COVINGTON

California Attorney General Releases Draft CCPA Regulations

October 11, 2019

Data Privacy and Cybersecurity

On October 10, 2019, California state attorney general Xavier Becerra announced the release of proposed implementing regulations concerning the California Consumer Privacy Act (CCPA). Interested stakeholders can submit written comments until December 6, 2019 at 5 PM (Pacific Time). In addition, four public hearings will be held on December 2nd (Sacramento), December 3rd (Los Angeles), December 4th (San Francisco) and December 5th (Fresno).

The draft regulations address five main areas: (1) Notice to Consumers; (2) Business Practices for Handling Consumer Requests; (3) Verification of Requests; (4) Special Rules Regarding Minors; and (5) Non-Discrimination.[1]

Notice to Consumers: The draft regulations provide various requirements for complying with the CCPA statute's notice provisions. For example:

- Privacy Policies (§ 999.308): The draft regulations contain additional elements that must be included in businesses' privacy policies. Specifically, for *each* category of information collected, policies must provide (i) the business or commercial purpose(s) for which the information was collected; (ii) the categories of sources from which the information was collected; and (iii) the categories of third parties with whom the business shares personal information. Policies must also include instructions for submitting verifiable consumer requests (and for doing so through an authorized agent), as well as a description of the business' process for verifying consumer requests (including what information consumers must provide).
- Notice of the Right to Opt-Out (§ 999.306): Under the proposed regulations, businesses that sell consumer information must provide a "Do Not Sell My Personal Information" (or "Do Not Sell My Info") link that takes consumers to a webpage (or link to the privacy policy) that provides a description of the consumer's right to opt-out, the webform by which consumers can submit their requests, and any proof required when a consumer uses an authorized agent to exercise their right to opt-out. Notably, the draft regulations do not provide requirements for the actual "Do Not Sell" button or logo (but commit to doing so at a later date, which may result in an extension of the notice and comment period). Businesses are exempt from having to provide a notice of the right to opt out if (i) they do not sell consumer data when the notice is not posted; *and* (ii) their privacy statement states that the business "does not and will not sell personal information."

[1] The regulations remain in draft form, and there are elements of the draft that add new obligations to the statute or are in tension with the plain language of the statute.

- Third-Party Accountability (§ 999.305(d)): Businesses that do not obtain personal information from consumers directly may now be responsible for ensuring that appropriate notice was provided from the source of data before they can sell the information. The draft regulations provide that, before selling, such businesses must either (i) contact the consumer directly in order to inform them that they sell data and notify them of their right to opt out; or (ii) contact the source from which they obtained the personal information to confirm that the source provided the consumer with appropriate notice and obtain signed attestations describing how notice was given at the point of collection (including an example of the notice provided).

Business Practices for Handling Consumer Requests: The draft regulations contain several requirements for receiving and responding to consumer requests to exercise their rights under the CCPA. Notable provisions include:

- Ways to Submit Requests for Access/Deletion (§§ 999.312, 999.318): The draft regulations detail the mechanisms that businesses must provide consumers in order to submit requests to access or delete their data. Notably, the draft regulations provide that a business must, in choosing which mechanisms to use, consider the methods by which it primarily interacts with consumers, and explains that in some cases businesses may have to provide three methods for submitting requests. As an illustrative example, the draft regulations provide that if a business operates a website but primarily interfaces with consumers in-person through a retail store, that business must provide (i) the required toll-free number; (ii) the required interactive webform accessible through the website; and (iii) a form that can be submitted in person at the retail location. The draft regulations also provide some clarity with respect to how requests from "households" are to be treated.
- Responding to Requests for Access/Deletion (§ 999.313): The draft regulations set forth the time frames by which businesses must respond to requests for access or deletion. Specifically, responses must be sent within 45 days from which the request was received, with an option to take up to an additional 45 days (for a maximum total of 90 days). In addition, the draft regulations detail various scenarios in which a business *need not* comply with a consumer's request to access their data. For example, if a business cannot verify the identity of the consumer making a request for disclosure of specific pieces of their information, the draft regulations provide that the business must deny that consumer's request and inform them of the reason for doing so (it may, but is not required, to deny requests for categories of personal information and requests to delete personal information for the same reason). Moreover, the draft regulations prohibit businesses from disclosing specific pieces of personal information if doing so would create a "substantial, articulable, and unreasonable risk" to the security of that information, the consumer's account with the business, or the business's systems or networks. In addition, specific pieces of information may *never* be disclosed in response to a request for access—such as Social Security numbers, driver's license numbers, financial account numbers, or security questions and answers.
- The draft regulations also provide a few options for complying with requests to delete information: in addition to "permanently and completely erasing" the information, the draft regulations also permit the business to instead de-identify the personal information or aggregate it.
- Complying with Right to Opt-Out (§ 999.315): Businesses are required to provide two or more designated methods for submitting requests to opt-out of the sale of personal

information. In addition to a "Do Not Sell My Personal Information" link, there are a variety of other acceptable methods provided by the draft regulations, including "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out." Notably, businesses also would be required to notify all third parties to which they have sold personal information within 90 days prior to receipt of the opt-out request and instruct those third parties to not further sell the information.

- Recordkeeping Requirements (§ 999.317): Businesses would be required to maintain various records of the requests they receive from consumers, as well as how they responded to each of those requests. In addition, businesses that use, sell, or share personal information of 4 million or more consumers for commercial purposes must provide in their privacy policies a variety of metrics regarding their receipt and responses to consumer requests for the previous calendar year.
- Service Providers (§ 999.314): The draft regulations state that service providers are prohibited from using personal information received for the purpose of providing services to a different person or entity. However, service providers may combine personal information received from one or more entities to which it is a service provider to the extent necessary to protect against fraudulent or illegal activity.

Verification: Consistent with § 1798.185(a)(7), the Attorney General's regulations also address verification of consumer requests:

- General Verification Methods (§ 999.323): The draft regulations are not overly prescriptive regarding how to verify requests. Instead, the draft regulations require businesses (or their third-party identity verification services) to match identifying information provided by the consumer to the personal information the business maintains, where feasible. Businesses can collect the personal information identified in California's data security law (Cal. Civ. Code § 1798.81.5(d)) for verification, but only if necessary. In addition, the draft regulations identify a series of factors to consider in developing its verification method (including the sensitivity of the information relevant to the request and the risk of harm).
- Account vs. Non-Account Verification (§§ 999.324, 999.325): The draft regulations provide different guidelines for verifying consumer identities based on whether the consumer has a password-protected account with the business. Notably, if the consumer does not maintain a password-protected account with the business, the draft regulations provide two levels of certainty that the business must arrive at with respect to the consumer's identity before complying with the consumer's request. These levels hinge on whether the consumer is asking for categories or specific pieces of information (for requests to access) and on the sensitivity of the information at issue (for requests for deletion).

Minors: The Attorney General also proposed regulations regarding how the CCPA applies to minors.

Notably, regardless of whether the business that collects personal information about minors sells the personal information, the following appears to apply:

- Minors Under 13 (§ 999.330): Businesses that actually know that they are collecting minors' information must document and comply with a reasonable method for determining that the person affirmatively authorizing the sale about the younger-than-13-year-old child is, in fact, that child's parent or guardian. The regulation also provides a

list of acceptable methods for making this determination, and provides that the method selected must be *in addition to* any verifiable consent required by the Children's Online Privacy Protection Act (COPPA).

- Minors 13 to 16 Years Old (§ 999.331): A business that has actual knowledge that they are collecting personal information from individuals between 13-16 years old must document a reasonable process by which such minors can opt-in to the sale of their personal information, which must be done via the two-step opt-in process described above.

Non-Discrimination: The draft regulations essentially reiterate the substance of several statutory provisions surrounding consumers' non-discrimination right.

- Calculating the Value of Consumer Data (§ 999.337): The draft regulations provide further clarity regarding how businesses must calculate the value of the consumer's data. Businesses would have eight methods to choose from: (1) the marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (2) the average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data; (3) revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value; (4) revenue generated by the business from sale, collection, or retention of consumers' personal information; (5) expenses related to the sale, collection, or retention of consumers' personal information; (6) expenses related to the offer, provision, or imposition of any financial incentive or price or service difference; (7) profit generated by the business from sale, collection, or retention of consumers' personal information; and (8) any other practical and reliable method of calculation used in good-faith.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Libbie Canter	+1 202 662 5228	ecanter@cov.com
Yaron Dori	+1 202 662 5444	ydori@cov.com
Jadzia Pierce	+1 202 662 5942	jpierce@cov.com
Alex Scott	+1 650 632 4743	ajscott@cov.com
Lindsey Tonsager	+1 415 591 7061	ltonsager@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com