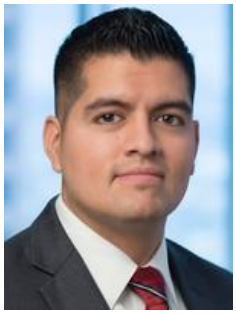
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What To Remember About Calif.'s Right To Be Forgotten

By **Grant Davis-Denny and Nefi Acosta**
(November 6, 2018, 1:43 PM EST)

Grant Davis-Denny



Nefi Acosta

Among the new rights for California residents in the California Consumer Privacy Act of 2018 is the ability to request that a business delete from its systems the consumer's personal information. Sometimes referred to as the "right to be forgotten," this new privilege will impose significant new duties on businesses that maintain data about California residents and that are within the CCPA's broad scope.

As part of a series of articles on the CCPA (see "**Confusion In Calif. Privacy Act's Anti-Discrimination Rule**," "**California's Consumer Privacy Act Vs. GDPR**" and "**What Corporate Attys Should Know About Calif. Privacy Act**"), in this piece we will explore the contours of California's right to be forgotten, ambiguities in this new right and the challenges that it may raise for the regulated community.

Which Consumers Can Request Deletion of Their Data?

Although the CCPA broadly defines "consumer" to include all California residents,[1] the CCPA's right to be forgotten may apply only to a particular subset of consumers: those from whom the business has collected personal information.

Imagine a California resident who has privacy concerns about two businesses that store data on consumers' movie watching preferences. The first business, a streaming service, collects data from its consumers based on the movies their users order through the streaming service. The second, a data broker, collects data on its consumers not directly from the consumers, but by purchasing the data from the streaming service. As a consumer, can the resident force both businesses to delete his or her data?

It is not clear that the resident can. The CCPA's text provides that "[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer."[2] While the streaming service collected data directly from the consumer, and thus is likely subject to the deletion duty, the data broker obtained the data through an intermediary business, not from the consumer.

Interestingly, the CCPA's drafters did not use the phrase "business has collected from the consumer"

when they defined the type of consumer information subject to other new rights and duties that the privacy law created. For example, while the CCPA requires businesses to notify consumers about what information they collect and the purposes for which it will be used, that requirement applies to a "business that collects a consumer's personal information,"[3] without specifying from whom the business must collect that information. Similarly, the duty to disclose a consumer's information to that consumer in response to a request applies to any "business that collects personal information about the consumer,"[4] and does not specifically refer to information collected directly from the consumer. Further, the CCPA's restrictions on selling the personal information of certain minors cover "a business that sells personal information about the consumer to third parties."[5] That the CCPA's drafters used the phrase "from the consumer" in the right to be forgotten provision but used the phrase "about the consumer" when defining other rights and duties could be interpreted by a court as a sign that "from the consumer" means direct collection from the consumer and not through an intermediary entity.

If the duty of deletion does not apply to information that a business collects through an intermediary, it could have consequences for the regulated community. First, it could cause businesses to reconsider how they obtain data about California consumers. They might, for example, use certain types of intermediary entities to collect data from consumers and transfer that data to a separate affiliate that can then take the position that it did not collect data from the consumer. Or businesses might put more value on data that they purchase through unaffiliated data brokers, as opposed to information that they receive from the consumer. For businesses that try to draw a line between the two categories of data — the information they receive directly from the consumer and consumer data that they obtain from other entities — they will have to face the operational challenge of tracking the source of each piece of data about a California resident and use that source data to determine the categories of data that they will keep and the categories that they will delete.

Which Third Parties Must Also Delete Data When a Business Receives a Request to Be Forgotten?

After receiving a verifiable request to delete data from a consumer, a business must not only delete data from its own records but must also "direct any service providers to delete the consumer's personal information from their records."[6] This aspect of the CCPA raises at least two issues.

The first arises from the CCPA's peculiar definition of "service provider." Under the CCPA, that phrase is limited to entities with whom the principal business has "a written contract" that "prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specified purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title."[7] Thus, when a business transfers information to a vendor but does not have the type of written contract described in the CCPA's definition of "service provider," the vendor would not meet the definition of "service provider." Therefore, the CCPA's text suggests that the principal business has no duty to direct such vendors to delete consumers' data. Read literally, this would appear to create an odd incentive for businesses not to enter into contracts with vendors protecting the privacy of consumer data. To be sure, the CCPA does create a countervailing incentive for businesses to enter into contracts with vendors. If they do so, they are not liable for the service provider's violations that they do not know or have reason to know will occur.[8] But some businesses may weigh the costs and benefits of treating vendors as "service providers" and conclude that they are better off without written contracts limiting the use of consumers' data.

The second issue concerns the new information tracking duties that businesses will have when they share information with "service providers." Suppose there is an e-commerce business — Widgets-R-Us — that sells a widget to a California resident named Sally Smith and receives her mailing information.

Over the course of several years, multiple employees of Widgets-R-Us then include Smith's data in spreadsheets containing information about tens of thousands of other former purchasers and distribute those spreadsheets to: (1) a marketing consultant that is helping the business to target potential buyers of the new and improved Widget Plus; (2) an economics consultant who is assisting the business with modeling long-term demand for widgets; and (3) an information technology consultant who is redesigning the businesses' customer relationship management database.

Smith submits a request to Widgets-R-Us to delete her data. Widgets-R-Us deletes that data from its own records, but now must figure out which service providers to direct to delete the data. It is exceedingly unlikely that any of the employees who circulated a spreadsheet containing Smith's name to a service provider would recall years later that this was done. It is conceivable that Widgets-R-Us's database stores details about when and who exported discrete pieces of data. But it is unlikely that the database has data about why the data was exported or to whom it was sent. Businesses may thus face significant operational challenges when determining which service providers they will need to instruct to delete data.

How Will Businesses Show the Verifiability of a Consumer Request to Be Forgotten?

A business' duty to delete data arises after the business has received "a verifiable request from a consumer to delete the consumer's personal information."[9] The CCPA's drafters, however, did not specify how businesses can verify the legitimacy of consumers' requests. Instead, they assigned to the California attorney general the task of developing regulations that will identify verification requirements.[10]

While we wait to see what verification requirements the attorney general will propose and then adopt, we can ponder a potential problem. The consumer making the request will have to submit his or her personal information to verify the legitimacy of the request to be forgotten. If the business verifies the request, the business will then use that information to delete the existing information about the consumer. Will the business then be able to retain the information that the consumer submitted to verify the legitimacy of her request? If not, then the business has no way to internally audit or show regulators whether it followed an appropriate process for verifying the legitimacy of a deletion request. Perhaps a business would be able to retain such verification data under one of the exceptions to the right to be forgotten, such as the internal-use or detecting-fraudulent-activity exceptions. But then what if the data the consumer has to submit in order to verify the data deletion request reveals as much about the consumer as the data that the consumer requested to be deleted in the first place. The verification process then would seem to have frustrated the consumer's original purpose in making the request.

What Are the Significant Exceptions to the CCPA's Right to Be Forgotten?

The CCPA enumerates nine exceptions to the right to be forgotten. Space prohibits us from exploring each in detail. But a few appear especially significant.

First, the CCPA allows businesses to retain consumer information where it is needed 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."[11] Although it is not exactly clear what the "reasonably anticipated" phrase modifies, it might allow a business to retain data if a reasonable consumer would have expected that a good or service could be

provided by the business as part of an ongoing business relationship and the information is necessary to provide that service.

This exception may raise a number of thorny questions for businesses about what constitutes an ongoing business relationship (or to put it differently, when does a business relationship come to an end), about what reasonable consumers expect, and about what qualifies as a service to the consumer. An online clothing business could argue that one service it provides to its customer base is keeping them informed of the latest fashion trends by way of its seasonal catalogues. After receiving a request from a customer to delete his or her data, but in the absence of a request from the customer to stop receiving catalogues or terminate the business relationship, is the business allowed to retain the customer's data for the purpose of providing this "service"? The CCPA does not provide a clear answer to this question.

The CCPA also contains two exceptions that allow businesses to retain data in certain circumstances where necessary for internal uses. One exception allows for data to be kept "[t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[12] Another allows businesses 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."[13]

The CCPA does not define "internal use" or any similar phrase. While sharing information outside the company probably would not qualify as an internal use, it is less clear whether a company's marketing department, for example, could leverage the data to design a marketing strategy In that example, the data is not leaving the company, though it is being used to generate external communications. It is unclear whether this is sufficient to remove this data usage from the "internal use" exception. The first internal use exception, moreover, ties the permissibility of an internal use to that use's reasonable alignment with the consumer's expectations. Determining how consumers would expect businesses to use data internally seems to be a highly speculative endeavor. Setting that concern aside, businesses may be able to help set consumer expectations about internal uses by identifying such internal uses in their privacy policies.

Does the CCPA's Right to Be Forgotten Raise First Amendment Concerns?

Imagine John Smith, a CPA, decides to run for his local school board in California. During the campaign, a former accounting client posts a negative review of Smith on a consumer-review website. Smith submits to the website a request to delete any data mentioning Smith. Does the First Amendment allow the government to impose a civil penalty on the website owner for violating the CCPA if the website owner refuses to delete the negative review of Smith?

Any such imposition of fines would seem to raise serious First Amendment concerns. The restriction appears content-based — i.e., the duty to delete and the threat to impose fines arise from the website review's reference to Smith. As a content-based restriction, the CCPA's right to be forgotten would be subject to strict scrutiny, and thus to survive review the law as applied to these circumstances would have to be narrowly tailored to serve a compelling government interest. And it seems unlikely the government could persuade a court that there is a compelling government interest in removing a review of a candidate's prior performance from the marketplace of ideas.

The CCPA's drafters appear to have foreseen potential First Amendment concerns, as they included an exception to the duty of deletion where "necessary for the business or service provider to maintain the consumer's personal information in order to … [e]xercise free speech, ensure the right of another

consumer to exercise his or her right of free speech, or exercise another right provided for by law."[14] Of course, even without such language, the First Amendment would limit the CCPA's reach. The critical question is where the dividing line sits between protected speech that can be preserved and unprotected speech that must be deleted in response to a consumer request. The CCPA provides no answer to that question.

In light of this uncertainty and in order to avoid a potential enforcement action by the California attorney general, a risk exists that the regulated community may err on the side of over-deletion. We expect courts to have to grapple with this important issue after the CCPA takes effect in 2020.

Grant Davis-Denny is a partner and Nefi Acosta is an associate at Munger Tolles & Olson LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Cal. Civ. Code § 1798.140(g).

[2] § 1798.105(a).

[3] § 1798.100(a).

[4] § 1798.105(a).

[5] § 1798.120(b).

[6] § 1798.105(c).

[7] § 1798.140(v).

[8] § 1798.145(h).

[9] § 1798.105(c).

[10] § 1798.140(y).

[11] § 1798.105(d)(1).

[12] § 1798.105(d)(7).

[13] § 1798.105(d)(9).

[14] § 1798.105(4).