CLIENT ALERT

Proposed CCPA Regulations from California Attorney General: Part II -- An Analysis of Handling Consumer Requests under the CCPA

Oct.18.2019

On October 10, 2019, California Attorney General Xavier Becerra announced a long-awaited notice of proposed rulemaking and draft regulations for the California Consumer Privacy Act (CCPA), California's new consumer privacy law, which we have analyzed here and here.

In part one of our multi-part series regarding the draft CCPA regulations, we focused on businesses' notice obligations. In this second part of our series, we focus on businesses' obligations to respond to consumer requests. As discussed below, the draft CCPA regulations provide detailed guidance that will have important ramifications for businesses that control or process information about California consumers, particularly in light of CCPA's broad definition of personal information.

Before these proposed CCPA regulations are approved and implemented, interested parties have until December 6, 2019, to submit written comments regarding the draft regulations and to participate in town hall meetings hosted by the Attorney General's Office in Sacramento, San Francisco, Los Angeles, and Fresno. Any businesses impacted by the CCPA should carefully consider whether submitting comments or requested amendments are appropriate.

Representatives of the Attorney General's office have indicated that July 1, 2020 is the anticipated date for CCPA enforcement to begin, but reiterated that CCPA takes effect on January 1, 2020, which means that class action exposure and other provisions apply as of that date.

ARTICLE 3: PRACTICES FOR HANDLING CONSUMER REQUESTS UNDER CCPA:

The proposed regulations provide guidance about how businesses must handle consumer requests, including the following:

- Requests to know what personal information is collected about the consumer;
- Requests by consumers to delete their personal information;
- Requests to opt-out of the business' sale of the consumer's personal information;
- Requests to opt-in to the sale of personal information after opting out; and
- Requests to access or delete household information.

These requirements impose additional obligations on businesses, and if a business is covered by the CCPA, it is possible the more onerous provisions of the CCPA may supersede existing California law (such as California Civil Code Section 1798.83, "Shine The Light" law) regarding required disclosures in privacy notices informing users of their ability to request information about sharing personal information with third parties for marketing purposes.

The proposed regulations impose a number of specific requirements regarding consumer requests, which we outline below.

Methods of Submitting Consumer Requests

Businesses must provide two or more methods for consumers to submit **requests to know what personal information has been collected about the consumer** including: (1) at a minimum, a toll-free telephone number; and (2) at least one additional method such as an interactive webform accessible through the business' website or mobile application, a designated email address, a form submitted in person, or a form submitted by mail. Section 999.312(a).

Similarly, businesses must provide two or more methods for consumers to submit **requests to delete personal information collected**, including but not limited to a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail. Section 999.312(b).

The proposed regulations make clear that, to facilitate consumer submission of requests, the business must provide a method for consumers to submit requests that is consistent with how the business typically interacts with its consumers. "At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know." Section 999.312(c). As a result, some businesses will not be able to rely solely on accepting consumer requests by telephone and online. The regulations give a brick-and-mortar retailer as an example of a business that *cannot rely* on an online form and telephone number alone, but must also accept forms in person at retail locations.

For businesses that do not interact directly with consumers, at least one method for submitting requests to know or to delete must be online. Section 999.312(e).

While businesses are only required to respond to "verifiable" requests, which we will address in our next installment of this series of CCPA client alerts, businesses must treat consumer requests that are submitted outside of the designated methods "as if they had been submitted in accordance with the designated manner" or "provide the consumer with specific directions on how to submit the request or remedy any deficiencies." Section 999.312(f).

Time for Responding to Consumer Requests

Businesses are required to **confirm** the receipt of requests to know and requests to delete within **10 days**. Unless the confirmation states that the request has been granted or denied outright, the confirmation must also describe the business' verification process and inform the consumer when to expect a response. Section 999.313(a).

Businesses have **45 days** from the date they receive a request to know or a request to delete to either **respond** to the request or to notify the consumer that the 45-day period will be extended for up to another 45 days (90 days total), with an explanation of why the additional time is necessary. Section 999.313(b).

Responding to Requests to Know

- **Requests to know** cover the 12-month period prior to the date the request is received, unless otherwise specified.
- **Requests to know the categories of personal information collected, shared, and/or sold** –Businesses must tailor their response to the information that the business actually has about the requesting individual. Businesses cannot simply describe general categories based on their general policies and practices, *unless* the response would be the same for all

consumers who submit a similar request *and* the public privacy statement discloses all information that would be otherwise required**.** Section 999.313(c)(9).

- **Requests to know specific items of personal information** rather than categories carry a few additional requirements–
    - Businesses cannot provide a consumer's Social Security number, driver's license number or other government issued identification number, financial account number, account password, or security questions and answers. Section 999.313(c)(4).
    - To the extent that a request to know a specific item is completely or partially denied (see below), the business must treat it as a request to know categories of personal information and respond accordingly. Section 999.313(c)(1).
- Businesses must use "reasonable security practices and procedures," terms not specifically defined in the proposed regulations, when transmitting personal information to the consumer. Section 999.313(c)(6).

Responding to Requests to Delete

- **Online requests to delete require a two-step process.** The consumer first initiates the request, and then separately confirms (e.g., via follow-up email with "confirm" link or similar separate communication from the business) that they want their personal information deleted. Section 999.312(d).
- Granting a request to delete means that a business has "permanently and completely" erased the personal information from existing systems, and the response must describe how deletion has been accomplished and state that a record of the request to delete will be retained.
    - Note that activities that de-identify or aggregate the personal information satisfy the deletion requirements**.** Section 999.313(d)(2).
    - For personal information on archived or backup systems, deletion may be delayed until it is next accessed or used. Section 999.313(d)(3). *As a risk management matter, care must be taken not to repopulate other business or third party systems with "to be deleted" data when those archived or backup systems are accessed.*
- Businesses may only offer an option to delete portions of a consumer's information in response to a deletion request if a global option to delete all personal information is also offered, and offered more prominently. Section 999.313(d)(7).
- If a business cannot verify the identity of the requestor, the business may deny the request to delete and instead treat the request as one to opt-out of the sale of personal information. Section 999.313(d)(1). This is discussed further below.

Responding to Requests to Opt-Out

- A business must provide two or more designated methods for submitting requests to opt-out of the sale of personal information, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business' website or mobile application. Section 999.315(a).
    - Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin, privacy setting, or other mechanism that communicates or signals the consumer's choice to opt-out of the sale of their personal information.

- If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, including via browser plugins or signals, as a valid request to opt-out for that browser or device, or, if known, for the consumer. Section 999.315(c). *As a risk management matter, note that this requirement is potentially at odds with the currently popular practice of **not** honoring "Do Not Track" signals and so stating in privacy statements. CCPA does not identify any applicable standards or limits with regard to opt-out signals that must be detected and honored, and we expect comments on the draft regulations to seek further clarification or to modify this requirement.*
- Businesses must act on opt-out requests "as soon as feasibly possible" but no later than **15 days** after receipt. This includes notifying all third parties to whom information was sold within 90 days prior that the consumer has exercised the opt-out right, and subsequently informing the consumer that third-party notification of the opt-out has been completed. Section 999.315(e)-(f).
- Opt-out requests may be submitted by a consumer's authorized agent, if the agent has written permission from the consumer. Section 999.315(g).
- Requests to opt-out **need not be a verifiable consumer request.** Businesses may only refuse based on a reasonable, good-faith, and documented belief that an opt-out request is fraudulent, and if so must inform the requesting party of the refusal and explain why it believes the request to be fraudulent. Section 999.315(h).

Responding to Requests to Opt-In After Opting-Out:

- If a consumer has previously opted-out of the sale of their personal information, businesses must use a two-step process to subsequently opt in, where the first step is the consumer's request to opt-in and the second step confirms the consumer's choice to do so. Section 999.316(a).
- A business may inform a consumer who has opts-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in to complete the transaction. Section 999.316(b).

Responding to Requests regarding Household Data:

- If a consumer does not have a password-protected account with a business, a business may respond to a request to know or a request to delete household information by providing "aggregate" household information. Section 999.318(a).
- A joint request for access or deletion of household data by all members of a household must only be complied with if a business can individually verify all members of the household. Section 999.316(b).

This type of request was suggested in the text of the CCPA, in which the definition of personal information includes "households," but it has only been addressed specifically in the proposed regulations. One key remaining issue is whether a business processing household data has an obligation to affirmatively inform a requesting consumer of the identity of any other individuals in a given household (whose information may be required for verification purposes to obtain access to household data).

Responding to Requests with Complete or Partial Denials

A business may deny a consumer's request to know or request to delete when it is unable to verify the identity of the requestor. If a request is denied because the requestor's identity cannot be verified, the consumer should be informed of as much. Section 999.313(c)(1)-(2).

- Requests to know specific items of information can be denied if disclosure **creates a substantial, articulable, and unreasonable risk** to the security of either the personal information, the consumer's account with the business, or the security of the business systems and networks. Section 999.313(c)(3).
- Businesses that deny requests must usually inform consumers of the reasons for denial. Section 999.313(c)(5).
- For requests that are only partially denied, the response must provide the remaining requested information. Section 999.313(c)(5).

Training and Record-Keeping

- All individual staff members responsible for handling consumer inquiries about privacy practices, **or a business' compliance with the CCPA,** shall be informed of all the requirements of the CCPA and these regulations. Section 999.317(a).
- Businesses must maintain records of requests received and the response given for at least 24 months. Section 999.317(b). Records of requests can be maintained in log format, if they show the:
    - Date of the request;
    - Nature of the request;
    - Manner in which the request was made;
    - Date of the response;
    - Nature of the response, and
    - Basis for denial, if the request was denied in whole or in part.
- A business that "alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, the personal information of **4,000,000 or more**" California consumers must:
    - Track and post either in their privacy policy directly or accessible from a link the number of requests to know, requests to delete, and requests to opt-out received in the previous calendar year, and the median number of days it took to respond.
    - Establish, document, and comply with training policies to ensure that all individuals responsible for handling consumer requests or the business' compliance with the CCPA are informed of all the requirements in the CCPA and the proposed regulations. Section 999.317(g).

* * *

In addition to detailing how businesses should handle consumer requests, this section of the Article 3 of the proposed regulations includes some new and updated information at Section 999.314 regarding the role of "service providers" under the CCPA, which we will cover in a subsequent analysis.

In the next installment of our series, we will provide additional analysis of Article 4, which addresses the issue of "verification."

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeane A. Thomas, CIPP/E
Partner – Washington, D.C., Brussels
Phone: +1 202.624.2877, +32.2.282.4082
Email: jthomas@crowell.com

Paul M. Rosen
Partner – Los Angeles, Washington, D.C.
Phone: +1 213.443.5577, +1 202.624.2500
Email: prosen@crowell.com

Kristin J. Madigan, CIPP/US
Partner – San Francisco
Phone: +1 415.365.7233
Email: kmadigan@crowell.com