LOEB & LOEB LLP

Privacy

OCTOBER 2019

A Little Clarity, A Lot of Questions: An Analysis of the California AG's Proposed CCPA Regulations

The California attorney general's office on Oct. 10 released the long-awaited proposed regulations to the California Consumer Privacy Act. As noted in the statement of reasons, these regulations are intended to "operationalize the CCPA and provide clarity and specificity to assist in the implementation of the law."

Key Takeaways:

- While the proposed regulations certainly offer more details on the Attorney General's expectations for how the California Consumer Privacy Act will be operationalized — often in the form of additional obligation on businesses — businesses hoping for complete clarity on how to verify consumers or how to structure their financial incentives may be left with more questions than answers.
- The regulations add new record-keeping obligations that were not included in the CCPA, including the obligation to maintain and disclose metrics on the number of requests received and the business's response time (for those that touch data of more than 4 million consumers). These obligations may create a costly administrative burden for companies that aren't set up to track this data. Additionally, businesses offering financial incentives will have to provide a "good faith estimate" of the value of the consumer's data to the business and a description of how that value is calculated. Companies who offer loyalty programs should pay close attention to how these requirements impact their programs.
- For companies that "sell" personal information, the regulations impose notification obligations that are not contemplated in the statute. Upon receiving a do-not-sell request, a business must notify all third parties it sold data to in the past 90 days that the consumer has opted out of the sale, and must notify the consumer when those notification are complete.

We don't expect that these regulations will be completely re-written following the comment period, but there are certainly areas where we can suggest changes or flag significant compliance challenges. Written comments can be submitted by mail or email or in person at four public hearings scheduled throughout California during the first week of December. The deadline to submit written comments is Dec. 6, 2019, at 5 p.m. (PST). Please reach out to a member of Loeb & Loeb's Privacy, Security & Data Innovations team if you would like to discuss the best approach to the submissions process.

The Proposed CCPA Regulations

While the regulations provide some clarity and give additional color to the verification obligations and placement of the do-not-sell button, they create additional ambiguity in a number of areas and impose

on businesses new requirements that do not exist in the CCPA. That said, they are the clearest indication of what the Attorney General will be looking for in July when the enforcement period begins and he starts to evaluate whether or not companies are in compliance.

Below we walk you through the key provisions of the regulations. Final comments are due on **Dec. 6**, and a series of public forums will be held that week to allow comments to be delivered in person. We encourage all companies to read these regulations closely to understand the impact on your business. We hope a robust comment period will help push these regulations to a form that gives businesses the guidance needed to comply with the CCPA.

Notice Requirements

Notice of Information Collection

- The regulations suggest businesses must provide consumers with a notice, separate from their full privacy policy, at or before the time of collection. Online, this means the homepage of a website or the mobile application download or landing page. Offline, the regulations envision a printed notice or signage. Online notices can link to the relevant section of the full privacy policy (rather than requiring a separate landing page), but the regulations suggest the link must be separate from the link to the full notice.
- The notice must disclose the categories of information to be collected and **for each category**, and the purposes for which that information will be used. The notice must also contain a link to the "Do Not Sell My Personal Info" page and the full privacy policy.
- Notably, businesses that do not collect information directly from consumers do not have to provide a notice at the point of collection; but before the data can be sold, the business must contact the consumer directly and provide a notice of the right to opt out, or they must contact the source of the data to confirm that notice was provided, and obtain a signed attestation describing the notice and an example of the notice. The attestations must be retained for two years and be provided to consumers upon request (it's unclear whether this right has to be disclosed to the consumer).

Notice of the Right to Opt Out of a Sale of Personal Information

- For businesses that sell information, the "Do Not Sell My Information" link must take the consumer to a page that includes the following information: 1) a description of the right to opt out of a sale of personal information, 2) a webform through which the consumer can submit a request (or an offline method for offline companies), 3) instructions for any other opt-out methods, 4) proof required when an authorized agent is used for the request and 5) a link to the privacy policy. This information can be provided by linking to the relevant section of the privacy policy rather than having a separate notice.
- Companies that do not and will not sell personal information do not have to provide the link, but they must state in their privacy policy that they do not and will not sell information. Information collected while this notice is up must not be sold.
- The regulations have a placeholder indicating that they are developing an opt-out logo, but the logo is in addition to, not in lieu of, the do-not-sell link, begging the question of what purpose it would serve. It's hard to understand why a business would add another task to its development list unless it would replace the do-not-sell link.

Notice of Financial Incentives

- A business that plans to offer a financial incentive to induce consumers not to opt out of sales must include a summary of services offered; the material terms, including the categories of personal

information implicated; and a mechanism to opt out of the incentive and a notification of the right to withdraw.

- Businesses must also disclose a good-faith estimate of the value of the consumer's data to the business and a description of the methods used to calculate that value.

Privacy Policy Requirements

A CCPA-compliant privacy policy must include the following:

- A list of the CCPA consumer privacy rights: the right to request that the business disclose what personal information it collects, uses, discloses and sells; the right to request deletion; the right to opt out of a sale of personal information; and the right to nondiscrimination for exercising consumer privacy rights.
- Instructions for submitting a verifiable consumer request and a description of the process used to verify requests.
- The categories of personal information collected about consumers in the previous 12 months (this is for all consumers, not specific to one consumer) and for each category of information: 1) the categories of sources from which that information was collected, 2) the business and commercial purposes for which it was collected, and 3) the categories of third parties it is shared with.
- Explanation of how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.
- Metrics about the number of requests received in the previous year, including the median response time.
- Contact information.
- Date of the privacy policy.

Verification of Consumer Requests

Businesses need to have a reasonable method to verify that the person making a request matches the consumer whose information was collected, taking into consideration the sensitivity and value of the information and the risk of fraud.

Notably, the Attorney General clarified that sensitive information, such as financial account numbers, government identification numbers, Social Security numbers, driver's license numbers, medical and insurance information, passwords, and security questions cannot be disclosed in connection with requests for specific pieces of information. This will be helpful to those companies concerned that a false verification request could put it in the crosshairs of certain state security breach notification laws.

Opt-outs do not require verification. With requests to delete that cannot be verified, the information will not be deleted, but rather the request will be treated as an opt-out. A business can deny the request only if it has a good-faith, reasonable and documented belief that the request is fraudulent.

With a request to opt out or delete, a business may give the consumer a choice to opt out or delete only portions of personal information, but only if a global option is given and is more prominently displayed.

Verification for Password-Protected Accounts

Where a consumer has a password-protected account with the business, the business may use the authentication process for the account to verify the consumer's identity.

Verification for Non-Account Holders

If a consumer does not have a password-protected account with the business, the regulations provide this guidance:

- Where categories of personal information are requested, the consumer's identity must be verified to a **reasonable degree of certainty**. This may include matching at **least two data points** from the consumer with data points in the information maintained by the business.
- Where specific pieces of information are requested, the consumer's identity must be verified to a **reasonably high degree of certainty**. This may include matching **at least three data points** and a signed declaration from the consumer stating that the requestor is the consumer. These declarations must be kept by the business.
- Verify the identity of the consumer to a reasonable or a reasonably high degree of certainty for a request to delete information. The more sensitive the information and the greater the risk to the consumer that deleting the information creates, the higher the degree of certainty needed.

If a business is unable to reasonably verify the consumer's identity to the degree of certainty required, it must say so in its response to the request. If this is the case for all personal information maintained by the business, it must state this in the privacy policy.

The business must also explain why it has no way to reasonably verify the requestor's identity and evaluate yearly whether it can establish such a method for verification.

Record-Keeping Obligations

In addition to requiring companies to retain signed declarations of identity received in connection with verification of consumer requests and signed attestations demonstrating that explicit notice and an option to opt out were presented to the consumer (for third parties that sell personal information), businesses must also generate and retain metrics on how they value consumer data (when financial incentives are offered). Businesses must maintain (for 24 months) records of consumer requests made pursuant to the CCPA and detail on how the business responded to said requests. Businesses that touch the personal information of more than 4 million consumers must compile metrics of the consumer requests they have received, including the median time it took the business to respond. This information must be included in the privacy policy.

We wanted guidance, but — as usual — be careful what you ask for.

Related Professionals

For more information, please contact:

Jessica Lee jblee@loeb.com

6091 REV1 10.28.2019