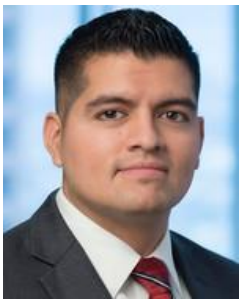
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The California Consumer Privacy Act: 3 Early Questions

By **Grant Davis-Denny, Jordan Navarrette and Nefi Acosta**
(July 2, 2018, 4:28 PM EDT)

Grant Davis-Denny

Jordan Navarrette



Nefi Acosta

Less than two weeks ago, the most far-reaching privacy measure ever to be enacted in this country had not even been introduced in the California Legislature. But careful deliberation was a luxury lawmakers no longer could afford. It was by then apparent that a ballot initiative called the California Consumer Privacy Act of 2018 was going to qualify for the November ballot. And there was growing concern that aspects of the initiative — such as a statutory damages provision for any violation of the CCPA's new duties, a new whistleblower and private attorney general enforcement system and a provision prohibiting future amendments to the initiative without 70 percent approval in the Legislature — were deeply flawed. Only a week before the deadline for removing the initiative from the ballot, legislators reached a compromise with the measure's proponent: If the Legislature passed and the governor signed a modestly amended version of the initiative by June 28, 2018, the proponent would withdraw his measure. And so, with limited opportunity for deliberation, the Legislature passed and the governor signed the compromise legislation just hours before the deadline.[1]

Barring major amendments, that bill, also called the CCPA, will dramatically change the privacy landscape in the United States on Jan. 1, 2020, when the law kicks into effect. It is difficult to overstate the law's scope. Unlike data breach statutes, which typically limit "personal information" to names plus Social Security numbers, driver's license numbers and certain other specific categories of data, the CCPA's new duties apply to nearly any data that identifies, relates to, describes or can be linked or associated with a California resident or household. Companies that possess personal information about California residents and that have more than $25 million in revenue are covered. So too are companies that have data on at least 50,000 California residents or that make at least 50 percent of their revenue from selling consumer data. Businesses located outside California but that do business in the state also are subject to the CCPA if they satisfy one of the tests previously mentioned. The law applies to California residents' personal information regardless of how it was collected or maintained (even by paper).

To highlight just a few of the new duties covered companies will face:

- Twice in any 12-month period, a California resident may request, and the company must promptly disclose: (1) the categories and specific pieces of data that the company has collected from that individual; (2) the categories of sources from which the data was collected; (3) the categories of third parties that the data has been disclosed or sold to; and (4) for what purpose it was disclosed or sold. Businesses must provide this information within 45 days (subject to a 90-day extension where necessary), for free, and — if provided electronically — in a portable and readily usable format (if technically feasible).

- Companies must provide California residents with advance notice of data that will be collected and the purpose for which it will be used, and must limit their use of the data to those disclosed purposes unless notice of the new use is provided.

- California residents can submit requests to be forgotten to companies. Subject to certain exceptions, companies must comply by deleting data about those individuals and by instructing their service providers to do the same.

- Customers must be given means to opt out of having their information sold. A covered business must include a clear and conspicuous link on its homepage titled "Do Not Sell My Personal Information."

These are certainly not all of the new duties. The law, for example, also imposes new requirements for website privacy policies and prohibits businesses in many circumstances from discriminating against customers who exercise rights created by the CCPA. The critical point is that the CCPA's new obligations are substantial, and most major businesses will need to hire new employees, perhaps even set up new departments, to respond to information demands, requests to be forgotten and opt-out communications. The CCPA will force companies that routinely receive and transmit information to third parties to rethink how they track and organize such data so that they can be in a position to respond to these requests and to ensure that information is not used for an undisclosed purpose.

For the regulated community, a new statutory damages provision also may have significant consequences. Businesses face up to $750 in damages liability per California resident per incident for certain breach events. Come 2020, an unencrypted list of records containing, for example, the names and Social Security numbers of 1 million California residents will represent a potential $750 million liability.

The CCPA has significant drafting defects. Portions of the bill are unintelligible. For example, it is unclear what the drafters meant to convey with the last phrase in the CCPA's definition of "publicly available": "information that is lawfully made available from federal, state or local government records, if any conditions associated with such information."[2] Because the CCPA's definition of "personal information" excludes "publicly available" data, and because the definition of "personal information" plays a critical role in defining the scope of the CCPA's new duties, this is a significant drafting error.

The CCPA also contains ambiguities that lawyers, courts and the regulated community will have to work through. Highlighted below are a few areas where the bill is likely to sow confusion and litigation.

What will plaintiffs have to show to recover statutory damages?

The CCPA's statutory damages clause provides in relevant part that any California resident "whose nonencrypted or nonredacted personal information, as defined in [Civil Code Section 1798.81.5], 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" is liable for statutory damages of between $100 and $750 per California resident and per incident.[3]

This statutory damages provision uses a narrower definition of "personal information" than the CCPA definition; this narrowed definition is more like ones found in state data breach statutes. To pursue a statutory damages remedy, a plaintiff must give the defendant and the attorney general advanced notice before filing a complaint. If the company cures the alleged violation within 30 days, it can avoid a lawsuit. The act also provides for 30 days' notice to the attorney general, who can then choose to prosecute the action, refrain from doing so and allow the consumer to proceed, or notify the consumer that he or she may not proceed with the action.

The CCPA's statutory damages provision raises at least two critical issues.

First, what is the significance of the phrase "subject to" unauthorized activity? Expect plaintiffs attorneys to argue that substandard security measures make a business liable for statutory damages even if no actual breach occurs. Courts will have to determine whether the Legislature intended such an extreme remedy when no evidence exists that unauthorized persons even accessed the data, let alone stole or used it in a manner that could actually harm a consumer.

Second, consumer attorneys may try to stretch this provision to cover violations of the CCPA's duties, and not just data theft incidents. While there are compelling arguments that this is not what the Legislature intended, plaintiffs may attempt to argue that any unauthorized disclosure — such as the sale of a consumer's information who has opted-out or the disclosure of data that exceeds the scope of what the business had disclosed to the consumer — opens the business up to statutory damages liability.

What obligation does the CCPA impose on covered businesses to make California residents' data portable?

When a California resident exercises his or her new right to data portability, a business is required to deliver that resident's information, free of charge, "in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit this information to another entity without hindrance."[4]

The CCPA appears to borrow the "technically feasible" qualifier from Article 20 of the European General Data Protection Regulation, which also addresses a right to data portability. Guidance from European regulators indicates that portability "aims to produce interoperable systems, not compatible systems"; that "[t]he terms 'structured,' 'commonly used' and 'machine-readable' are a set of minimal requirements"; and that "formats that are subject to costly licensing constraints would not be considered an adequate approach."[5] It remains to be seen whether California regulators will import this interpretive guidance from Europe or instead apply their own gloss to Californians' newfound right to data portability. Their answer could significantly impact the cost of compliance for businesses that maintain structured data about consumers in proprietary formats or formats that require substantial licensing fees to access.

How much flexibility will businesses have in responding to requests to be forgotten?

California's new right to be forgotten — i.e., the duty of businesses to delete data regarding California residents when residents submit such a request — is subject to several important yet ambiguous exceptions that find no analogue in the European GDPR.

First, businesses are not required to delete data if it is necessary to maintain the data to "[c]omplete the transaction for which the personal information was collected, *provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer*, or otherwise perform a contract between the business and the consumer."[6] The italicized language leaves considerable room for interpretation. In determining what is reasonably anticipated, whose expectations — the business', the customer's or both — matter? Another issue is what constitutes an "ongoing business relationship," a phrase the CCPA leaves undefined. Consumers may contend that the relationship ends the moment an ordered good or service is delivered; but covered businesses may contend that it continues until an affirmative step is taken to terminate the relationship.

Second, the CCPA allows businesses to decline deletion requests in two circumstances where data is needed for internal operations: (1) "to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business"; and (2) to "[o]therwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."[7] Although neither exception grants businesses an unfettered right to keep information for purely internal purposes in all instances, the qualifiers in the two exceptions — i.e., the California resident's expectations based on his or her relationship with the business and compatibility with the context in which the data was provided—leave considerable room for debate and interpretation.

Finally, the CCPA's right to be forgotten may raise new document preservation challenges for large organizations that routinely battle lawsuits on multiple fronts. The CCPA does contain an exception to the right to be forgotten where a company needs to keep the data to comply with legal obligations, an exception that should allow a company to deny a deletion request where the company appreciates the need to preserve the data. The problem then is not so much a legal one as it is logistical: in companies with thousands or tens of thousands of employees, the relevance of a California resident's data to an ongoing litigation matter may not be apparent to the employee responsible for responding to deletion requests, particularly where that resident is not a named party in the case. Adverse parties could contend that this inadvertent destruction constituted spoliation, and request that a court impose sanctions on the company for failing to properly preserve evidence. On the other hand, a policy that denies data deletion requests as a matter of course to avoid any risk of spoliation likely runs afoul of the CCPA's right to be forgotten. Companies will have to craft appropriately-tailored procedures that balance the right to be forgotten with their data preservation obligations in litigation.

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

[1] Cal. Assem. Bill No. 375 approved by Governor, June 28, 2018.

[2] Cal. Civ. Code § 1798.140(o)(2).

[3] Cal. Civ. Code § 1798.150(a)(1).

[4] Cal. Civ. Code § 1798.100(d).

[5] Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability at 17, 16/EN WP 242 rev.01, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf.

[6] Cal. Civ. Code § 1798.105(d)(1) (italics added).

[7] Cal. Civ. Code § 1798.105(d)(7), (9).