TRAUB LIEBERMAN

CYBER LAW BLOG

November 26, 2019

A Look at California's Draft Regulations Under the CCPA

BY: Jason Taylor

The California Consumer Privacy Act ("CCPA") was enacted in 2018 and takes effect on January 1, 2020. This landmark piece of legislation secures new privacy rights for California consumers. Among other things, the CCPA creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. It also requires the Attorney General to solicit broad public participation and adopt regulations to further the CCPA's purposes. On October 10, 2019, California Attorney General Xavier Becerra released draft regulations under the CCPA for public comment. The proposed regulations would establish procedures to facilitate consumers' new rights under the CCPA and provide guidance and clarity to businesses for how to comply.

In general, the CCPA applies to a "business" that does business in the State of California, collects personal information (or on behalf of which such information is collected), alone or jointly with others determines the purposes or means of processing of that data, *and* satisfies one or more of the following thresholds: (i) annual gross revenue in excess of $25 million; (ii) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (iii) derives 50 percent or more of its annual revenues from selling consumers' personal information. According to estimates, the CCPA will protect over $12 billion worth of personal information that is used for advertising in California each year. Preliminary estimates suggest a total of $467 million to $1.6 billion in costs to comply with the draft regulations, if finalized, during the period 2020-2030.

The proposed regulations are intended to operationalize the CCPA and provide clarity and specificity to assist in the implementation of the law. The draft regulations specifically address Notices to Consumers, Business Practices for Handling Consumer Requests, Verification of Requests, Special Rules Regarding Minors, and Non-Discrimination. Below is a summary highlighting some of the more significant aspects of the proposed regulations.

NOTICES AT COLLECTION OF PERSONAL INFORMATION

The CCPA requires that businesses give "notice at collection" to a consumer at or before the time a business collects personal information from the consumer. The purpose of the notice at collection is to inform consumers of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used. The notice at collection must be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer, including those with disabilities, use plain, straightforward language, and avoid technical or legal jargon. Importantly, the notice at collection must be visible or accessible where consumers will see it before any personal information is collected.

The proposed regulations provide that a business must include the following in its notice at collection:

- A list of the categories of personal information about consumers to be collected. Each category of personal information must be written in a manner that provides consumers with a meaningful understanding of the information being collected;

- For each category of personal information, the business or commercial purpose(s) for which it will be used;
- If the business sells personal information, a link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info,” or, in the case of offline notices, the web address for the webpage to which it links; and
- A link to the business’s privacy policy, or, in the case of offline notices, the web address of the business’s privacy policy.

A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer. If, however, the business later decides to sell a consumer’s personal information, it must either (a) contact the consumer directly to notify him or her that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out, or (b) contact the source of the personal information to confirm that the source provided a notice at collection to the consumer and obtain signed attestations from the source describing how it gave the notice at collection, with an example of the notice. Attestations must be retained by the business for at least two years and made available to the consumer upon request.

NOTICE OF RIGHT TO OPT-OUT OF SALE OF PERSONAL INFORMATION

The notice of right to opt-out of sale of personal information informs consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop and refrain from doing so in the future. As with other notices, the notice of right to opt-out must be designed and presented in a way that is easy to read and understandable to an average consumer.

A business that sells personal information must provide a notice of right to opt-out to the consumer by posting the notice of right to opt-out on the webpage where the consumer is directed after clicking on the “Do Not Sell My Personal Information” or “Do Not Sell My Info” link on the business’s website or mobile application.

Specifically, the website or app must include:

- A description of the consumer’s right to opt-out of the sale of their personal information by the business;
- The webform by which the consumer can submit their request to opt-out online, or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;
- Instructions for any other method by which the consumer may submit their request to opt-out;
- Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, or in the case of a printed form containing the notice, a webpage, online location, or URL where consumers can find information about authorized agents; and
- A link or the URL to the business’s privacy policy, or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy. A business may use an opt-out “button” or logo, in addition to posting the notice of right to opt-out, that links to a webpage or online location containing the required opt-out information, or to the section of the business’s privacy policy containing the same information.

A business that substantially interacts with consumers offline or does not operate a website must also provide notice to the consumer by an offline method to facilitate consumer awareness of the consumer’s right to opt-out, and establish, document, and inform consumers of their right to direct a business that sells their personal information to stop selling their personal information.

NOTICE OF FINANCIAL INCENTIVE

The CCPA and proposed regulations require businesses to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the retention or sale of the consumer's personal information so that the consumer can make an informed decision on whether to participate.

Under the proposed regulations, regulated entities must include the following in their notices of financial incentive:

- A succinct summary of the financial incentive or price or service difference offered;
- A description of the material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference;
- How the consumer can opt-in to the financial incentive or price or service difference;
- Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data.

PRIVACY POLICY

The proposed regulations set forth the scope of what is required in a business' privacy policy and how that policy must be made available to consumers. Generally, the proposed regulations require that the privacy policy include a "right to know" about the personal information collected, disclosed, or sold; right to request deletion of personal information; right to opt-out of the sale of personal information; the right to non-discrimination for the exercise of a consumer's privacy rights; and provide consumers with a contact for questions or concerns about the business's privacy policies and practices. The privacy policy must explain these rights to consumers and provide instructions or describe the process for how to exercise these rights.

BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

The proposed regulations also provide for the methods required for submitting requests to know and requests to delete personal information, as well as how a business must respond to such requests.

For example,

- Upon receiving a request to know or a request to delete, a business must confirm receipt of the request within 10 days and provide information about how the business will process the request. The information provided must describe the business's verification process and when the consumer should expect a response. A business generally must respond to the request within 45 days.
- A business must provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application;
- The business also must provide two or more designated methods for submitting requests to delete;

- At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires the business to offer three methods for submitting requests to know;
- A business must also provide two or more designated methods for submitting requests to opt-out, 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’s website or mobile application;
- A business shall use a two-step process for online requests to delete where the consumer must, first, clearly submit the request to delete, and then, second, separately confirm that they want their personal information deleted;
- For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request, the business cannot disclose any specific pieces of personal information to the requestor and must inform the consumer that it cannot verify their identity;
- For requests that seek the disclosure of *categories* of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity;
- The proposed regulations prohibit a business, at any time, from disclosing a consumer’s Social Security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers;
- In responding to a consumer’s verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business must provide an individualized response to the consumer as required by the CCPA. Merely referring the consumer to the business’s general practices outlined in its privacy policy is generally not permitted, unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories;
- For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business must inform the requestor that their identity cannot be verified and instead treat the request as a request to opt-out of sale;
- To comply with a consumer’s request to delete their personal information, the business must permanently and completely erase the personal information on its existing systems (with an exception for archived or back-up systems); de-identify the personal information, or aggregate the personal information;
- In its response to a consumer’s request to delete, the business must also specify the manner in which it has deleted the personal information;
- In cases where a business denies a consumer’s request to delete the business must inform the consumer, describe the basis for the denial, including any statutory and regulatory exception therefor; delete the consumer’s personal information that is not subject to the exception; and not use the consumer’s personal information retained for any other purpose than provided for by that exception.

TRAINING AND RECORDKEEPING

The proposed regulations also set forth training and record-keeping requirements for businesses.

For example, the proposed regulations mandate that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA must be informed of all the requirements in the CCPA and its regulations, and how to direct consumers to exercise their rights under the CCPA and regulations. The proposed regulations also include guidance on how businesses verify requests from consumers and require that businesses maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months. The regulations include additional obligations for businesses buying, receiving, sharing, or selling personal information of 4,000,000 or more consumers, and requirements for collecting or maintaining information of minors.

The draft regulations are open for public comment until December 6, 2019. California's Attorney General will consider all comments and may revise the regulations in response, which will open up an additional public comment period. Following the comment period, the Attorney General will submit the final text of the regulations, a final "Statement of Reasons", responding to every comment submitted, and an updated informative digest to the Office of Administrative Law to review the regulations for approval.