SQUIRE PATTON BOGGS

# Countdown to CCPA Compliance

Passed in the wake of the GDPR's May 25, 2018 effective date, the California Consumer Privacy Act (the "CCPA") creates new rights for California residents and imposes new obligations on businesses that conduct business in California and collect or process data on California residents.

Regardless of physical location, these businesses are subject to the statute if they have annual gross revenue in excess of $25 million; derive 50% or more of annual revenue from selling California residents' personal information; or receive, sell, or otherwise share the personal information of 50,000 or more California consumers, households, or devices.

By way of background, then-Governor Jerry Brown signed the CCPA into law on June 28, 2018, and the Act goes into effect January 1, 2020. Over the past year, both supporters and detractors have posed questions regarding the scope of the statute and proposed amendments to address those open questions.

The clock is now ticking on compliance as 2019 comes to a close, but there is still a cloak of uncertainty over just how broadly the CCPA will reach, which will impact data privacy and protection generally and the extent of privacy litigation that will result from the Act.

This article explores the hurdles to businesses preparing for CCPA compliance and the importance of that compliance. The article begins with an analysis of the current scope of the CCPA, taking into account currently pending amendments that will shape consumers' rights and businesses' obligations under the Act. The article next discusses the significant litigation risks that businesses will face for failing to comply with the CCPA.

## Current Standing of the CCPA

The CCPA provides California residents with rights regarding businesses' collection, access, use, sale, deletion, and disclosure of "personal information." Since the enactment of the law, the California state legislature has considered notable amendments going to the very threshold of the CCPA, including the definitions of "personal information" and "deidentified information," who is deemed a "consumer" with rights under the statute, and the scope of businesses' compliance obligations.

Despite the title of the statute, the law as originally drafted, contemplated more than only "consumers," covering customers, employees, vendors, and contractors. The CCPA similarly interpreted "personal information" with a wide brush to include any information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."

The Judiciary Committee of the California Senate held a marathon hearing July 9, 2019, to consider several proposed amendments to the CCPA. The committee approved a handful of the most notable bills, but primarily with revisions limiting their impact. For instance:

- As presented to committee, Assembly Bill 25 proposed amending the definition of "consumer" under the CCPA to exclude job applicants, employees, contractors, or agents of a business to the extent that their personal information is collected and used in their roles as applicants, employees, contractors, or agents, and foreclosing a private right of action data breaches impacting employment data.

  As revised and approved, however, employee data will be exempt only from certain CCPA provisions, such as the right to access or deletion. But employers still must notify employees what information is collected and why, and employees can still bring private CCPA claims based on breaches regarding employee data.

- The committee also passed Assembly Bill 846, carving out an exception allowing businesses to treat customers differently when participating in customer reward and loyalty programs, with the condition that the bill be amended to expressly prohibit companies from selling the data of loyalty program members.

- The committee approved Assembly Bill 874 without amendment. That bill seeks to narrow the definition of "personal information" by clarifying that both "publicly available information" and de-identified or aggregate consumer information are excluded from the definition.

Other amendments failed to advance, though the legislature may revive them in later sessions:

- AB 873 proposed amending the definitions of "personal information" and "deidentified information" to narrow the type of data covered by the CCPA. With competing concerns over creating a workable definition for businesses subject to the CCPA or, alternatively, creating a large loophole that would weaken the effects of the CCPA, neither side won a majority, and AB 873 failed in a deadlock vote.

  The committee has granted a request for reconsideration, however, so this is likely not the last we will hear of AB 873 and the threshold definitions of data covered by the CCPA.

- Assemblyman Ken Cooley removed his own bill, AB 1416, from consideration before the hearing.

AB 1416 sought to create CCPA exemptions for businesses complying with government information requests or selling information solely to detecting and protecting against data breaches. While opponents previously expressed concern over AB 1416 creating too large a loophole, Assemblyman Cooley has not yet commented on his decision to remove the bill from the committee's July 9th agenda. With no debate or discussion yet in committee, it remains to be seen which way the committee may lean on this proposed amendment and how the bill may be revised if presented again in a future session.

Even those amendments that passed the July 9th committee hearing have another step to go. The California Senate must pass any remaining CCPA amendments by September 13, 2019, in order for Governor Newsom to sign the bills into law before January 1, 2020.

Businesses cannot take a wait-and-see approach and should prepare plans assuming that the CCPA will apply broadly. While monitoring legislative developments changing the scope of the CCPA's reach, businesses must prepare for compliance or face the significant liability risk for violating the CCPA.

## Anticipated CCPA Litigation

With the potential for significant per-claimant recovery, the CCPA incentivizes litigation generally and class actions in particular. Businesses preparing for CCPA compliance should keep this risk in mind when creating and documenting their data collection and data privacy practices and procedures.

The CCPA provides a private cause of action when a consumer's "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Consumers bringing a private suit can recover the greater of either actual damages or statutory damages of between $100 and $750 per consumer per incident.

Before bringing an individual or class action, consumers seeking statutory damages must first provide a business 30 days' written notice of alleged non-compliance, giving an opportunity to cure. But consumers seeking actual damages need not provide this same opportunity to cure before bringing suit.

The language of the CCPA private-right provision—which leaves much open to interpretation—may spur litigation based on the parameters of a business's data privacy obligations. A business's failure to maintain "reasonable security procedures and practices appropriate to the nature of the information" triggers a consumer's right to file suit. What a court deems "reasonable," however, is nowhere to be found in the CCPA. Nor does the CCPA provide a guideline for what practices are "appropriate" based on certain types of information maintained by a business.

While some third parties such as the Center for Information Security and the National Institute of Standards and Technology have created security frameworks deemed reasonable in the industry, the CCPA itself leaves businesses with little to argue that certain security measures meet CCPA standards *as a matter of law*. On the other hand, the CCPA leaves the window open for consumers to argue whether certain security measures are reasonable and appropriate on a case-by-case basis during litigation.

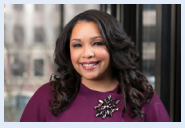
## Conclusion

The CCPA will have an immediate impact on businesses subject to the statute, as they prepare for compliance in January and work to safeguard against the litigation likely to follow. In preparation, businesses should document their data security procedures and practices for all personal information collected and maintained, using industry sources as guides. Businesses should assume a broad interpretation of "personal information" and "consumer" and have written documentation of all data maintained on customers, employees, vendors, and contractors.

More far-reaching, though, is the impact the CCPA will have on U.S. privacy laws in general. With the CCPA set to take effect in 2020, at least 13 other states, including Hawaii, Maine, Maryland, Massachusetts, Mississippi, Nevada, New Jersey, New Mexico, New York, North Dakota, Rhode Island, Texas, and Washington, have now considered similar privacy statutes aimed at creating rights for consumers and protecting consumer information. As the leader of the pack, the CCPA will set the standard not only for California but for the future of data privacy laws across the country.

*This article first appeared in the Spring 2020 edition of the American Bar Association's Tort Trial & Insurance Practice (TIPS) Cybersecurity & Data Privacy Committee Newsletter, and reprinted here with permission.*

## Contact



**Petrina Hall McDaniel**
Partner, Atlanta
T +1 678 272 3207
E fpetrina.mcdaniel@squirepb.com

Petrina McDaniel is a partner in Squire Patton Boggs' Litigation and Data Privacy & Cybersecurity practices. Petrina is a commercial litigator and Certified Information Privacy Professional (CIPP/US) whose practice uniquely blends complex litigation, regulatory compliance, and privacy counseling.