Insight

State Legislation Shows the Need for a Comprehensive Privacy Law

JEFFREY WESTLING | MARCH 3, 2022

- Congress continues to discuss federal privacy legislation designed to protect consumers and give people more control over their data, but significant disagreement over how to structure such protections have thus far prevented legislation from moving forward.
- In the meantime, many states have passed or are considering legislation that would impose significant costs on businesses trying to comply with these new procedures.
- These costs harm businesses and competition in isolation, but the effects are compounded as a patchwork of differing state laws develop; Congress could mitigate this issue by moving forward with a national framework for data privacy.

For years, Congress and privacy advocates have pushed for a national framework to govern how businesses handle and protect user data. As it stands, two major roadblocks remain for federal privacy legislation: a private right of action, and preemption of state laws governing privacy. Democrats have been insistent on creating a cause of action for individuals to bring claims directly against companies, while Republicans worry that allowing an influx of lawsuits will drive up costs significantly. At the same time, Republicans mainly desire a federal standard to resolve conflicting state requirements, while Democrats want to allow states to go further than the baseline standards. Congress continues to work through these issues, but states have begun to move on privacy laws that take differing approaches and impose significant costs on businesses as they try to comply with often conflicting requirements.

California passed the California Consumer Privacy Act (CCPA), which sparked major concerns about a patchwork of state laws and the effects these can have on behavior outside of the state, as well as the significant compliance costs for firms operating in those states. A California Department of Finance study found that initial compliance costs of businesses across the state would be $55 billion. The CCPA has also inspired similar legislation among states across the nation. All too often, these CCPA-inspired bills differ substantially from other state privacy approaches and create multiple compliance regimes for businesses.

Take, for example, Florida House Bill 9. The bill would apply to almost every sector of the economy because its scope extends to all companies that receive or share personal information, and establishes consumer rights related to accessing, deleting, or opting out of the sale of personal information. While in isolation these protections could make sense for consumers, they are structured in a way that imposes major costs for almost all Florida businesses, such as allowing trial lawyers to develop "gotcha" lawsuits that hope opt-out and deletion requests get overlooked by businesses. A recent study by a Florida tax watchdog group found that compliance costs could be up to $21 billion in Florida. As Florida State Representative Andrew Learned explained, "[w]hether you are taxing them or requiring them to spend on new lawyers, you're still taxing Florida Businesses."

Some point to Virginia's law as a better model for state privacy legislation, citing, most notably, its lack of a private right of action. While the Virginia law provides many of the same protections as the Florida's CCPA,

companies do not have to worry about an influx of lawsuits and instead simply deal with Virginia's Attorney General. Yet even if Virginia's approach could be used as a model, a growing number of differing state laws will continue to add confusion and compliance costs to businesses trying to navigate new obligations and requirements.

The Florida bill represents the growing problem with privacy legislation at the state level. While undoubtedly well-intentioned to protect consumer privacy, it would come with significant costs to Florida businesses and can be exploited by taken advantage of by opportunists. States across the country continue to explore their own standards and regimes, all adding costs to firms that often operate across state lines.

Congress could resolve these issues by moving forward with a national framework to create a single unified standard for privacy. By doing so, Congress could minimize the impact of a patchwork of state laws with conflicting standards, and include similar protections for users without the additional costs of differing state standards. In the meantime, states must carefully consider how proposed legislation will affect businesses and the relative costs of the bill. Some models strike a better balance, protecting user privacy without imposing significant costs on all sectors of the economy. But the patchwork remains.