DrinkerBiddle

Privacy Alert

October 2019

CCPA Amendments & Proposed Implementing Regulations

By Peter Blenkinsop | peter.blenkinsop@dbr.com | +1 202-230-5142

On October 10, California Attorney General Xavier Becerra released long-awaited proposed regulations to implement the CCPA. Public comments on the proposed regulations are due by December 6. Just one day later, on October 11, California Governor Gavin Newsom signed amendments to the CCPA that passed the legislature last month. This Privacy Alert serves to summarize these developments.

I. Legislative Amendments to the CCPA

Five bills amending the CCPA, and one related bill creating new obligations for data brokers, have now been signed into law. They are: AB 25 (Chau), AB 874 (Irwin), AB 1146 (Berman), AB 1202 (Chau), AB 1355 (Chau), and AB 1564 (Berman). The amendments make the following changes to the law, amongst others:

- Personal information collected about an employee, job applicant, or contractor, as well as employee emergency contact information and information collected for administration of an employee benefits program, is now exempt through January 2021 from many aspects of the CCPA. Specifically, CCPA rights of access and deletion, and the right to opt out of the sale of personal information, will not apply in these contexts. (Employee rights under other California laws to inspect personnel files and payroll records are unaffected.) However, the CCPA right to a notice at or before the point of data collection will still apply, as will the right to bring an action for statutory damages in the event of a data breach.
- Personal information collected about an individual in the course of certain business-to-business ("B2B") contacts will be exempt through January 2021 from many aspects of the CCPA. The exemption applies to "personal information reflecting a written or verbal communication or a transaction between the business and the [individual]" where that communication or transaction occurs "within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from [the other business]." CCPA rights of notice, access, and deletion will not apply in this context; however, the right to opt out of the sale of personal information will still apply, as will the private right of action in the event of a data breach.
- The CCPA now expressly states that it "shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business [or] retain personal information for longer than it would otherwise retain such information in

the ordinary course of its business." Thus, businesses that collect only pseudonymized or indirectly identifiable information will not be required to obtain additional information for purposes of responding to data subjects' rights requests.

- The definition of "personal information" has been modified to more clearly exclude information lawfully made available from federal, state, or local government records ("publicly available information"). Another change adds "reasonably," as follows, to one part of the "personal information" definition, although it is less clear what the ultimate impact of this change will be: " 'Personal information' means information that identifies, relates to, describes, is **reasonably** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- Certain sector-specific exemptions have been added or broadened. In particular, the CCPA now excludes from its scope (except for the private right of action in relation to data breaches) "an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" by a consumer reporting agency, by a furnisher of information for use in a consumer report, or by a user of a consumer report, to the extent such activity is already regulated under the Fair Credit Reporting Act (FCRA). In addition, the CCPA right to opt out of the sale of personal information no longer applies to vehicle or ownership information shared between a vehicle manufacturer and dealer for purposes of vehicle warranty or recall.

A number of other changes clarify aspects of the CCPA or fix drafting errors.

In addition to the above amendments to the CCPA, AB 1202 creates a new requirement that data brokers register with the California Attorney General. A "data broker" is defined as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." As explained in the legislative findings, the bill is not intended to apply to businesses with whom consumers have a direct relationship. This direct relationship may have been formed in a variety of ways, including but not limited to a consumer visiting a business' premises or internet website, or a consumer's intentional interaction with a business' online advertisements.

II. CCPA Proposed Regulations

The California AG's proposed regulations cover six topics: (A) the notices that business must provide to individuals; (B) practices for handling consumer requests for information and/or for deletion, including practices for verifying the identity of individuals making requests; (C) practices for handling consumer requests to opt-out of the sale of their personal information; (D) practices for handling personal information of minors; (E) service providers; and (F) recordkeeping. Notably, the regulations provide no further guidance on the scope of the definition of "personal information," acceptable methods for the de-identification of information, the scope of the definition of the "sale" of personal information, or the scope of the various CCPA exemptions.

A. CCPA Notices

The regulations address four notices required under the CCPA: (i) notice at or before collection of personal information; (ii) notice of the right to opt-out of the sale of personal information; (iii) notice of financial incentives; and (iv) the privacy policy. These notices must be designed and presented in a way that is easy to read and understandable to the average consumer, including through the use of plain, straightforward language, in a format that draws consumers' attention to the notice, in languages in which the business ordinarily interacts with consumers, and they must be accessible to consumers with disabilities.

i. Notice at Collection

A business that collects information directly from consumers must provide a notice at the point of collection. The notice at collection must be accessible where consumers will see it before personal information is collected. This can include through the use of online links to the notice on web pages where personal information is collected, inclusion of the notice on printed forms where personal information is collected, and in-store signage that directs consumers to the web address of the notice. The notice must identify each category of personal information to be collected "in a manner that provides consumers a meaningful understanding of the information being collected." *For each category*, the business must identify the purposes for which the information will be used. A business is not permitted to use a consumer's personal information for any purpose other than those disclosed in the notice at collection unless it obtains the explicit consent of the consumer for the new purpose.

The notice must also include a link to the business's notice of the right to opt-out of the sale of personal information (to be titled "Do Not Sell My Personal Information" or "Do Not Sell My Info") if the business sells personal information. Finally, the notice must include a link to the business's privacy policy. For online interactions, instead of including all of this information in a separate notice, it is acceptable for the notice to simply link to a section of the business's privacy policy that contains all of the required information.

ii. Notice of Right to Opt-Out of Sale

A notice of the right to opt-out of the sale of personal information must be provided before a business can sell personal information. This is the notice that links to the "Do Not Sell My Info" link that must be included on the homepage of businesses that sell personal information, as well is in the Notice at Collection of such businesses. It is acceptable for this notice to be contained in a section of the business's privacy policy rather than structured as a separate notice. A business that does not sell personal information is not required to maintain a notice of the right to opt-out, but it must instead state in its privacy policy that it does not and will not sell personal information. Should the business later decide that it wishes to sell personal information, it must change its privacy policy and treat information collected prior to the change as opted out of future sales.

The notice of the right to opt-out must include a webform by which the consumer can submit opt-out requests as well as instructions for any other method by which the consumer can submit opt-out requests. It must also describe any proof that is required when a consumer uses an authorized agent to exercise their right to opt-out. Finally, the notice must contain a link to the business's privacy policy.

iii. Notice of Financial Incentive

A notice of financial incentive is required if a business offers a price or service difference, or some other financial incentive, in exchange for the retention or sale of a consumer's personal information. The notice must include a summary of the incentive offered, as well as a description of the material terms and categories of personal information implicated, how the consumer can opt-in to the incentive, and the right of the consumer to withdraw at any time and how to do so. The notice must include an estimate of the value of the consumer's data that forms the basis for the incentive and a description of the method used by the business to calculate this value. It is acceptable for this notice to be contained in a section of the business's privacy policy rather than structured as a separate notice.

In calculating the value of a consumer's data for the above purposes, a business is permitted to use any reasonable, practical, and reliable method, provided it documents its analysis. This could include, for example, determining the marginal value or the average value of a typical US consumer's data.

iv. Privacy Policy

All businesses are required under the regulations to maintain a privacy policy that comprehensively describes the business's online and offline personal information practices and the CCPA rights of consumers. The privacy policy must be posted online and include the following information:

- A list of the categories of personal information the business has collected about consumers in the preceding 12 months. The list must be written so as to provide consumers with a meaningful understanding of the information collected. *For each category of personal information*, the policy must indicate the categories of sources of the information, the purposes for which the information was collected, and the categories of third parties with whom the information is shared.
- A statement as to whether the business has sold or disclosed personal information to third parties in the preceding 12 months. The policy must list the categories of personal information disclosed or sold (in separate lists, according to the CCPA itself). It must also include a statement that the business does not sell the personal information of minors under age 16 without affirmative authorization.
- An explanation of the consumer's right to request deletion of personal information, as well as instructions for how to do so. The policy must also describe the process the business will use to verify consumer requests for deletion.
- If the business sells personal information, an explanation of the consumer's right to opt-out of the sale of personal information, as well as a link to the notice of the right to opt-out.
- A statement explaining the right of the consumer not to be subject to discrimination for exercising their CCPA rights.
- An explanation of how the consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.
- A contact for questions or concerns about the business's privacy practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- The date the privacy policy was last updated. This date should reflect the CCPA requirement that a business review and update its privacy policy at least once every 12 months.

- If a business annually buys, receives, sells, or shares the personal information of 4 million or more consumers (approximately 10% of the population of California), certain metrics concerning the business's receipt of CCPA requests and its response to those requests must be disclosed. (*See "Recordkeeping," below*.)

B. Practices for Handling Consumer Requests to Know and Requests to Delete

The regulations set forth acceptable methods businesses can provide for consumers to submit requests, how they must respond to requests, and record-keeping requirements. Businesses must designate two or more methods for consumers to submit "requests to know," and requests to delete. At least one of these methods must reflect the manner in which the business primarily interacts with the consumer. Upon receipt of a request, a business must confirm receipt within 10 days and provide information that describes its verification process and when the consumer should expect a response. A business has 45 days to respond, which runs from the date of receipt of the request. If necessary, a business can take up to an additional 45 days, for a total of 90 days from receipt of the request, to provide a response, provided that the business provides the consumer with notice and an explanation for the delay within the initial 45-day period.

If a consumer submits a request in a manner that is different than one of the designated methods, or if the request is deficient in some other way (excluding verification of the requestor's identity), then the business either must treat the request as if it had been submitted through one of the designated methods or it must provide the consumer with directions on how to properly submit the request.

Businesses must establish and document a method for verification of requests to know and requests to delete. The method should involve, whenever feasible, matching the identifying information provided by the consumer to personal information of the consumer already maintained by the business or using a third-party identity verification service. The chosen method should take into account the sensitivity of the information, the risk of harm of unauthorized access or deletion, the likelihood of malicious actors seeking to access or delete the information, and the manner of interaction with the consumer. In general, businesses should avoid requesting additional information from a consumer solely for purposes of verification unless absolutely necessary, in which case the information should be deleted as soon as practical after processing the request. If there is no reasonable method by which a business can verify the identity of consumers making requests according to the standards discussed further below, then the business must explain this in its privacy policy, along with its rationale. This determination must then be re-evaluated on a yearly basis. If a consumer maintains a password-protected account with the business, the business is permitted to use its existing authentication practices for account access as its verification process, although consumers must be required to re-authenticate themselves before a business discloses or deletes their data in response to a request.

The CCPA permits consumers to authorize agents to submit requests to know and requests to delete on their behalf. If a business receives a request from a person or entity purporting to be a consumer's authorized agent, the business is permitted to require proof in the form of a copy of written permission by the consumer authorizing the person/entity to act on their behalf. The business is also permitted to require that the consumer him or herself verify their identity directly with the business.

i. Requests to Know

The CCPA requires that in response to a verified consumer request, a business must provide a consumer with the categories of personal information it has collected about that consumer as well as certain other information, including, upon request, the specific pieces of personal information collected. The regulations state that *for each category of personal information*, the business must identify the categories of sources, the purposes for the collection, the categories of third parties to whom the information has been sold or disclosed, and the purposes for such sales or disclosures. The regulations refer to these requests as "requests to know" and stipulate that responses to requests to know must be individualized unless a response would be the same for all consumers or all consumers in a particular category.

Business must provide both a toll-free telephone number and an interactive webform for consumers to submit requests to know. If a business primarily interacts with some consumers in a different manner, then it must include a method that reflects this method of interaction with such consumers, such as an email address, a form for submission in-person, or a form for submission through the mail.

For requests that seek disclosure of *specific pieces of information* about the consumer, a business must verify the identity of the consumer making the request to a *reasonably high degree of certainty*. This high threshold can be met by, for example, matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that the business has determined to be reliable for identity verification purposes. In addition, the requestor should be asked to submit a declaration under penalty of perjury that he or she is the consumer whose personal information is the subject of the request. If the business cannot verify the identity of the requestor according to these high standards, then the business must deny the request and instead evaluate it as if it were a request for disclosure of the *categories of personal information* that the business has collected about the consumer. The standard for verification of a consumer's identity for purposes of requests to know categories of personal information is a *reasonable degree of certainty*. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business. If the business cannot verify the identity of a requestor to a reasonable degree of certainty, then the business may deny the request in whole or in part and must instead direct the consumer to its privacy policy.

The regulations stipulate that a business shall not provide a consumer with specific pieces of personal information where the disclosure would create a substantial, articulable, and unreasonable risk to the security of the personal information, the consumer's account with the business, or the security of the business's systems or networks. Moreover, they state that a business shall not disclose 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 any security questions and answers in response to a right to know request. These are types of information that may trigger a breach notification requirement under California's breach notification law were they to be acquired by unauthorized persons; notably, however, medical information is not included in the list of restricted disclosures even though it is also a category of information that can trigger breach notification requirements.

When transmitting personal information in response to a request to know, a business must use reasonable security measures. If a business maintains a password-protected account with the consumer, it can comply with a request to know by providing a self-service portal for consumers to access, view, and receive a portable copy of their personal information.

ii. Requests to Delete

A business must provide two or more methods for consumers to submit requests to delete. However, in contrast to the requirements surrounding requests to know, businesses are free to decide what methods to offer, provided that at least one method reflects the manner in which the business primarily interacts with the consumer. Businesses are permitted to offer consumers the choice to delete select portions of their personal information provided that a global option to delete all information is also offered more prominently. The standard for verification of a request to delete may be a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm posed by any unauthorized deletion. Businesses must determine the appropriate standard on a case-by-case basis. If a business cannot verify the identity of a consumer pursuant to the standard determined to be appropriate, the business must instead treat the request as a request to opt-out of sale.

A business can comply with a consumer's request to delete their personal information by permanently erasing the information on its systems, by de-identifying the information, or by aggregating the information. In its response to the consumer, the business must specify the manner in which it has deleted the personal information. It must also explain that it will maintain a record of the request. The regulations provide an exception to the obligation to comply with a deletion request with respect to archived or back-up systems. If one of the statutory exceptions applies to the business's obligation to delete personal information, the business must inform the consumer of the basis for the denial of the request, delete any information that is not subject to the exception, and then limit its use of the remaining personal information to the purposes allowed under the exception.

C. Practices for Handling Consumer Requests to Opt-Out of Sale

A business that sells personal information must provide two or more designated methods for consumers to submit opt-out requests, including, at a minimum, a webform. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. If a business collects personal information from consumers online, the business must treat user-enabled privacy controls, such as browser plugins and privacy settings that communicate or signal a consumer's opt-out choice as to the sale of personal information, as a valid request for that browser or device. A business is permitted to present consumers with the choice to opt-out of the sale of only certain categories of personal information provided that a global opt-out option is presented more prominently.

Requests to opt-out of the sale of personal information are not subject to the CCPA's verification requirements. The proposed regulations permit a business to deny a request to opt-out only where the business has a "good-faith, reasonable, and documented belief" that the request is fraudulent. In such a case, the business must, nevertheless, provide a response to the request with "an explanation why it believes the request is fraudulent." A business must act upon a request to opt-out as soon as feasibly possible, but no later than 15 days from receipt of the request. If the business has sold the personal

information of the consumer within 90 days prior to receipt of the request, the business must notify the third-party recipients and instruct them not to further sell the information.

A business must accept requests from a consumer's authorized agent to opt-out on the consumer's behalf. The business is permitted to require proof from the purported agent that they have permission to act on the consumer's behalf. User-enabled privacy controls are to be treated as requests made directly by the consumer and not as requests made by an agent for which the business can require proof of authorization.

Following a consumer's request to opt-out, a business is permitted to inform a consumer when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions for opting-in, without running afoul of the CCPA restriction on needing to wait 12-months before the business can ask the consumer to opt-in again. The opt-in process must involve two steps – an initial selection and then confirmation of that selection – in order to ensure opt-ins are intentional.

If a business that receives personal information from a third party other than the consumer wishes to sell that information, the business must first either provide a notice to the consumer informing them of the right to opt-out or obtain a certification from the source of the information that a CCPA notice was provided at the point of collection. If the business follows the latter method, the business must also obtain signed attestations from the source describing how notice was provided and including an example of the notice. These attestations must be retained for at least two years and made available to the consumer upon request.

D. Practices for Handling Personal Information of Minors

If a business has actual knowledge that it collects or maintains personal information of minors under age 16, the business must establish, document, and comply with a reasonable method for obtaining opt-ins before selling such information. For minors at least 13 years old but less than 16, the process must inform the minor of the right to opt-out at a later date and the process for doing so. For minors under age 13, the authorization of the child's parent or guardian is required. Acceptable methods for obtaining such parental authorization include providing a consent form to be signed under penalty of perjury and returned to the business, requiring a parent to use a payment method that provides notification to the primary account holder of the transaction, having a parent contact trained personnel via a toll-free phone number or other contact method, or checking a form of government-issued identification against databases of such information.

E. Service Providers

Service providers are prohibited under the regulations from using any personal information received in the course of providing services to a business (whether received from the business or through direct interaction with the consumer) for purposes of providing services to another person or entity. A limited exception is provided for combining personal information received from one or more businesses to the extent necessary to detect data security incidents, or to protect against fraudulent or illegal activity.

Should a service provider receive a request to know or a request to delete from a consumer that relates to any information that the service provider processes on behalf of a business, the service provider must

either comply with the request (if permitted by the business) or explain the basis for denying the request. If the service provider denies the request, it must inform the consumer that it should make the request directly to the business and, where feasible, provide the consumer with the business's contact information.

F. Recordkeeping

The regulations contain fairly extensive recordkeeping requirements. A business must maintain records of consumer requests made pursuant to the CCPA and of how the business responded for a period of at least 24 months. Each record must include the date of the request, the nature of the request, the manner in which the request was made, the date of the business's response, the nature of the response, and the basis for any denial of the request if the request is denied in whole or in part. Information maintained for recordkeeping purposes may not be used for any other purposes.

A business that annually buys, receives, sells, or shares personal information of 4 million or more consumers is required to compile and disclose in its privacy policy, or in a link accessible from the privacy policy, various CCPA metrics. These include the number of requests to know, number of requests to delete, and number of requests to opt-out that the business received, complied with in whole or in part, and denied, and the median number of days it took the business to substantively respond.