ALERT MEMORANDUM

The CCPA Takes Shape with Proposed Regulations, as Companies are Encouraged to Comply by January 1

October 22, 2019

The final version of the California Consumer Privacy Act of 2018 (the "CCPA") is coming into view. On October 10, California's Attorney General released the long-anticipated draft regulations (the "Regulations") to implement the CCPA, and on October 12, the Governor signed into law five amendments to the CCPA passed during the 2019 legislative session. (We previously discussed the CCPA here and the amendments here.) While the Regulations are currently subject to public comment and may be further modified by the Attorney General in response to such comments, the shape of the law that will come into effect on January 1 seems largely in place.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

Katherine Carroll
+1 202 974 1584
kcarroll@cgsh.com

Jon Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

Jane Rosen
+1 212 225 2026
jcrosen@cgsh.com

Michelle Butler
+1 212 225 2662
mibutler@cgsh.com

Given the scope of the Regulations and some unanticipated new requirements they contain, this alert memorandum provides a guide for understanding the Regulations by (i) highlighting some welcome clarifications included in the Regulations; (ii) identifying unexpected new obligations they impose; (iii) describing inconsistencies between the Regulations and the CCPA; and (iv) discussing other provisions in the Regulations that implement the CCPA.

Key Clarifications in the Regulations

The Regulations provide clarity regarding, and establish explicit requirements in, certain areas that companies have been struggling to understand under the CCPA, particularly with respect to verification procedures and the processing of consumer requests.

— Practices for Verifying Consumers' Identities. Companies' obligations under the CCPA to comply with consumer requests for information and deletion are contingent upon such requests constituting "verifiable consumer requests." The CCPA requires the Attorney General to establish the rules and procedures by which companies should determine whether a request qualifies as a verifiable consumer request. The Regulations provide the following guidance:

- Requests from Account Holders. Companies are permitted to follow their existing password authentication processes to verify requests made through password-protected accounts, provided that they implement reasonable security measures to detect fraud. If fraud is suspected, companies should refrain from complying until further verification procedures confirm the request is authentic.
- Requests from Non-Account Holders. With respect to requests made outside of password-protected accounts:
  - Requests for disclosure of specific information. The identity of a requestor of specific pieces of personal information must be verified to a "reasonably high" degree of certainty (such as by matching at least three items of personal information provided by the requestor with information already maintained by the company and requiring a signed declaration under penalty of perjury).
  - Requests for categories of personal information. Companies are only required to verify the identity of a requestor of categories of information to a "reasonable" degree of certainty (such as by matching two items of personal information to preexisting data held by the company).
  - Requests to delete. The standard for the verification for deletion requests is dependent upon the sensitivity of the personal information and risk of harm posed to the consumer by the unauthorized deletion of the information.

— Requests to Access or Delete Household Information. Many companies have been struggling to understand their disclosure and deletion obligations under the CCPA with respect to household information. The Regulations clarify that:

- Where a consumer does not have a password-protected account, a company may respond to a verified request as it pertains to household personal information by providing aggregate household information; and
- If all consumers in the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the company can individually verify all the members of the household, the company shall comply.

— Service Providers' Role. The Regulations provide some clarity on service providers' obligations with respect to consumer requests and permitted uses of personal information processed on behalf of another company.

- According to the Regulations, service providers are not required to comply with consumers' requests to know or requests to delete information they collect, maintain, or sell on behalf of a company they service, provided that the service providers inform consumers that they should submit their requests directly to the company (and provide contact information for such company, where feasible).

- The Regulations prohibit service providers from using personal information received from an individual or entity they service for the purpose of providing services to another individual or entity. However, service providers are expressly permitted to combine personal information received from multiple entities to the extent necessary to detect security incidents or protect against fraudulent or illegal activity.

Obligations Imposed in the Regulations but Not Expressly Included in the CCPA

In addition to offering clarifications on some of the less fully developed areas of the CCPA, the Regulations impose additional obligations on companies which do not appear in the statute.

— Obligations Relating to Notices to Consumers. The CCPA grants consumers the right to receive notices regarding the collection, use, and sale of their personal information. The Regulations set forth the information that must be included in each type of notice, in some cases going beyond what was required by the statute.

- Notice of Collection of Personal Information. The CCPA requires companies to disclose to consumers from whom they are collecting personal information, at or before the point of collection, the categories of personal information to be collected and the purposes for which the categories of personal information will be used. The Regulations add the following requirements for this initial notice of collection:
  - the categories should be described in the notice in a way that provides consumers a "meaningful understanding" of the information being collected and, importantly, companies must map the purposes to each specific category (for each category of personal information, identifying the business or commercial purpose(s) for which it will be used);
  - a link to or web address for the webpage containing the company's privacy policy (though for a company collecting the information online, this link itself may serve as the notice of collection if the privacy policy contains all the relevant information); and
  - if the company engages in the sale of personal information, a link to or web address for the webpage containing the "Do Not Sell My Personal Information" link.

  Companies that do not directly collect personal information from consumers (such as data brokers) need not provide any notice of collection but if they want to sell such information, they need to either (i) contact the consumer directly and give the consumer an opt-out right or (ii) contact the source of the information to confirm the consumer was given a proper notice of collection at the time of collection and obtain (and retain for at least two years) a signed attestation from the source regarding the sufficiency of such notice.
- Notice of Right to Opt Out of Sale. The CCPA requires companies to notify consumers of their right to opt out of the sale of their personal information, including by providing a link to a webpage that is titled "Do Not Sell My Personal Information." The Regulations further mandate that the foregoing notice include: a description of consumers' opt-out right, the web form by which consumers may exercise this right (or for companies that substantially interact with consumers offline, an alternative offline method consumers may use), instructions for using any alternative methods, any proof required for utilizing an authorized agent to submit an opt-out request, and a link or URL to the webpage with the company's privacy policy. A company that does not provide a notice of the right to opt out must state in its privacy policy that it does not and will not sell personal information.

- Privacy Policy. In addition to the CCPA's requirements for privacy policies (including a description of consumers' access and deletion rights, a list of categories of information collected, disclosed for business purposes or sold in the last 12 months, descriptions of consumers' opt out right, and a link to a "Do Not Sell My Personal Information" webpage), the Regulations impose further obligations. The Regulations require a company's privacy policies to cover both its online and offline privacy practices, and to be posted on the website, homepage or the landing page of its mobile application or otherwise made conspicuously available to consumers (to the extent a company does not have a website). In addition, the Regulations require the inclusion in a company's privacy policy of certain additional information not specifically noted in the CCPA, such as instructions for submitting a verifiable request, the procedure by which a consumer may designate an authorized agent to make requests, a description of the company's verification processes, a designated contact that the consumer can use for questions or concerns about the company's privacy policies, and a statement of "whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization."

— Obligations Relating to the Offer of Financial Incentives. Under the CCPA, companies are prohibited from discriminating against consumers for exercising their rights under the law (including by denying consumers goods or services, providing goods or services of a lesser quality, or charging different rates for goods or services), except that the company may offer a price or service difference that is reasonably related to the value that the consumer's data provides to the company. The CCPA also prohibits companies from entering a consumer into a financial incentive program unless the consumer has notice of the material terms of the incentive and opts in (which may be revoked at any time). The Regulations require additional disclosure regarding the categories of personal information implicated by the incentive and the process by which consumers can opt in to receive the incentive (and potentially opt out at a later time).

  Additionally, the Regulations require companies to determine and disclose the estimated value to the business of the personal information that forms the basis for offering the financial incentive or price or service difference, using one or more of the enumerated methods in the Regulations, including: the average value to the business of the sale, collection or deletion of a consumer's personal information, the revenue generated from having separate tiers of consumers, or "any other practical and reliable method of calculation used in good-faith." Companies must detail in a notice the method by which the value to the business is calculated.

— Deadlines to Respond to Consumer Requests. The Regulations impose significant new requirements with respect to the timing of companies' processing of consumer requests. For instance, companies must respond to requests to opt out within 15 days of receipt of such a request. Additionally, companies must provide confirmation of receipt of consumer requests to know and requests to delete, and information regarding how such requests will be processed (including information with respect to the verification process and anticipated response time, which may not exceed 45 days from the request, unless the company provides the consumer with notice and an explanation for requiring an additional period of up to 45 days), within 10 days of receipt of such requests.

— Obligations Relating to Requests to Delete. The Regulations include several new requirements with respect to deletion requests that are not suggested by the CCPA. For deletion requests made online, companies must use a two-step process with a request and a separate confirmation. Once a company approves a request to delete, it must either permanently and completely delete such

information on its systems (other than any archive or back-up systems), de-identify the information, or aggregate the information. In addition, the company must inform the consumer which of the foregoing methods it has selected to comply with the deletion obligation. If it denies the consumer's request, it must describe its basis for the denial (including any statutory or regulatory exception therefor) and not use the retained information for any other purpose other than that exception. If a request to delete is denied because a company cannot verify the identity of the requestor, the company must inform the requestor of this fact and treat the deletion request as a request to opt out of the sale of data.

— Obligations Relating to Requests to Opt Out. The Regulations also include several new requirements with respect to opt-out requests. Companies that collect personal information online must treat user-enabled privacy controls which indicate a desire to opt out, including a browser plugin or privacy setting, as if it were an affirmative request to opt out for that browser or device or, if known, for the consumer. In addition, when a consumer opts out, companies must notify all third parties to whom they have sold such consumer's personal information within 90 days prior to such request that the consumer has exercised the opt-out right, and must notify the relevant consumer when this notification obligation has been met. Further, the Regulations provide that once a consumer opts out, companies must use a two-step opt-in process in the future before selling the consumer's data (which under the CCPA cannot be requested until at least 12 months after the opt-out request). The Regulations permit a company to deny a request to opt out that it reasonably believes to be fraudulent, but the company must inform the requesting party and provide an explanation as to why it believes the request is fraudulent.

— Additional Record Keeping Obligations. Pursuant to the Regulations, companies must maintain, in a specified format, for at least 24 months records of all consumer requests under the CCPA and how they responded to such requests. Additionally, companies that annually buy, sell, or receive or share for commercial purposes the personal information of at least four million consumers must disclose in their privacy policies or on their website the number of requests to know, requests to delete, and requests to opt-out received, complied with and denied, and the median number of days it took the company to respond to such requests.

Inconsistencies between the Regulations and the CCPA: Request Methods

Because the Regulations were being drafted at the same time the law was being amended, there are inconsistencies between the law and the Regulations which will need to be addressed prior to the issuance of final regulations, specifically with respect to the methods for consumer requests that companies must make available.

For example, while the original rule under the CCPA requires companies to provide two or more designated methods for consumers to submit access requests (provided that one such method is a toll-free telephone number), a recent amendment to the law allows companies that operate solely online and have direct relationships with consumers from whom they collect personal information to provide only an email address and a website (to the extent a company has one) for the purposes of enabling access requests. The Regulations, however, require all companies to provide a toll-free telephone number.

Additional Implementing Provisions

The Regulations include specific detail on certain other areas of the CCPA, such as disclosure of personal information and the opt-in process for the sale of minors' information.

— Disclosure of Personal Information. The Regulations provide rules and guidance for situations where companies cannot verify the identity of a consumer who exercises a right to know or have concerns about the disclosure of information in response to a request. For example,

in the event a company is unable to verify the identity of a consumer who requests specific information, a company must not disclose specific pieces of information, must inform the consumer of that fact, and may process the request as if it were a request for categories of information. The Regulations also state that companies should not disclose any specific information if such disclosure presents a substantial, articulable and unreasonable risk to security, and should never disclose certain types of sensitive information, such as social security numbers, passwords, or financial account numbers.

— Sale of Minors' Information. The CCPA requires companies to obtain affirmative consent prior to engaging in the sale of personal information of minors under 16 years of age (with such consent originating from the parent or guardian of any minor under the age of 13) but does not provide specific guidance regarding the method for obtaining such consent. The Regulations clarify this opt-in process.

- Minors between 13 and 16. Companies with knowledge of their collection of personal information of minors between the ages of 13 and 16 must establish, document, and comply with a reasonable two-step opt-in process whereby such minors first clearly request to opt in to the sale of their personal information and then separately confirm their choice to opt in.
- Minors under 13. Companies with knowledge of their collection of personal information of minors under the age of 13 must establish, document and comply with reasonable processes for confirming that the person opting into the sale is a parent or guardian of the minor data subject. Confirmation could take various forms, including, for example, by providing a consent form for a parent or guardian to sign under penalty of perjury, having a parent or guardian communicate with trained personnel via video conference or a toll-free telephone number, or verifying a parent or guardian's government-issued identification.
- Right to Opt Out. Once the consent of a minor is obtained, companies must disclose the right to opt out at a later date and the process for doing so.

Next Steps - Public Comment

The Attorney General will be accepting comments on the Regulations through December 6, including through four public hearings the first week of December. While the Regulations may be modified prior to and potentially after the CCPA's January 1 effective date, companies should begin working towards compliance under its current provisions by that date, particularly given the fact that the Attorney General made clear during his October 10 public remarks that companies could be liable for instances of non-compliance with the CCPA that occur between January 1 and the date on which enforcement efforts may commence (the earlier of six months after the publication of the final regulations or July 1).

…

CLEARY GOTTLIEB