

Updated July 30, 2020
June 24, 2020

STATE LAWS

How to Comply With Key CCPA Notice and Consumer Request Requirements

By *Hilary Lane, Quarles & Brady*

On June 1, 2020, after four iterations and several rounds of comments, the California Office of the Attorney General (AG) submitted the **final text** of the California Consumer Privacy Act Regulations (the Regulations) to the Office of Administrative Law (OAL). This article highlights some of the CCPA's key requirements regarding notices to consumers and handling consumer requests to exercise their rights to know and delete and offers steps to take to prepare for enforcement.

See also CSLR's two-part series examining the CPPA close-up: "[Review of Amendments and How to Prepare for Compliance](#)" (Oct. 2, 2019); and "[The GLBA Carve-Out and How Financial Institutions Can Evaluate Applicability](#)" (Oct. 9, 2019).

Timing and Procedural History of the Regulations
Under the CCPA, effective on January 1, 2020, the California legislature granted regulatory enforcement authority to the AG and required the AG to adopt regulations to further its purposes. The AG released its first proposed regulations in October 2019. Following public comment periods that generated thousands of pages of comments and included four public hearings, the AG issued substantially revised regulations in February 2020, and, after another round of comments, released a second modified version in March 2020.

With a July 1, 2020 enforcement date and deadline for promulgating regulations, the final proposed regulations were issued on June 1, and they are virtually identical to the March version. Together with the final regulations, the AG published a 59-page Final Statement of Reasons (FSOR), which includes responses to the comments received during the rule-making process and provides some insight into the AG's reasoning.

See also "[The Growing Role of State AG in Privacy Enforcement](#)" (Nov. 28, 2018).

Approval Process Could Delay Effective Date
The Regulations become effective and enforceable once approved by the OAL and filed with the Secretary of State. The OAL typically has 30 working days to complete its review of the proposed regulations. Two executive orders issued by Governor Gavin Newsom in response to COVID-19 give the OAL an additional 120 days if needed. Thus, the OAL has until November 13, 2020 to approve the Regulations.

Generally, regulations filed with the Secretary of State become effective on the first day of the quarter after they are approved. However, earlier effective dates can be granted for good cause.

The AG asked the OAL to expedite the review process to complete its review within 30 business days and also requested that the Regulations become effective upon approval, citing the July 1 deadline for adopting the regulations as good cause to justify the expedited timeline.

It is uncertain if the OAL will expedite its review or if it will grant the AG's request that they become effective upon approval.

Enforcement Will Not Wait
Regardless of whether the OAL grants the AG's request for expedited review and approval, the AG has authority to enforce the statutory requirements under the CCPA starting July 1, 2020. Despite calls from industry groups to delay enforcement of CCPA in light of the COVID-19 pandemic, the AG declined to extend the enforcement date, noting in its press release that "[b]usinesses have had since January 1 to comply with the law, and we are committed to enforcing it starting July 1."

In a June 30, 2020 alert, the AG reminded consumers of their rights under the CCPA and provided guidance - including a shareable graphic explaining how to exercise those rights. The alert also reaffirmed the AG's commitment to enforcing the law starting July 1.

1

At a webinar on July 7, 2020, California Supervising Attorney General Stacey Schesser confirmed that the AG had issued enforcement letters on July 1. Speaking broadly to preserve confidentiality, Schesser stated that the letters did not target a particular industry or sector, but noted that the "initial swath" focused on businesses that operated online and were required to provide online mechanisms for consumers to exercise their rights.

Schesser specifically mentioned the right to opt out of the sale of personal information and stated that businesses that are selling personal information that do not have a clear and conspicuous DO NOT SELL link should cure as quickly as possible.

The businesses that received notices have 30 days to cure the alleged violations. If they do not cure, the AG could launch a confidential investigation or an enforcement action. We should learn more on July 31 when the cure period expires.

The key takeaway is that businesses should be prepared to meet the CCPA statutory requirements and should consider taking steps to comply with the requirements under the Regulations when they become effective.

See also "[Privacy Settings May Serve as One-Step CCPA Opt-Out From Sale](#)" (Cybersecurity Law Report, June 17, 2020)

Notice Requirements
The CCPA requires all businesses to have a privacy policy. Additionally, businesses that collect personal information must provide a notice at or before collection, informing consumers of the categories of personal information to be collected and the purposes for which the categories will be used (Notice of Collection).

The Regulations include requirements and guidance, some of which appear to go beyond the language of the statute, relating to the substance of the notices and how the notices should be presented.

Contents and Delivery of the Privacy Policy
The CCPA requires that the privacy policy include, among other things, information about the categories of information collected, disclosed and sold and a description of consumers' rights under the CCPA.

The Regulations require that the privacy policy include:

- the categories of personal information collected about consumers in the preceding 12 months;
- the categories of sources from which the personal information was collected;
- the business or commercial purpose for collecting or selling personal information;
- the categories of personal information the business has disclosed for a business purpose or sold to third parties in the preceding 12 months; and
- for each category identified, the categories of third parties to whom the information was disclosed or sold.

Additionally, the Regulations require that the policy describe the categories "in a manner that provides consumers a meaningful understanding of the information being collected," why it was collected or sold, and the type of third party to which information is disclosed or sold.

The privacy policy should be posted online through a conspicuous link using the word "privacy" on the business's website or on the download or landing page of a mobile application. Additional provisions regarding the policy provide:

- Mobile applications **may** also include a link to the privacy policy in the application's settings menu.
- If the business has a California-specific description of consumers' privacy rights on its website, the privacy

2

policy should be included in that description.

- A business that does not operate a website should make the privacy policy "conspicuously available" to consumers.
- The privacy policy must be available in a format that allows a consumer to print it out as a document.

Contents and Presentation of Notice at Collection
The CCPA requires that a business provide notice at or before the point of collection of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. The notice must also include or, in the case of offline notices, disclose where the consumer can find:

- a link to the business's privacy policy; and
- if the business sells personal information

With respect to employment-related information, the notice does not need to include the Do Not Sell link or the link to the privacy policy. And a business that does not collect personal information directly from the consumer does not need to provide a notice at collection if it does not sell the consumer's personal information.

The notice at collection must be readily available where consumers will encounter it at or before the point of collection of any personal information. The Regulations provide "illustrative examples" of how the business "may" present the notice:

- **Online collection.** Post a "conspicuous link" to the notice on the introductory page of its website and on all webpages where personal information is collected.
 - May be provided through a link to the section of the privacy policy containing the required information.
- **Mobile applications.** Provide a link on the mobile application's download page and within the application, such as through the application's settings menu.

• **Offline.** Include notice on printed forms that collect personal information, provide a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

• **Telephone or in person.** Provide notice orally.

The AG confirms in the FSOR that businesses have discretion to determine how to provide notice in various contexts that these are "some of the ways in which the business can make the notice readily available to consumers in a variety of contexts" The AG further states that the use of the term "may" allows businesses discretion in determining the best way to communicate the required information and provides them with the flexibility to craft the notices and privacy policy in a way that the consumer understands them.

Disclosures About Consumers' Rights and Processes for Minors
The Regulations also require more detailed disclosures with respect to consumers' rights including:

- instructions for submitting a verifiable request to know or delete, which link to an online request form or portal for making the request, if either are offered;
- a general description of the process the business will use to verify the consumer request, including any information the consumer must provide;
- instructions about how an authorized agent can make a request on a consumer's behalf; and
- a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

Additionally, the Regulations require that a business that has actual knowledge that it sells the personal information of minors provide a description of the processes for:

3

- obtaining affirmative authorization from the parent or guardian of children under 13 years old to sell their personal information; and
- allowing minors between the ages of 13 and 16 to opt in to the sale of their personal information.

See "[How to Approach CCPA's Under-16 Opt-In Consent](#)" (Feb. 12, 2020).

Requirements That Go Beyond the Statute
The Regulations include two requirements that appear to go beyond the CCPA. In response to comments that these two provisions are outside the scope of the CCPA, however, the AG states in the FSOR that the ability to adopt regulations that "fill in details not specifically addressed by the CCPA, but fall within the scope of the CCPA" is inherent in the authority to adopt regulations as necessary to further the purposes of the CCPA. The AG further states that the sections are "consistent with the language, intent, and purpose of the CCPA."

1) Mobile Device Just-in-Time Notice
The Regulations require a "just-in-time" notice for the collection of personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect. The notice must include a summary of the categories of personal information being collected and a link to the full notice at collection.

This requirement is not in the CCPA. The AG states in the FSOR that the provision is necessary "to provide transparency into business practices that defy consumers' reasonable expectations, particularly when those uses are not reasonably related to an application's basic functionality."

2) Explicit Consent Requirement for New Users
The CCPA provides that a business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with "notice consistent with the notice at collection requirements."

The Regulations go beyond the CCPA notice requirement and require the business to directly notify the consumer and obtain explicit consent "for the use of previously collected personal information "for a purpose materially different than what was previously disclosed to the consumer in the notice at collection."

The AG disagrees with comments that the CCPA "only requires an additional notice and prohibits a consumer-consent requirement" and states that requiring explicit consent puts the consumer in the same position they would have been had the material change been disclosed during the consumer's first engagement with the business." The AG further states that simply updating the privacy policy or providing notice without obtaining explicit consent does not serve the purpose of the CCPA.

While businesses with account holders or that otherwise have contact information for consumers may be able to directly notify those consumers and obtain their consent, it is unclear how a business can directly notify and obtain consent from users for which it has no contact information.

Presentation of the Notices
The CCPA requires that the notices should be presented in a form that is reasonably accessible to consumers. Additionally, all required notices must use "plain straightforward language and avoid technical and legal jargon and be in a format that draws the consumer's attention to the notice and makes the notice readable on smaller screens."

4

Notices also must be:

- available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements and other information to consumers.
- reasonably accessible to consumers with disabilities. For online notices, businesses must follow "generally recognized industry standards" such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018 from the World Wide Web Consortium.

Business Practices for Handling Consumer Requests
The CCPA grants consumers the rights to request that a business disclose information about the personal information that it has collected about the consumer (Right to Know) and to request deletion of personal information about the consumer that the business has collected from the consumer (Right to Delete).

The Regulations provide requirements and guidance relating to methods for submitting and responding to these requests.

Methods for Submitting Requests to Know
The CCPA requires businesses to make available two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number.

The Regulations provide that other acceptable methods include but are not limited to:

- designated email address;
- form submitted in person; or
- form submitted through the mail.

The statute further provides that businesses that:

- operate exclusively online and have a direct relationship with consumers from whom they collect personal information shall only be required to provide

an email address for submitting requests.

- maintain an internet website must make the internet website available to consumer to submit requests to know.

The Regulations reiterate the CCPA provision regarding the requirement to provide an email address for submitting requests to know. However, comments were submitted that the statute has not defined the term "exclusively online," to which the AG responded that they did not address the definition "in an effort to prioritize drafting regulations that operationalize and assist in the immediate implementation of the law and that further analysis is required to determine whether a regulation is necessary on this issue." The AG added that whether a business is operating "exclusively online" may be a fact-specific determination.

Method for Submitting Requests to Delete
The Regulations require two or more designated methods for submitting requests to delete as well. When determining which methods to use to submit requests, however, a business shall consider the methods by which it primarily interacts with consumers. For example, if the business interacts with consumers in person, it should consider an in-person method such as a printed form, a tablet or portal that allows the consumer to submit an online form, or a telephone by which the consumer can call the toll-free number.

A toll-free number is not required (however, as a practical matter, since many businesses have to have a toll-free number for a request to know, the toll-free number is a logical choice for requests to delete), but it is one of the acceptable methods, which also include, but are not limited to a:

- link or form available online through a website;
- designated email address;
- form submitted in person; and
- form submitted through the mail.

5

- *Requests to delete* – verify to a reasonable or reasonably high degree of certainty depending on the sensitivity of the data and the risk to the consumer from deleting the information.

Timeframe for Responding to Consumer Requests
The CCPA requires a business to respond to consumer requests within 45 calendar days of receipt of the request. It also permits an additional 45 calendar days when reasonably necessary so long as the consumer is provided notice of the extensions within the first 45 calendar-day period. The response period begins on the day that the business receives the request, regardless of the time required to verify and, if the business cannot verify the consumer within the 45 calendar-day time period, it may deny the request.

The Regulations additionally require the company to confirm receipt within 10 business days and provide information about how the business will process the request including:

- a general description of the verification process; and
- when the consumer can expect a response.

Responding to Requests to Know
The Regulations provide guidance with respect to searching information in response to requests to know. A business is not required to search for personal information if it:

- does not maintain personal information in a searchable or reasonably accessible format;
- maintains the personal information solely for legal or compliance purposes;
- does not sell personal information and does not use it for any commercial purpose; and
- describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions.

The Regulations prohibit the disclosure of Social Security number, driver's license number, or other government-issued ID number, financial account number, any health insurance or medical identification number, account password, security questions and answers or unique biometric data in a company's response to a request to know. However, the business should inform the consumer with sufficient particularity if it has collected that type of information.

The Regulations further provide that when transmitting personal information to the consumer, businesses should use reasonable security measures. For password-protected accounts, businesses can comply with request to know by using a secure self-service portal for consumers to access, view and receive a portable copy of their personal information.

Responding to Requests to Delete
The Regulations provide three methods for complying with requests to delete:

- permanently and completely erase the personal information on its existing systems with the exception of archived or back-up systems;
- deidentify the personal information; or
- aggregate the personal information.

The Regulations require the business to inform the consumer whether or not it has complied with the request. If the business has complied with the request, it is required to inform the consumer that it will maintain a record of the request as required by the Regulations.

If the business denies the request, it must:

- inform the consumer that it will not comply with the request and describe the basis for the denial unless prohibited by law;

6

- delete the consumer's personal information that is not subject to an exception; and
- not use the consumer's personal information retained for any other purpose than provided by that exception.

If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if that individual would like to opt out of the sale of his or her personal information and shall include either the contents of or a link to the notice of right to opt out.

Immediate Notice and Consumer Request Action Items
To comply with the CCPA and the accompanying Regulations, given the impending July 1 enforcement date, if they have not done so already, companies should take the following steps now:

1. Review and update your privacy policy to ensure it meets the CCPA requirements as well as the more detailed notice requirements in the Regulations with respect to substance and presentation.
2. Identify where you collect personal information and ensure you have a notice at or before the point of collection informing consumers of the personal information collected and the purpose for which it will be used.
3. Make sure all required notices, including the privacy policy and other notices at collection meet accessibility standards and are in the appropriate language.
4. Ensure you have a written consumer rights management policy and verification process that meets the requirements of the CCPA and the Regulations.

7

See also CSLR's two-part series on CCPA priorities: "[Turning Legislation Prep Into a Program Shift](#)" (Jun. 5, 2019); "[Tackling Data Subject Rights Requests and Vendors](#)" (Jun. 12, 2019).

©2020 Cybersecurity Law Report. All rights reserved.

8