



Issue Brief

NOVEMBER 18, 2020

BY ANDREW WILFORD

States Follow California's Ill-Advised Lead on Consumer Privacy Legislation

Just under a year ago, the National Taxpayers Union Foundation (NTUF) published an [analysis](#) of the California Consumer Privacy Act (CCPA), controversial legislation which imposed burdensome new restrictions on businesses' use of personal information. Our analysis highlighted the risk that the new regulations could cause significant economic harm in the form of burdensome compliance costs, but also because of the potential to create an overlapping web of state privacy rules.

The CCPA officially went into effect in the beginning of July, but it was only in the middle of August that [enforcement regulations were finalized](#). Unfortunately, while enormous compliance costs were always a given (California's own attorney general estimated \$55 billion in costs for California businesses alone), fears of overlapping state-based privacy regulations have also proven to be justified.

Overlapping state rules can put businesses in a Catch-22 situation. For example, each state in the nation has enacted rules governing how businesses should handle data breaches. Yet while many states require that businesses experiencing a data breach notify potentially affected customers of the circumstances of the breach, Massachusetts [mandates](#) that businesses not release details about the breach.

Key Facts:



Earlier this year, California's consumer privacy legislation went into effect, joining two other states with similar legislation that could prove burdensome for small businesses.



While only a few states have passed consumer privacy legislation thus far, a California ballot measure passed in November expanding its landmark consumer privacy law may prove the starting gun for a new wave of state consumer privacy legislation.



Congress should consider drafting legislation creating a single, uniform national standard, pre-empting potentially overlapping state laws and reducing the compliance burden for affected businesses.

California legislators were not the first to conceive of state-based consumer privacy rules, but their adoption of them threatened to mainstream the concept. And indeed, just one year after California signed its consumer privacy legislation into law, two other states have already passed consumer privacy laws of their own.

States That Enacted Consumer Privacy Laws

California

The CCPA was fairly expansive, granting consumers the right to know what information businesses are collecting, the right to have personal information collected from them deleted, and the right to opt out of having their personal information sold, among other things. Businesses were required to comply with these regulations if they bought, received, shared or sold 50,000 Californians' data.¹

While that may sound like a high bar, the truth is that many small businesses that one would rarely think of as “businesses transacting in American consumers' data” can easily reach this threshold. After all, 50,000 Californians would represent roughly 0.16 percent of the state's adult population.

And in our internet-based economy, small businesses use consumer data in very innocuous ways. Restaurants, for example, often collect email addresses for reservations or restaurant wifi access, then use these emails to send promotions or encourage customers to return to their establishments. That's led to absurd situations like California restaurant patrons [receiving a CCPA notice with their menus](#).

And California is not done there. This November, Californians approved a referendum on the California Privacy Rights Act (CPRA), an expansion of the CCPA. The CPRA will go a step further by establishing [even stricter obligations](#) for businesses handling “sensitive personal information.” This will likely create even more significant compliance obligations for businesses already struggling to get in line with the CCPA.

Maine

Maine's [Act to Protect the Privacy of Online Consumer Information](#) is far less extensive than California's sweeping privacy regulations. Most notably, Maine's law applies only to Internet Service Providers (ISPs), requiring them to receive affirmative consent before selling consumers' personal information. Consumers must opt out to prevent information not specific to the consumer, such as broadband speeds or general data usage, from being sold.

While this approach is far less burdensome than California's, particularly for small businesses with only a tangential interest in consumer data, it still represents an issue better solved at the federal level. For example, what qualifies as “personal information” is only lightly defined in the text of the legislation, leading to a high possibility of cases where one state considers information to be “personal” while another state does not.

Nevada

Nevada's privacy law, [Ch. 603A](#), is more similar to California's approach than Maine's. Though passed after the CCPA, Nevada's privacy law went into effect on October 1, 2019, well before the CCPA.

¹ Businesses could also be required to comply with the CCPA if they derived 50 percent or more of revenues from sale of Californians' data, or if they had annual gross revenues of \$25 million or more and transacted in a single Californian's data. However, these thresholds are less concerning as they are, almost by definition, far less likely to ensnare small businesses that collect consumer data only in the course of normal business operations, not for the purpose of buying or selling such data.

In a few ways, Nevada’s privacy law improves upon California’s flawed approach. Most notably, Nevada does a far better job [defining terms](#) than California does, narrowly defining terms such as “sale,” and, most importantly, “personal information,” leaving far less room for creative bureaucratic interpretation.

On the other hand, however, Nevada’s legislation includes no safe harbor for small businesses at all, applying to any person who owns and operates a website, collects any “personal information” from Nevada residents, and transacts with any Nevada residents. If 50,000 is too low a threshold for California, Nevada’s effective threshold of “one” represents an even greater danger to interstate commerce.

This hands state regulators an unprecedented tool in potential enforcement actions against businesses. This could be deployed in the course of enforcing existing regulations or, perhaps more worryingly, against businesses that have done nothing to run afoul of any other Nevada rules. Giving regulators effective “privacy audit” power over any company that has data on even a single Nevadan is a risky proposition in a modern economy, given that nearly every business operating in interstate commerce is likely subject to the rule.

Other States Considering Consumer Privacy Legislation

Yet while only two states other than California have gone forward and passed consumer privacy legislation, efforts are underway to considerably expand the list of states with similar legislation on the books. Between 2018 and now, [24 states](#) have introduced legislation that would enact similar consumer privacy protections.

While that may appear as good news to consumer privacy advocates, the reality is that each additional state represents further complications and compliance burdens for businesses that operate in multiple states. This is particularly true for e-commerce businesses, which can have customers around the country despite having relatively small operations.

Of the 39 pieces of legislation coming out of these 24 states, only six have made it out of committee, while five have passed their original chamber, and two have passed two chambers. These two pieces of legislation still did not make it all the way through the process — in Hawaii, the measure was substituted for a task force to study the issue and make recommendations, while in Washington, the proposal is in the conference committee process. Five states other than Hawaii — Connecticut, Louisiana, Massachusetts, North Dakota and Texas — have seen consumer privacy legislation substituted for task forces.

Undoubtedly the coronavirus has altered legislative priorities in many of these states, resulting in consumer privacy legislation being tabled for the moment. Nonetheless, this reveals that legislation addressing consumer privacy issues was gaining traction in a diverse array of states across the country in the immediate aftermath of the CCPA.

Conclusion

NTUF started the Interstate Commerce Initiative in order to attempt to rein in the growing trend of states taxing and regulating beyond their borders. That in itself sounds like an abstract legal concern, but cases such as this reveal the concrete issues with cross-border reach — when states take it upon themselves to regulate areas best left to Congress, the result is a hodgepodge of conflicting and overlapping state rules that are far more difficult for businesses to comply with than a single national standard would be.

And absent Congressional action, businesses taking their first breaths in the aftermath of the coronavirus pandemic could well be met with a barrage of new and conflicting compliance burdens as states take up previously tabled legislation on consumer privacy. The pandemic may have forced states to take up more urgent matters, but that does not mean they should not be mindful of the struggles of small business owners even after the legislative crisis subsides.

The surest path towards consumer privacy protections that minimally burden small businesses, therefore, is indeed forward-looking Congressional action that preempts overly aggressive state enforcement, sets a uniform national standard, and creates appropriate safe harbors for small operations. The longer it takes Congress to do so, the more complex the web of state privacy rules will likely become.

About the Author

Andrew Wilford is the Manager of the Interstate Commerce Initiative at the National Taxpayers Union Foundation (NTUF), a project which seeks to protect taxpayers from the pernicious effects of states attempting to exercise power outside their borders. NTUF is a nonpartisan research and educational organization that shows Americans how taxes, government spending, and regulations affect them.



*2020 National Taxpayers Union Foundation
122 C Street NW, Suite 650, Washington, DC 20001
ntuf@ntu.org*