BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Preempt to Protect: The Need for Federal Privacy Protection Law to Curtail the Pending Patchwork of State Laws

By Liz Bramley, J.D. Candidate 2021 | March 5, 2019

In the wake of Cambridge Analytica, the concern for privacy protection is no longer limited to the IT team down the hall. In its place, public protest prompted the first state-wide privacy protection law with the potential to drive comprehensive federal legislation.

The California Consumer Protection Act ("the CCPA") is a bill the heightens consumer protection and privacy rights for the residents of California. Instead of absently accepting terms and conditions with the presumption to opt-in, users are given clear notice and the power to opt-out if a company intends to collect their data. The CCPA affects for-profit companies doing business in California that earn more than $25 million, gather information from 50,000 or more consumers, or make half of their revenue selling personal information. And with an effective date of January 1, 2020 on the horizon, large companies across the country are panicked.

This much was apparent at recent Congressional Data Privacy Hearings, where the tech industry seemed open and eager to support federal privacy legislation. While it may seem out of character for companies like Facebook and Apple to welcome regulations with open arms, when backlit by the CCPA, their intentions become transparent.

The tech industry wants Congress to pass a more lenient federal privacy law that pre-empts the CCPA and any subsequent state privacy laws. It's no surprise the industry wants an alternative law to reduce costs and narrow liability. And politicians and advocacy groups have been quick to criticize. But in reality, the push for a Federal Law is more nuanced and necessary than big businesses desire to circumvent the CCPA.

From a business perspective, the patchwork of subsequent state laws, albeit a lawyer's dream, is a compliance and regulation nightmare. Already there are issues. Washington State has proposed a privacy protection law that parallels the CCPA. But while California specified an exemption allowing financial institutions to adhere to the more lenient privacy regulations of the GLB Act, there is a debate about whether Washington will follow suit.

This concern is just one provisional variance between two actors. A few more states with a few more differences and the ensuing inefficiency is a ripple effect. Companies qualified or doing business in multiple states will face issues categorizing and storing consumer information, not to mention the difficulty implementing internal data management policies.

But most worrying is that a ripple, which started with the best of intentions, may grow into a fatal wave for small companies. Most software and app development start-ups cater to large

clients across the county. These fragile companies, meant to fall outside the CCPA, will need to build out different versions of the same product to ensure various levels of compliance. For instance, a company in a state without a privacy law looking to integrate outside software into their product isn't going to buy the version that adheres to the CCPA. Instead, they are going to want a version that allows them to retain and sell consumers' personal information. In this way, multiple state-wise privacy laws could increase development costs past sustainability.

Insofar as laying a foundation, the CCPA is a win. But the need for a federal privacy protection law is beyond big business' desire to cut corners, and costs. A federal law will create manageable bright-line rules and reduce costs or at least provide predictability to start-ups with fixed development budgets. The real victory, for companies and consumers alike, awaits the day privacy protection advocates and the tech industry can find a way to agree on a governing federal law.