Published on *The National Law Review* https://natlawreview.com

The Uncertain “State” of US Data Protection Law: California Leads the Way

Article By:

Austin Mooney

When it comes to US data protection law, all eyes are on California. The California Consumer Privacy Act of 2018 (CCPA), which took effect this year, introduced a complicated data protection framework for the personal information of California residents, imposing a variety of new obligations on affected businesses. Although the interpretation of many of the CCPA’s provisions remains unsettled—and proposed regulations are still pending— the CCPA’s original architects have already advanced another proposed law, the California Privacy Rights Act (CPRA), which will be decided in a statewide referendum this November. If enacted, the CPRA would substantially amend the CCPA, granting consumers additional rights and imposing further liability on businesses. Whether or not it passes, the proposed CPRA highlights the fluid state of the US legal environment for data protection, which has left businesses around the world struggling to account for the uncertain risks and compliance costs posed by these developments.

It did not have to be this way. The developments in California are due in part to the failure of the US Congress to enact comprehensive federal data protection legislation. Despite widespread support, compromise on a federal standard remains elusive, with legislators unable to agree on critical questions, such as whether or not the law will pre-empt state laws like the CCPA.

CCPA: ORIGINS AND OVERVIEW

The CCPA originated as a state “ballot initiative,” a type of referendum that is uniquely powerful in California. After negotiations with the California legislature, the initiative’s sponsors withdrew the initiative from the 2018 ballot in exchange for the enactment of a slightly watered-down version of the CCPA through the standard legislative process. As enacted, the CCPA applies to the broadly-defined “personal information” of California residents, granting individuals various rights with respect to businesses that process their information. Businesses that process California personal information and either exceed US$25 million in annual revenue, process the data of more than 50,000 consumers per year, or generate 50% of their revenues from data sales, are subject to the law. Because a business need satisfy only one of these thresholds to be covered by the CCPA, the law applies to a wide range of companies, including many that have only a handful of California customers or otherwise incidentally process the personal information of California residents. Notably, businesses need not have a physical presence in California—or even in the United States—to be subject to the CCPA.

Perhaps the most interesting right under the CCPA is the right of consumers to opt-out of "sales" of personal information. Whether or not a data transfer amounts to a "sale," as defined by the CCPA, depends on a number of factors, including the purpose of the transfer, whether or not any "value" was provided in exchange, the contract terms, and how the data is ultimately used. The applicability of these provisions remains hotly contested, especially in data-centric industries such as digital advertising. Many companies have opted to take risk-based positions while waiting for the meaning of these provisions to be clarified. In addition to the CCPA's privacy rights, which are enforceable only by the California Attorney General (AG), the CCPA grants California residents a private right of action to sue companies whose unreasonable security practices lead to a data breach. This right only extends to breaches of certain sensitive categories of personal information, such as financial account information. Impacted individuals can obtain guaranteed statutory damages of US$100 to US$750 per person, a fact that has already resulted in a surge of class action lawsuits following the law's entry into force in January 2020. The AG is also responsible for issuing regulations.

The proposed final regulations would clarify a number of procedural and substantive ambiguities in the CCPA's text and impose additional recordkeeping and procedural requirements on businesses. At the time of publication, however, the final regulations are still pending administrative approval and are unlikely to take effect until October 2020 or later, adding to the compliance uncertainties that businesses face.

THE CPRA JOINS THE FRAY

Without doubt, the CCPA's impact is large. By the state of California's own estimates, compliance costs alone will exceed US$50 billion for covered businesses. Dozens of amendments have been carefully considered by California legislators; in drafting the CCPA regulations, the AG produced over 500 pages of analysis. Despite this effort, the proposed CPRA would substantially amend the CCPA. The proposed changes are numerous. As one example, the CPRA would create a right for California consumers to "limit" the processing of "sensitive personal information," which is a new subcategory of personal information that combines and builds on existing "sensitive data" categories under US and EU law. While the steps companies would take to comply with such requests would be similar to the obligations they face under the CCPA in relation to consumer requests to opt out of the "sale" of their data, the applicability of this right is potentially far broader, and many companies that do not "sell" personal information under the current law would have to substantially revise their data practices to comply with the CPRA. Further, the law would modify the definition of "sale" to explicitly encompass digital advertising, with significant implications for the vast majority of websites.

Unlike the ballot initiative behind the CCPA, which was ultimately withdrawn, advocates have given no indication that a legislative compromise will be reached for the CPRA. Early signs point to widespread support for the initiative, which will be voted on in November. If passed, most of the provisions would not take effect until 2023, but preparations for many businesses would need to begin immediately.

FEDERAL LEGISLATION REMAINS STALLED

The surge in data protection law in California can be attributed in large part to the ballot initiative process and the efforts of a group of well-funded advocates. These developments can, however, also be partly attributed to the failure of the US Congress to pass even baseline federal data protection legislation, leaving the states to respond to heightened public support for privacy regulation on their own. Congress has the power to pass laws regulating data protection throughout the entire country and, if it wishes, to pre-empt state laws such as the CCPA.

A federal standard is supported by members of both political parties, business interests, and privacy advocates alike, and various stakeholders have proposed legislation that would establish such a standard. Despite this widespread agreement on the need for a federal law, little consensus has emerged on the details. Proponents have split along two primary fault lines: the mechanisms for enforcement, and the scope of state pre-emption. Democratic politicians and privacy advocates have tended to support strong enforcement, including private rights of action and minimal preemptive effect, allowing more-restrictive state laws like the CCPA to remain in force. Republicans and business interests, on the other hand, have generally advocated against private enforcement and in support of widereaching pre-emption. Adding to the impasse, other issues that intersect with online privacy, such as the moderation of social media content, have given rise to sharply partisan debates, threatening the viability of any bipartisan efforts to reach a compromise, especially in a Presidential election year. Accordingly, while a US federal data protection law is possible in the coming years, it is not likely to happen anytime soon and, even if passed, its potential impact on state laws like the CCPA is unclear. For the foreseeable future, then, businesses that collect or process California data will need to grapple with the moving target of California law.

National Law Review, Volume X, Number 266