect consumers.

Republicans and Democrats may find some common ground if strong preemption comes with a few narrow carveouts for issues such as cybersecurity standards designed to prevent data breaches. These carveouts would allow states to go beyond the baseline of the federal standard without passing their own laws related to privacy and data management. This, paired with state-level enforcement of the federal standards, could finally lead to some resolution on the issue.

## Conclusion

Congress has contemplated privacy legislation designed to regulate “Big Tech” for the last few years but has thus far failed to overcome disagreement over whether to include a private right of action and whether the national framework should preempt state law. As the patchwork of state laws expands, however, support for a national law will continue to grow. Congress should be able to find a compromise on these issues with a strong federal privacy law that adequately protects consumers without adding unnecessary costs to businesses.