Insight

Assessing the State of U.S. Privacy Laws

JOSHUA LEVINE, JOHN BELTON, | AUGUST 9, 2023

Executive Summary

- In the absence of a federal data privacy framework, many states have introduced or passed state-specific legislation, often incorporating ideas from the European Union's stringent General Data Protection Regulation (GDPR).
- These differing state laws, combined with sector-specific federal regulations, have created a complex and costly environment for U.S. businesses, raising barriers to entry for startups and small firms without creating tangible benefits for consumers.
- As Congress begins to craft a national data privacy framework, it should carefully consider the impact on U.S. businesses of mirroring overly burdensome legislation such as the GDPR, which has already had a chilling effect on European tech innovation and driven up regulatory costs for U.S. firms.

Introduction:

The United States lacks a national data privacy framework, which has prompted states to create their own data privacy laws. These differing state laws, combined with sector-specific federal regulations, have created a costly and complex regulatory patchwork for U.S. businesses.

With no comprehensive federal data privacy protection, five states have passed their own unique versions of privacy legislation, many based in part on the principles found in the European Union's (EU) General Data Protection Regulation (GDPR). Since its enactment in 2018, GDPR has been considered the "toughest privacy and security law in the world." Indeed, the law has had chilling effect on innovation and competition, due particularly to its threat of fines up to 4 percent of firms' global revenue and rising compliance costs. As states incorporate the principles of GDPR into their own laws in patchwork fashion, businesses face significant compliance costs as they attempt to navigate the growing list of state laws and the differing and often conflicting provisions found across the regulatory landscape.

As Congress develops a comprehensive privacy law, it should take note of the negative effects of the EU's GDPR, both on European companies and in the states that follow Europe's lead, and perhaps instead opt to use a lighter touch.

One such piece of legislation that could offer a more measured approach is the previously introduced American Data Privacy and Protection Act, a product of bipartisan compromise, which attempts to strike a balance between protecting user privacy online and hold businesses to account without overburdening them.

The State of U.S. Federal Privacy Legislation

Over the past 50 years, the United States has implemented many industry-specific laws regulating the collection and processing of sensitive information. These regulations target a broad range of essential sectors, including health care

, credit reporting, education, and financial services. The United States has also implemented the Child Online Privacy Protection Act, which restricts the collection of data from children under 13 without parental consent. While these laws created protections for data in specific sectors, privacy advocates argue there are significant gaps related to consumers' online data that should be addressed through comprehensive legislation. These gaps exist for key pieces of data: Phone location, genomic, social media, and web browsing are not currently covered.

Congress has worked on privacy legislation in past sessions, with a variety of proposals falling short. The most promising effort emerged in 2022 in the American Data and Privacy Protection Act, a product of compromise between both parties.

State Fragmentation and GDPR's Influence

In the absence of federal comprehensive privacy laws, some states have implemented their own, many of which use parts of GDPR as a model. The California Consumer Privacy Act, Virginia Consumer Data Protection Act , as well as bills proposed in other states, have several similarities to GDPR, such as a private right of action to sue for violations of the law, as well as the inclusion of consumer rights such as the right to delete, right to know , and transparency obligations. Previous work by the American Action Forum has analyzed GDPR's specific provisions and its negative impacts on business and innovation. GDPR continues to have long-run effects on business globally; companies exposed to the regulation in 61 countries saw an 8 percent reduction in profits and a 2 percent decrease in sales. As states incorporate GDPR-like provisions into state-specific legislation, these costs will continue to grow, harming growth and innovation in the U.S. tech sector.

Further, small differences among state laws can also drive-up compliance costs. Specifically, variation in states' definitions of terms such as "personal data" and enforcement policies create regulatory uncertainty, which can increase costs for businesses. A recent Information Technology and Innovation Foundation study found that "the costs associated with data privacy laws adversely affect small businesses, often more so than their larger counterparts," to the tune of $200 billion over 10 years. Over the next three years, five more states' data protection legislation will go into effect, and nine other states currently have bills in committee.

A Better U.S. Model

There is a bipartisan consensus that the United States needs comprehensive privacy legislation to protect Americans online, but there are significant policy differences about what to include in the legislation. Congress' challenge is to develop a U.S. framework that avoids the anti-competitive impacts seen in Europe. While comprehensive legislation has yet to be introduced in the 118th Congress, it has been named a priority by lawmakers on both sides of the aisle. In the 117th Congress, the American Data Privacy Protection Act (ADDPA) passed out of the Energy and Commerce Committee (53-2), but never received a full House vote.

The ADPPA was the product of bipartisan compromise surrounding key issues. The agreement on implementing preemption – the provision that allows a federal law to supersede state laws of a similar nature – would harmonize data protection legislation nationally. The legislation also includes a tamed version of private right of action, allowing individuals to sue businesses for violating policies of the ADPPA. Significantly, there are three key policies to reduce the number of legal actions: a 45-day "right to cure," forced arbitration agreements, and a requirement that plaintiffs inform the state attorney general before suing. These policies serve as a potential remedy to endless lawsuits that could emerge while also allowing for Americans to hold businesses accountable for violating their privacy rights.

The ADPPA attempts to avoid the significant regulatory burden privacy regimes can place on businesses large and small and seeks to balance these costs with the consumer benefits that a national privacy law would provide. As lawmakers continue to work on privacy legislation, GDPR offers a convenient, albeit significantly flawed, source of inspiration. Specifically, Congress should note the burdens placed on startups and how these regulatory costs harm consumers by depressing new market entrants, thereby lessening competition and innovation in the market for technology and data-driven services. Consumer-focused legislation can address data concerns for a broad range of Americans, while also instituting measured compromises to address issues important to both sides of the aisle.

Conclusion

With the lack of a federal data privacy framework, multiple states have implemented their own versions of privacy legislation to accompany the host of national sector-specific laws. This complicated system will continue to make compliance both challenging and expensive, particularly for small businesses. While some lawmakers are looking to the EU's GDPR as a model for a U.S. framework, research has shown that the overly burdensome law is already harming innovation and competition in Europe. Congress should instead work from the framework laid out in ADPPA, which will benefit consumers and reduce costs for businesses.