Interstate Commerce Initiative

NTUF
NATIONAL TAXPAYERS UNION FOUNDATION

Issue Brief

OCTOBER 18, 2019

BY ANDREW MOYLAN & ANDREW WILFORD

California Attempting to Make National Law...Again

How the California Consumer Privacy Act Threatens Interstate Commerce

In June of last year, California Governor Jerry Brown signed into law the California Consumer Privacy Act (CCPA), a bill that claims to protect consumer privacy on the internet through complex European-style regulation. This is the latest in a series of moves (not limited to privacy law) by the state to effectively make national law by imposing its own rules and regulations on businesses and individuals all across the country.

From auto emissions standards to cage-size rules for agriculture to imposition of business tax on out-of-state residents, California has regularly used its size and national influence to exercise power outside its borders, often in backdoor attempts at making national law. This has led to the state being challenged in federal court and by the executive branch to scale back its ambitions lest it cause significant economic harm.

Key Facts:

The California Consumer Privacy Act (CCPA) is a complex scheme targeting online businesses with new regulations in the name of privacy.

In effect, CCPA is an attempt by California to make national law, with access to the fifth-largest market in the world as cudgel.

This law threatens to impose huge costs on businesses while undermining the free flow of interstate commerce, which Congress is charged with protecting.

But by aggressively moving to implement its own privacy standards, California is again taking steps to enforce its laws on out-of-state businesses. This threatens to set off an avalanche of complex, overlapping, and possibly conflicting state consumer privacy laws that will severely hamper internet innovation. These laws could have a severe negative impact on the free flow of interstate commerce, raising questions about whether Congress should legislate in this area. Additionally, they pose a serious risk of further accelerating the trend of states taxing and regulating entities outside their borders, undermining the federalist structure of the constitution.

The European General Data Protection Regulation (GDPR)

Despite vigorous pushback from technology and privacy experts, the European Union (EU) passed the General Data Protection Regulation (GDPR) which went into effect in May of 2018. GDPR created a set of standards for companies handling EU citizens' digital information. These standards included consent requirements for handling consumer data, data security regulations, and notification in cases of data breaches, among others. Some companies were even required to appoint a special data protection officer to oversee GDPR compliance. Failure to adhere by these standards saw reputable U.S. businesses such as the *LA Times* and *The Chicago Tribune* being temporarily blocked in many European countries.

Yet compliance with GDPR was far more costly than a temporary blackout. Businesses spent billions of dollars trying to comply with the new law, and smaller businesses were hardly exempt. Seventy-four percent of small- to mid-sized businesses spent more than $100,000 on GDPR compliance, while 20 percent spent more than $1 million.

There were concerns beyond the financial cost of compliance as well. Non-EU businesses, even some without any direct operations in the EU, were often required to comply with GDPR. In effect, the EU was regulating well beyond its own borders. For Americans it was a preview of states using the ever-increasing power of the internet to grant themselves ever-increasing power as well.

California's Turn to Regulate

Shortly after businesses both large and small jumped through the hoops of complying with GDPR in Europe, California required that they invest significantly in complying with the state's new privacy law. While both laws are sweeping frameworks for data privacy protection that bear strong similarities, there are significant differences that mean that a GDPR-compliant business is not immediately in compliance with CCPA. As a result, a new round of regulatory burdens is likely to befall many online businesses just to be able to maintain access to California's market.

An analysis performed for the California Attorney General showed staggering costs associated with implementing CCPA. The study identified $55 billion in upfront compliance costs on California-based businesses, and up to another $16.5 billion over the coming decade. These are decidedly non-trivial amounts, with $55 billion amounting to 1.8 percent of California's gross state product in 2018. For some context, that's more than the state's entire agriculture, forestry, and fishing industries combined according to Bureau of Economic Analysis data.[1]

Small businesses were not immune. The analysis forecast that small businesses, those with fewer than 20 employees would be forced to spend $50,000 on CCPA compliance. Medium-sized companies, those with 20 to 100 employees, would have $100,000 in initial compliance costs.

[1] Bureau of Economic Analysis. "Regional Data: GDP and Personal Income." (Author's calculations. Retrieved from: https://apps.bea.gov/itable/iTable.cfm?ReqID=70&step=1.)

These estimates doesn't even begin to count the costs imposed on out-of-state businesses. Even if one assumes that CCPA will have just one-tenth as much impact on state economies elsewhere in the country as it does in California, that's more than $31 billion in additional costs imposed on businesses not present in the state.[2]

Interstate Commerce Implications of the CCPA

California's governor signed the CCPA into law just a week after the Supreme Court handed down its decision in the landmark case of *South Dakota v. Wayfair*, the case in which the Court granted states sweeping new powers to impose tax collection requirements on out-of-state businesses. The Court's approval of a so-called "economic nexus" standard, where a state can wield power over any company regardless of its location based only on a purported economic connection, is part of a years-long trend of states utilizing the development of the internet and related technologies to blur the lines that limit their power.

There are many clear parallels to be drawn between the CCPA and South Dakota's economic nexus law. At their core, both serve to grant states much greater power to regulate and tax individuals, businesses, and commerce taking place outside the state.

The similarities continue. Both laws have safe harbors for small businesses which also, effectively, serve as the "nexus" justification for the state to be regulating out-of-state businesses utilizing a transaction number and a dollar threshold for determining their nexus standard. South Dakota's law requires 200 transactions in-state, while the CCPA's standard is lower. It applies to businesses that buy, receive, share, or sell 50,000 California citizens' data. That means that any entity transacting in data for 0.18 percent of the state's adult population will be required to comply with California's law, regardless of their location, a standard likely to ensnare a significant number of businesses.

This threshold of 50,000 would force an astonishingly wide array of businesses to comply with California's new law. According to reporting from the *Wall Street Journal*, "Some 500,000 U.S. businesses across all sorts of industries meet that criteria, according to the International Association of Privacy Professionals. They include companies as varied as Starbucks Corp. and Gap, health insurer Aetna Inc., financial-services firm Wells Fargo & Co., American Airlines Group Inc. and toy maker Mattel Inc. —as well as hundreds of thousands of small and medium-size businesses."[3]

This standard is substantially lower than the one written by the activists that spurred the legislature to pass CCPA in the first place. In draft language for a ballot initiative (which was eventually withdrawn when the legislature began work on a bill), Alastair MacTaggart and his group Californians for Consumer Privacy crafted a standard that businesses must transact in more than 100,000 California citizens' data before being subject to the law. His proposed follow-up ballot initiative, aimed at making changes to CCPA, suggests returning to that standard from the CCPA's lower 50,000 level in order to minimize impact on small businesses.[4][5]

CCPA's threshold also requires compliance of any business that processes the personal information of California residents and has annual gross revenues of $25 million or more, or that derives 50 percent or more of its income from the sale of Californians' consumer data. South Dakota's law, meanwhile, applies to firms with more than 200 transactions into the state or greater than $100,000 in sales.

---

[2] *ibid*.
[3] Haggin, Patience. "Businesses Across the Board Scramble to Comply With California Data-Privacy Law." The Wall Street Journal, September 8, 2019.
[4] Hautala, Laura. "New California privacy initiative proposed for 2020 ballot." C|Net, September 25, 2019.
[5] The California Privacy Rights and Enforcement Act of 2020. Office of the Attorney General of California. (Ballot Initiative.)

And like with South Dakota's law, the concern with the CCPA goes beyond a stuffy legal critique of a state regulating outside its borders. The practical effect of *Wayfair*, and the ensuing avalanche of state economic nexus laws, was to create a compliance nightmare where small businesses were forced to contend with a web of differing state laws, rates, and definitions.

That risk is present with the CCPA as well. Compliance with California's law, particularly for businesses with no physical operations in California, is confusing enough. Were the other 49 states and the District of Columbia to follow suit, the confusion would only multiply, lending real-world concerns to the legal uncertainty at the heart of the law.

Failure to comply with the CCPA can result in far more than just a slap on the wrist. Unintentional violations of the CCPA result in $2,500 fines per instance, while intentional violations are fined at a rate of $7,500 per violation. A small business that fails to become CCPA-compliant, either out of ignorance or lack of resources, could quickly find itself swamped by fines.

Similar laws show how regulatory overlap can create a Catch-22 for businesses. For example, each state in the country has enacted data breach notification laws. Yet while Massachusetts prohibits businesses from disclosing the circumstances of a data breach when they notify affected consumers, other states mandate that businesses do describe the breach.

Other clear issues with CCPA suggest it may not survive legal challenges, even in an environment more permissive of states exercising cross-border reach. For example, though the exemption in CCPA of $25 million in annual revenue is a fairly reasonable definition of a small business, it is undermined by other conditions in the bill. Specifically, small operations that handle large amounts of consumer information as a matter of course, such as retailers, could find themselves handling more than 50,000 California consumers' personal information without ever being involved in the selling of that data and regardless of their size and ability to handle compliance.

Perhaps more worrying is how a nexus standard like this might be replicated in other areas of law, or by other states. For example, Hawaii, Pennsylvania, and Texas have taken steps to expand their corporate income tax power by establishing a *Wayfair*-style nexus standard that ropes in more out-of-state businesses.[6] It is easy to see how some states may begin employing a CCPA-style nexus standard for tax purposes, imposing their corporate tax requirements on any business that is subject to its data privacy requirements.

This concept has already been discussed in California, with Governor Newsom announcing support for a "data dividend" proposal in his State of the State address earlier this year. Under the proposal, any company that buys or sells a consumer's data would be required to make a payment to the consumer or the state to offset the transaction. This proposal would threaten the ad-funded internet model that provides trillions of dollars in payment-free services to American consumers.

California would likely have to design a bespoke tax system in order to implement such a plan given that most of the major data-centric online companies already operate in the state and pay corporate income tax. But other states across the country that do not serve as home bases for major tech companies could decide that they, too, would like a pound of flesh and may decide that the easiest path toward securing it is by redefining nexus for corporate income tax to include transacting in data for a certain number of citizens.

In the context of the recent explosion in economic nexus laws, this represents a triple whammy for online businesses. While they are already reeling from the need to comply with new sales tax collection and

[6] Koklanaris, Maria. "States Turning to Economic Nexus To Extend Biz Tax Reach." Law360, October 11, 2019.

remittance requirements in states around the country, some retailers could soon be hit by the need to comply with California's sweeping new data privacy law *and* be subject to new corporate income tax levies if states pursue their own "data dividend" concepts. Add on top of that the risk that other states begin drafting conflicting data privacy laws, and some online businesses could be left in an impossible position.

Conclusion

The California Consumer Privacy Act consists of burdensome regulations that will hamper an internet infrastructure built on making sense of disparate pieces of data. In doing so, it employs a theory of state power that acknowledges few practical limits to its scope, potentially causing significant economic damage.

Should the country wish to act on data privacy protections, Congress would be a far better place to do it. This would preclude the danger of a tangle of overlapping state privacy protection laws, as well as returning the role of regulating issues that involve interstate commerce to the legislative body intended by the Constitution: the United States Congress.

Clearly, data privacy is a growing concern for many Americans, owing to the increasing importance of services fueled by analysis of information. The California Consumer Privacy Act, though, is a misguided and dangerous approach to the issues. California's legislative adventurism is once again posing serious risks for individuals and businesses, for other states, and for the free flow of interstate commerce that underpins America's economy.

About the Authors

Andrew Moylan *and* ***Andrew Wilford*** *lead 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.*

NATIONAL TAXPAYERS UNION FOUNDATION

2019 National Taxpayers Union Foundation
122 C Street NW, Suite 650, Washington, DC 20001
ntuf@ntu.org