California's New Privacy Law Has Teeth: Civil Penalties, a Private Right of Action for Consumers, Statutory Damages, and Voiding of Consumer Arbitration Agreements

Published in the Association of Business Trial Lawyers Orange County Report
Volume XXI No. 1; Spring 2019

Authors:

Travis Brennan
Chair, Privacy & Data Security practice
(949) 725-4271
TBrennan@sycr.com

Katie Beaudin
Associate, Business Litigation practice
(949) 725-4074
KBeaudin@sycr.com

On June 28, 2018, California's legislature passed the California Consumer Privacy Act ("CCPA"), Civil Code §1798.100, et seq., after just one week of debate, and Governor Brown signed the act into law the same day. Despite that rush, the law will not take effect until January 1, 2020. Given the CCPA's broad scope, vague terms, and a generous delegation of rule-making authority to the California Attorney General's Office that has yet to produce any rules, that 18-month delay is not as long as it sounds. While not quite as ambitious as Europe's General Data Protection Regulation ("GDPR") that took effect last spring, the CCPA imposes significant new data protection obligations on a wide swath of businesses. And perhaps most significantly for trial lawyers and their clients, the CCPA creates a new private right of action that may grow in scope before the law takes effect.

Sections 1798.100-1798.125 of the CCPA (broadly defined to include all California residents) establish four basic "privacy" rights to help consumers assert greater control over personal information that businesses collect about them:

- the right to know, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
- the right to require a business to delete their personal information, with some exceptions;
- the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parent's, opt-in); and
- the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the act

Since enactment, the CCPA has already been amended once to correct a handful of drafting errors and clarify certain terms, and bills for further amendments have already been proposed. This article will outline the major changes that the CCPA is introducing into the world of data privacy, offer some observations about compliance, and describe the new and significant legal exposures for compliance failures.

Who is Subject to the CCPA?

The CCPA applies to any entity that "does business in the State of California" and satisfies one or more of the following thresholds: (1) has annual gross revenues in excess of $25 million; (2) alone, or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information.

The statute does not define what "doing business in the State of California" entails. Foreign entities should not assume they are exempt, particularly if they have customers, employees or offices in California. Barring official guidance from the Attorney General, the "doing business" test used by California courts to make state tax determinations offers some guidance. Under that test, factors that indicate an entity is "doing business in California" include physical presence in California, employees in California, or holding licenses to conduct business within California. For example, California Revenue and Taxation Code § 23101, provides that a company is doing business in California if it is "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit" in California.

Therefore, it is important for attorneys advising clients that are foreign entities to consider whether they are indeed doing business in California if they believe they satisfy at least one of the three revenue and activity thresholds described above.

Before launching compliance roadmaps, however, businesses and their counsel should carefully examine section 1798.145(c) through (f), which limits application of the CCPA to healthcare providers, financial institutions and other types of businesses that are already covered by federal sector-specific privacy laws. For example, a financial institution covered by the Gramm-LeachBliley Act may conclude that it is exempt from the CCPA entirely under subsection (e), depending on the nature and scope of its operations.

What Information Does The CCPA Cover?

The CCPA defines "personal information" much more broadly than previous data privacy statutes to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA identifies numerous examples such as online identifiers, Internet Protocol addresses, email addresses, browsing history, search history, geolocation data, and information regarding a consumer's interaction with a website or online application or advertisement. Most controversially, the CCPA's definition also includes any "inferences drawn" from any personal information that is used "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

A recently introduced bill, Assembly Bill 1130, would expand the definition of "personal information" under California's data breach notification law, Civ. Code § 1798.140, to include "other government-issued identification numbers[s]" and "[u]nique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data." Government-issued identification numbers would include passport numbers. This revision anticipates a time in the future in which the use and storage of biometric data is more prevalent than it is today.

What Does the CCPA Require Of Covered Businesses?

The CCPA requires business to adopt new policies and procedures with respect to the consumer rights that it establishes. It provides for the Attorney General to create guidance for establishing these rules and procedures that companies should evaluate and use as a guide for creating their own procedures.

Covered businesses should have procedures for the following:

1) Facilitating and governing the submission of a request by a consumer to opt out of the sale of personal information
2) Governing a consumer's request to delete personal information
3) Preparing and responding to consumer requests for information about personal data
4) Governing business compliance with a consumer's opt out request

5) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer
6) Ensure that opting out or requesting information does not discriminate against the consumer
7) Establishing rules and guidelines regarding financial incentive offerings, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information

As a practical matter, meaningful implementation of these procedures requires that a business first develop a mature "data map" to understand exactly what personal information it has about consumers, why it has that information, and where that information is stored. Therefore, data mapping is a crucial first step to ensure compliance while controlling related costs and disruption to business operations.

What Is The California Attorney General's Role?

The CCPA authorizes the Attorney General to provide compliance opinions to businesses and third parties, and a business may request such an opinion. However, another recently proposed amendment, Senate Bill 561, contemplates replacing the Attorney General's duty to provide compliance opinions to businesses and third parties with the authority to publish general guidance on how to comply with the CCPA. Attorney General Becerra, who supports the proposed amendment, was quoted as saying that his office's concern is not "giv[ing] out free legal advice" to businesses.

The CCPA requires the Attorney General to solicit broad public participation and adopt regulations to further the purposes of the law. The Attorney General must complete that process "on or before July 1, 2020." This means that the CCPA may take effect on January 1, 2020 but lack certain regulations critical to implementation for up to six months following that date. For example, the regulations must include rules "to govern a business's determination that a request for information received by a consumer is verifiable consumer request." Given that a "verified consumer request" is necessary to trigger many of the business's obligations under the CCPA's privacy provisions, one of the biggest uncertainties facing covered businesses is how to make a "verified consumer request" determination with respect to any particular request before receiving official guidance form the Attorney General. The Attorney General's Office concluded the comment period and preliminary public forums on March 8, 2019 and intends to publish its Notice of Proposed Regulatory Action by fall 2019, so covered businesses should anticipate material changes to the compliance roadmap potentially just a few months before the CCPA takes effect, and possibly after the effective date if the Attorney General's office does not meet its self-imposed deadline.

Finally, the Attorney General may institute enforcement actions against businesses that violate the CCPA. However, a business will have an opportunity to cure before an action is commenced. A business shall be in violation if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. If the business is found to have intentionally violated the CCPA, it may be liable for a civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation.

What Does The Private Right Of Action Cover, And How Might It Expand?

Section 1798.150 sets forth a private right of action for consumers whose personal information is the subject of a data breach, which means an incident in which 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' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

This section further provides for statutory damages of not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. The availability of statutory damages means that plaintiffs may sue, individually or as a class, and recover up to $750 per person per incident without having to prove they were actually harmed by the data breach.

In assessing the amount of statutory damages, courts are to consider: the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth. It remains to be seen how courts will weigh

these factors when determining the amount of statutory damages. For example, will the defendant's assets weigh more heavily if the number of violations is higher?

Consumers must meet several requirements before bringing suit. First, the consumer must provide the business with 30 days' written notice identifying the specific provisions of the consumer alleges have been or are being violated. This allows the business an opportunity to cure, but there are likely to be violations that are not amenable to cure. For example, a cure may not be feasible once third-party exfiltration of nonencrypted personal information has been verified. However, if the business cures and provides the consumer a written statement that the violations have been cured and no further violations shall occur, the consumer cannot bring suit. If the business later breaches the express written statement, the law provides a private right of action to enforce the written statement, which includes statutory damages.

The scope of the private right of action will expand dramatically if SB 561 passes. First, it would allow for private enforcement under the CCPA immediately, without prior written notice to the business. This would eliminate business's ability to cure a violation prior being sued. Second, the amendment would expand the private right of action to cover violations of the CCPA's privacy provisions, not just the data breach provision in section 1798.150. For example, a consumer would be able to sue for a business's failure to respond to "verified con- sumer requests," or a business's failure to treat consumers who have exercised their privacy rights under the CCPA equally with consumers who have not exercised those rights. It is unclear whether this bill will pass before the CCPA becomes operative on January 1, 2020, but covered businesses and their counsel should monitor its status to understand the full scope of potential legal exposure.

Notably, subsection (c) of Section 1798.150 states "Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law." Based on this amendment, it appears to preclude having a violation of the CCPA serve as a basis for a claim under California's Unfair Competition Law, California Business and Professions Code §§ 17200 et seq., which permits a private right of action for claims based on unlawful, unfair, or fraudulent business acts or practices – or under "any other law." However, an aggressive plaintiffs' bar may take the position that because the "nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law" clause is found in the data breach section of the law, it should not be interpreted as applying to UCL actions premised upon violations of the privacy sections of the law. Therefore, covered businesses should be prepared to defend actions under both the CCPA and UCL early on before courts apply the language in the statute.

How Does The CCPA Impact Consumer Agreements To Arbitrate?

Section 1798.192 of the CCPA provides, "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

The provision appears to prohibit a business' use of consumer arbitration clauses, but enforcement efforts are likely to trigger preemption challenges under the Federal Arbitration Act. Businesses would be wise to include delegation clauses to minimize the opportunity for judges hostile to consumer arbitration to void arbitration clauses outright. *See, e.g., Henry Schein v. Archer & White Sales*, 139 S. Ct. 524 (2019).

Conclusion

Several months remain before the CCPA takes effect, and there are pending bills that might change the language of the statute before it becomes operative. However, all companies doing business in California who determine that they are covered by the law should begin to prepare policies and procedures for dealing with new and expansive consumer rights and potential litigation over the handling of personal information.

- *Travis P. Brennan is a shareholder in the Newport Beach office of Stradling Yocca Carlson & Rauth, where his practice focuses on business litigation, data privacy counseling and security incident response.*
- *Katie Beaudin is an associate in the Newport Beach office of Stradling Yocca Carlson & Rauth. Her practice focuses on commercial litigation including business torts, unfair competition, intellectual property, and shareholder disputes, as well as data privacy and employment counseling.*