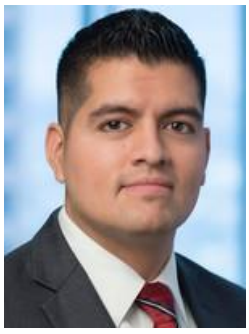
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What Corporate Attys Should Know About Calif. Privacy Act

By **Grant Davis-Denny, Najee Thornton and Nefi Acosta**
(September 25, 2018, 1:47 PM EDT)


Grant Davis-Denny


Najee Thornton


Nefi Acosta

The recently enacted California Consumer Privacy Act will bring significant changes not only to the world of data privacy and security law, but also to the practices of corporate lawyers and litigators. In this article, we highlight aspects of the CCPA that transactional attorneys, particularly those involved in mergers and acquisitions and in drafting contracts with vendors and business partners, should become familiar with before the law takes effect in January 2020.

What Are the CCPA's Key Rights and Duties?

Although a thorough discussion of **the CCPA's new rights** for California consumers and its associated new duties for businesses is beyond the scope of this article, readers should generally understand that the CCPA differs dramatically from any privacy law we have seen in the United States. Its closest analogue is the European General Data Protection Regulation, though, **as we've explained**, comparisons between the CCPA and the GDPR tend to gloss over the two laws' significant differences. Suffice it to say that the CCPA grants California residents a bevy of new rights, including the right to:

- Request that businesses give them access to their personal data and be provided with such data;[1]
- Receive advanced notice at or before the time of data collection of the data that is being collected and the purposes for which the data shall be used;[2]
- Demand that a business delete any personal data it has about the California resident, subject to certain exceptions;[3]
- Opt out of information sales such that a business cannot sell the California resident's data to a third party;[4]
- Recover statutory damages in certain circumstances.[5]

Importantly, the CCPA is not limited to particularly sensitive personal data; it applies to all information that can be reasonably linked to a California resident or California household, unless that information has been made publicly available through government records.[6] Moreover, the CCPA is not restricted to data collected over the Internet; it expressly applies to data collected through any means.[7]

Who Is Subject to the CCPA?

The CCPA's sweeping new requirements generally apply to any entity that qualifies as a "business." Therefore, the CCPA's scope depends significantly on that term's definition.

The CCPA defines a "business" as a legal entity (including a sole proprietorship) that is "organized or operated for the profit or financial benefit of its shareholders or other owners" and that "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information."[8] Further, to qualify as a "business" within the meaning of the CCPA, such an entity must do business in the state of California and satisfy at least one of three thresholds. These thresholds, however, are not demanding and will capture most medium-sized businesses and enterprise-level businesses. Annual gross revenue in excess of $25 million or the receipt of personal information on 50,000 California residents, households or devices, for example, will make the business subject to the CCPA.[9]

When Is a Related Entity Considered Part of the Business?

The definition of "business" includes certain, though not all, related entities of the business that collected the data. The CCPA governs any entity (1) that is controlled by a "business" as defined above and (2) that shares common branding with the business.

The CCPA's definition of "control" includes familiar concepts. An entity is "controlled" by a business where the business: (1) owns more than 50 percent of the outstanding equity securities of the entity; (2) has the power to vote more than 50 percent of the outstanding voting securities of the entity; (3) controls, in any manner, the election of a majority of the directors (or individuals exercising similar functions); or (4) has the power to exercise a controlling influence over the management of the entity.[10]

However, the scope of related entities that fall within the definition of "business" is significantly limited by the CCPA's common-branding requirement. The controlled entity and the affiliated entity must share common branding with the business, which means a "shared name, servicemark, or trademark."[11] Thus, portfolio companies of an investment fund or business segments of a corporation that do not share common branding with the parent generally will not be subject to the CCPA unless they themselves independently qualify as a business under the CCPA.

Can Data Regarding Residents Who Have Opted Out of Data Sales be Transferred as Part of an M&A Transaction?

As we saw above, a key provision in the CCPA gives consumers the right to opt out of future sales of their data by the business. For the purposes of the CCPA, the definition of "sell" is expansive. It includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by

the business to another business or a third party for monetary or other valuable consideration."[12] Under this broad definition of "sell," a business could breach the provisions of the CCPA by selling its business to another business or third party, coming under the control of a third party, or even disclosing personal information in connection with the diligence process.

Fortunately for the regulated community, the CCPA expressly exempts from the definition of "sell" certain M&A transactions. Subject to certain conditions, a business does not "sell" personal information when the business transfers such information "as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the business."[13] The acquiring entity must use or share personal information of California residents in a manner consistent with the CCPA's right-of-access provisions. Moreover, before the third party acquiring entity can use or share the consumer's information in a way that is materially inconsistent with the promises made at the time of collection, the acquiring entity must provide prior and robust notice to the consumer.

During the due diligence phase of an M&A transaction, in circumstances where California consumer data held by the target has value to the acquiring entity, counsel for the acquiring entity should analyze what notice the target gave to consumers at the time the target collected their data and whether that notice is consistent with the ways in which the acquiring entity plans to use or share the data. (It is unclear whether a target's notice or lack thereof prior to the CCPA's effective date (Jan. 1, 2020) limits the use or sharing of data by an acquiring entity.) If the acquiring entity anticipates altering the use or sharing of the data, counsel should also evaluate whether it will be practical to provide additional notice to California consumers. For example, the available data might not provide an easy means for communicating with the California consumer, or giving the requisite notice may impose high costs on the acquiring entity.

Counsel for potential acquisition targets should also carefully consider the impact privacy policies and notices today may have on the future value of California consumers' data that the target is currently collecting. Companies hoping to be acquired should consider whether their privacy disclosures accurately capture not only their own needs for the use and sharing of such data, but also the needs of companies that may acquire them in the future.

Can a Court Disregard the Formalities of a Series of Transactions to Find a Violation of the CCPA?

Imagine a scenario in which a parent company has received thousands of opt-out requests from California consumers. The requests have significantly reduced the value of that data to the parent because its business strategy partly involves selling the collected data to third parties. So the parent decides to create a subsidiary. Although the subsidiary is under the parent's control, there is no common branding used by the parent and subsidiary. The parent then transfers the data of California residents who have opted-out to the subsidiary as part of an M&A transaction.

May the subsidiary now sell that data to an unaffiliated third party notwithstanding the California consumers' prior act of opting-out of information sales? As a technical matter, based only on what we've covered so far, the answer would seem to be "yes." The subsidiary is not part of the parent "business," as that term is defined in the CCPA, because it does not share common branding. Because this data transfer from the parent to the subsidiary occurs as part of an M&A transaction, no "sale" occurs, based on the CCPA's definition of "sale." Finally, the subsidiary has not received an opt-out request from the consumer and is not part of the parent business that did receive an opt-out request and so is apparently free to sell the data to a downstream purchaser.

But the CCPA has an anti-circumvention provision that would raise significant risks for such a strategy. The CCPA's step-transaction provision requires a court in certain circumstances to "disregard the intermediate steps or transactions" in a series of steps or transactions. Those circumstances exist where the intermediate steps or transactions were (1) "component parts of a single transaction"; (2) that transaction was "intended from the beginning to be taken with the intention of avoiding the reach" of the CCPA and (3) disregarding those steps or transactions would further the CCPA's purposes.[14]

Anticipating future circumvention efforts, the CCPA's drafters appear to have borrowed tax law's judicially created step-transaction doctrine. Eighty years ago, the U.S. Supreme Court disregarded a transaction's intermediate steps for purposes of analyzing its tax consequences, explaining that "[a] given result at the end of a straight path is not made a different result because reached by following a devious path."[15] Since then, courts have held that a series of steps can be collapsed for tax purposes when any of three conditions are present: (1) the end result test, which asks whether there was an intent from the start to achieve the result of the combined steps; (2) the interdependence test, which examines whether the steps are so mutually related that they would have been pointless without the completion of all steps and (3) there is a binding commitment from the start to enter into a series of transactions.[16]

In modeling tax law's step-transaction doctrine, the CCPA's drafters imported into privacy law a concept that has produced vagueness and uncertainty for scholars, taxpayers and courts for decades. As one tax professor long ago remarked, "prediction is difficult to the point of impossibility"[17] when it comes to anticipating how a court will apply the step-transaction doctrine to a particular sequence of transactions.

In any event, the CCPA identifies a specific type of avoidance strategy that the step-transaction provision is concerned with: "the disclosure of information by a business to a third party in order to avoid the definition of sell." Our hypothetical scenario set forth above could result in application of the step-transaction provision. To determine that provision's applicability to our hypothetical, however, a court would have to delve into whether (1) the data transfer to the subsidiary and the sale of data to a third party were contemplated from the beginning of the series of transactions; (2) whether the intent at the beginning of these steps was to avoid the CCPA and (3) whether collapsing the steps into a single transaction would serve the CCPA's purposes.

Are Businesses Liable for the CCPA Violations of their Data Vendors?

The CCPA creates a new incentive for businesses to enter into contracts with their vendors that restrict the way in which those vendors can use California residents' data. The CCPA protects a business from liability for violations committed by its service provider if the business, at the time it discloses the information to the service provider, does not know or have reason to know the service provider intends to commit a violation.[18]

But the statute defines "service provider" as a business that processes data pursuant to a written contract that prohibits it from retaining, using or disclosing the data for any purpose other than that set forth in the contract or as otherwise permitted by the CCPA.[19]

Put differently, if a business fails to enter into a contract with its vendors that limit the processing of California residents' data to the business's specific processing objectives, the business runs the risk that it will be liable for its vendors' violations of the CCPA.

Grant Davis-Denny is a partner and Najee Thornton and Nefi Acosta are associates at Munger Tolles & Olson LLP.

[1] Cal. Civ. Code §§ 1798.110, 1798.115.

[2] § 1798.100(b).

[3] § 1798.105(a), (c), (d).

[4] § 1798.120(a).

[5] § 1798.150(a)(1).

[6] § 1798.140(o).

[7] § 1798.175.

[8] § 1798.140(c).

[9] § 1798.140(c)(1)(A), (B).

[10] § 1798.140(c)(2)

[11] § 1798.140(c)(2).

[12] § 1798.140(t)(1).

[13] § 1798.140(t)(2)(A)(D).

[14] § 1798.190.

[15] Minnesota Tea Co. v. Helvering, 302 U.S. 609, 613 (1938).

[16] Kenna Trading, LLC v. Commissioner of Internal Revenue, 143 T.C. 322, 355-56 (2014).

[17] Ralph S. Rice, Judicial Techniques in Combating Tax Avoidance, 51 Mich. L. Rev. 1021, 1047 (1952-1953).

[18] § 1798.145(h).

[19] § 1798.140(v).