The Bipartisan House Privacy Bill Would Surpass State Protections

By Stacey Gray     Thursday, July 21, 2022, 8:54 AM

After decades of negotiations, federal efforts toward a comprehensive data privacy law progressed significantly this week with the House Energy and Commerce Committee approving the American Data Privacy and Protection Act (H.R. 8152) (ADPPA). Although many proposals have been introduced in recent years, the ADPPA represents the first bipartisan, bicameral compromise on a federal privacy law that practitioners and advocates agree is long overdue. Despite strong sectoral privacy laws, the United States does not yet have a comprehensive privacy law that would create safeguards for personal information collected by general data-driven products and services.

Despite this progress, recent objections have emerged from a coalition of California leaders, including the California attorney general and regulators at the California Privacy Protection Agency (CPPA) that may threaten the bill’s passage. Specifically, California leaders are urging Democrats in Congress to preserve California’s existing privacy law, the California Privacy Rights Act (CPRA), as well as the CPPA’s enforcement and regulatory powers in the face of a national standard that would preempt California and other state privacy laws.

Any successful federal privacy law in the United States must be at least as protective as California’s current data protection framework for reasons that are both political and substantive. Politically, House Democrats from California represent the largest voting contingency by state and must be satisfied with a bill for it to move forward. On the merits, it is important to recognize that residents of California—the largest U.S. state by population and the fifth largest global economic power—enjoy significant, if imperfect, privacy protections in the absence of federal legislation. Any federal law that would preempt those protections in favor of creating uniform national standards must ensure that Californians end up equally or better protected under a federal regime.

Fortunately, the substantive protections in the ADPPA as presently drafted are significantly stronger than the California Privacy Rights Act in nearly every way. In particular, the federal proposal’s civil rights provisions are substantially stronger than those existing in any state privacy law. In the most recent version approved this week, the legislation also resolves some of the CPPA’s procedural concerns with the ADPPA, including the possibility that it could nullify the state agency’s current enforcement and rulemaking powers.

In upcoming weeks, Congress can continue to strengthen and clarify the law to ensure that it exceeds the CPRA’s substantive provisions; preserves the CPA’s existing enforcement powers; and establishes a single, strong comprehensive national privacy standard. Politically, the window for legislative action is closing rapidly as midterms approach in the fall and the Democrats face the possibility of losing their majority in either or both chambers. Congress can use this opportunity to learn from California’s previous successes in establishing privacy protections for citizens by explicitly incorporating targeted rulemaking that would provide clarity for businesses and ensure that the law can keep pace with evolving technologies, business practices, and societal norms.

Substantive Provisions: ADPPA vs. CPRA
As the Future of Privacy Forum testified recently, the ADPPA incorporates these substantive rights and goes significantly further by requiring affirmative individual consent (opt in) for the collection and use of many types of inherently sensitive data—including precise geolocation, information related to health conditions, and biometrics—while creating a broadly applicable private right-of-action (the ability for individuals to bring civil lawsuits to directly enforce their rights). The bill would also regulate a far broader scope of entities (all businesses and nonprofits) than most privacy laws currently do.

Perhaps most significantly, the ADPPA would establish groundbreaking new national civil rights protections for marginalized communities affected by potentially discriminatory uses of personal information. In contrast to state privacy laws that typically do not directly address data-driven discrimination aside from codifying existing laws, the ADPPA would significantly expand civil rights protections. These include prohibiting direct and indirect algorithmic discrimination affecting housing, employment, financial, and similar opportunities; addressing racial and other discrimination in online spaces, such as price discrimination, that is already illegal in offline spaces; and including corporate accountability mechanisms, such as algorithmic auditing and the requirement of designating privacy and data security officers and executive certifications of compliance. The ADPPA would also provide pathways for individual redress of privacy violations in some circumstances and create new protections for children, including a prohibition on targeted advertising to minors under the age of 17.

**CPPA's Objection: Enforcement Powers**

In its letter, the California Privacy Protection Agency raised valid concerns with respect to preserving its current administrative enforcement powers. This matters because the most consequential achievement of the CPRA thus far has been the establishment of the first U.S. regulatory body dedicated solely to privacy and data protection. Specifically, there were concerns that the ADPPA preserved "civil" but not "administrative" enforcement authority and did not sufficiently acknowledge the role the CPPA plays in enforcing existing privacy law.

Fortunately, the version of the ADPPA passed by the House committee this week also appears to address these concerns. In addition to providing for express enforcement by both state attorneys general and "state privacy authorities," the bill has added new text explicitly naming the CPPA and stating that the agency "may enforce this Act, in the same manner, as it would otherwise enforce the California Consumer Privacy Act[.]" Importantly, the bill appears to anticipate that state administrative enforcement may not end with California. Currently, there may be only one state agency (the CPPA) with the necessary "expertise in data protection" as laid out by the statute, but other states could establish similar agencies in the future. Such an expansion would increase the level of enforcement for consumers and potentially elevate expertise among enforcers for the business community.

Finally, to enforce a federal law, the California Assembly would likely need to update the CPPA's statutory authority or pass a technical fix to ensure that the agency retains the necessary powers to enforce federal ADPPA requirements. However, there is no reason to think that this could not happen expeditiously, given that the California Assembly has previously worked quickly both to pass the original California Consumer Privacy Act (in 2018) and to amend it in a variety of ways since.

**Rulemaking, Preemption, and Durability**

Finally, a concern raised by the CPPA and other stakeholders, including a coalition of state attorneys general, has been the ability of the ADPPA to respond to emerging technologies and business practices over time. If the ADPPA displaces state laws through federal preemption, it is argued, states will lose their power to respond legislatively to new privacy threats in the future. Ultimately, Congress must make a political decision about the extent to which federal standards will broadly or narrowly preempt current and future state laws and regulations governing privacy. However, the question is not all-or-nothing: In its current version, the ADPPA would preempt most comprehensive state privacy laws, while preserving...
Rulemaking is another area where lawmakers can improve on the successes and challenges of California, which has similarly led the way in U.S. privacy law through the ongoing rulemaking activities of the California attorney general and the CPRA. Beginning in 2019, the attorney general’s office engaged in at least five rounds of rulemaking, resulting in extensive regulations supplementing the law. Following the enactment of the CPRA and significant public input, the CPRA released additional draft regulations that it hopes will come into effect in 2023. So far, the regulations have introduced significant costs for covered businesses, while simultaneously being limited by the underlying scope, strength, and clarity of the CPRA itself. For example, one of the CPRA’s key legal features—mandating universal opt-out mechanisms such as the Global Privacy Control—has been introduced repeatedly through regulations but has yet to be widely adopted due to ongoing disagreements about whether the underlying statute requires it.

Under the ADPPA, the FTC can follow a stronger, more long-lasting approach that relies on Congress to have resolved core political questions up front, while maintaining the flexibility to respond to the emergence of new technologies and business practices that impact privacy. For example, in 2013, the FTC updated its rules for the 1998 Children’s Online Privacy Protection Act (COPPA) in response to the rapid rise of a new market for smartphones and mobile apps directed toward children. In doing so, the FTC expanded the definition of “personal information” to include device identifiers that were being used to track and serve ads to children, preventing the law from becoming outdated and ensuring that COPPA remained relevant in light of changing technologies and business practices.

Ideally, the ADPPA will be capable of addressing not only privacy threats in 2022 but also anticipated privacy threats in 2032, 2042, and beyond. The rise of virtual reality and other immersive technology, autonomous vehicles, and brain-machine interfaces will strain existing laws and regulations, requiring updating and refreshing of key concepts, such as “personal information” and “biometric data” over time. The current version of the ADPPA does provide for some rulemaking and guidance from the FTC: for example, through commission-approved compliance guidelines (Section 305). The law could be strengthened even further to provide for targeted rulemaking around key concepts, such as interpreting what is and is not considered “sensitive covered data” in new and emerging contexts.

**A Path Forward**

At the end of the day, House lawmakers should not lose sight of the significance of what’s being negotiated. A comprehensive privacy law in the United States would address very real, current privacy threats caused by gaps in legal protections for highly sensitive information from web browsing, mobile apps, “Internet of Things” devices, and other emerging data-driven sectors. A baseline national standard would also provide protections to people across the country, ease business compliance difficulties, inspire implementation of more privacy-protective business models, and reclaim the United States’s global leadership in the midst of 150-plus nations that have already adopted strong data protection laws.

Although the ADPPA will not be the end of the conversation—lawmakers will likely continue to grapple with privacy for decades to come—a strong national law that can stand the test of time will do immeasurable good for the United States and its many and diverse communities, all of whom deserve privacy.

**Topics:** Privacy

**Tags:** data privacy, House Energy and Commerce Committee