ALERT MEMORANDUM

California AG Proposes Modified CCPA Regulations: Significant Changes and Helpful Clarifications

February 12, 2020

On Friday, February 7, 2020, the California Attorney General released an amended set of proposed regulations (as supplemented on Monday, February 10, 2020, the "Revised Regulations") implementing the California Consumer Privacy Act of 2018 (the "CCPA"), including substantial changes to the draft regulations issued in October. While the Revised Regulations eliminate certain requirements that businesses found to be onerous and provide clarification on several points of lingering ambiguity, they also impose additional new compliance obligations and still fail to address certain thorny issues. Comments on the proposed regulations are due February 25, 2020.

This alert memorandum highlights certain notable changes that may affect the mechanisms and procedures businesses must implement in order to be in compliance with the CCPA, particularly with respect to public privacy policies, other notices to consumers, receipt and processing of CCPA consumer rights requests, and avoiding discriminatory practices.

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

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

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

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

Jonathan S. Kolodner
+1 212 225 2690
jkolodner@cgsh.com

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

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

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

Amendments Relating to Service Providers

The Revised Regulations provided several new obligations and clarifications specific to "service providers", as defined in the CCPA.

— Retention, Use, and Disclosure of Personal Information. As originally drafted, the regulations prohibited a service provider from using personal information received from the business it services or from interaction with a consumer for the purpose of providing services to any other person or entity. In the Revised Regulations, this prohibition has been replaced with a list of five purposes for which personal information obtained in the course of providing services can be used, retained, or disclosed, including "for internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source."

  This new structure may be interpreted to give a bit more leeway for certain businesses (e.g., data analytics providers) to use data they receive from clients to improve their services. However, it may be an unhelpful clarification for service providers (e.g., in ad-tech or data networks) that seek to use personal information to build or augment profiles or to clean or augment data from other sources.

— Sale of Personal Information. The Revised Regulations explicitly prohibit a service provider from selling data on behalf of a business when a consumer has opted out of the sale of their personal information with such business.

— Responding to Requests to Know and Requests to Delete. Under the original regulations, a service provider was required to explain to a consumer its basis for denying a request to know or a request to delete and direct the consumer to instead submit the request directly to the business (and, when feasible, provide the consumer with the business's contact information). The Revised Regulations clarify that a service provider that receives a request to know or a request to delete from a consumer may either respond on behalf of the relevant business or inform the consumer that it cannot act upon the request because it is a service provider. Businesses subject to the CCPA should therefore consider addressing in service agreements their service providers' rights and obligations with respect to access and deletion requests.

Amendments Relating to Requests and Responses

New Obligations Relating to Consumer Requests

— New Obligations Relating to Requests to Know. In response to a verified request to know categories of personal information, the Revised Regulations now require a business to separately disclose a list of categories of personal information that it has sold in the preceding 12 months and a list of categories of personal information that it has disclosed for a business purpose in the preceding 12 months, and in each case, identify the categories of third parties to whom it sold or disclosed for a business purpose each category of information. Businesses also still need to disclose the commercial or businesses purposes for which they collect and sell (but not disclose as required by the original regulations) personal information. The Revised Regulations also add certain biometric data to a list of types of information that a business should not disclose in response to a request to know.

— New Obligations Relating to Requests to Delete. Businesses that sell personal information must ask a consumer who is requesting the deletion of their personal information whether such consumer would like to opt out of the sale of their personal information (assuming such consumer has not already opted out) and provide the consumer either the contents of, or a link to, the notice of right to opt-out. Based on context, this requirement seems intended to apply only if a business receives a request for deletion that cannot be verified, though this is not clear under the text of the Revised Regulations. Further, under the Revised

Regulations, businesses need to let the consumers know whether or not they have complied with requests to delete, although they no longer need to disclose to consumers the manner in which they deleted personal information as required by the original regulations.

— New Obligations Relating to Requests to Opt-Out. Businesses must ensure that their methods for enabling consumers to opt-out of the sale of their personal information are easy to execute and require minimal steps, and are not designed with the purpose or substantial effect of subverting or impairing consumers' decision to opt-out.

— New Obligations Relating to Verifying Consumer Requests. The Revised Regulations impose new obligations and restrictions on business' processes for verifying consumer requests, including through a prohibition on businesses' requirements that consumers pay a fee (or unreimbursed costs of obtaining a notarized affidavit) in connection with the verification of a request to know or request to delete and expanded obligations in the event a business determines it cannot reasonably verify the identity of *any* consumer to the degree of certainty required by the Revised Regulations.

Reduced Obligations Relating to Consumer Requests

— Methods of Enabling Requests to Know and Requests to Delete. The Revised Regulations removed a number of specific requirements with respect to the designated methods businesses must provide to consumers for submitting requests to know and requests to delete. For example, while the CCPA requires businesses that maintain an internet website to make such website available to consumers to submit requests for information, the Revised Regulations no longer require all such businesses to provide an interactive web form accessible through the business's website or mobile application for such purpose. Further, businesses are no longer required to offer a method of enabling requests to know and requests to delete that reflects the manner in which the business primarily interacts with the consumer. Businesses that do not interact directly with consumers in the ordinary course of business do not need to provide an online method for submitting such requests.

— Responding to Requests to Know and Requests to Delete. The Revised Regulations permit a business to deny a request to know or a request to delete in the event it cannot verify the identity of the consumer initiating such request within 45 days of receipt of the request, and make clear that businesses are not required to search for personal information maintained solely for legal or compliance purposes (and not sold or used for commercial purposes) in response to a request to know if certain conditions are met. Additionally, businesses are no longer required to use a two-step process to confirm that consumers want their personal information deleted.

— Reduced Obligations Relating to Requests to Opt-Out. Pursuant to the Revised Regulations, a business that receives an opt-out request must only notify third parties to whom it has sold such consumer's personal information in the period between receipt of, and compliance with, the request of the consumer's exercise of the opt-out right (rather than all third parties to whom the business has sold such consumer's personal information in the 90 days prior to receiving the request, as required under the original regulations), and direct such third parties not to sell that consumer's information. Further, the business no longer needs to provide the consumer a notice confirming it has taken such steps.

- Exercising the Right to Opt-Out. As originally drafted, the regulations required businesses to treat any user-enabled privacy controls, such as browser plug ins or privacy settings, as signals that the consumer wanted to opt-out of the sale of their data. It was difficult to reconcile this requirement with the multistep procedures generally required in connection with a request to opt-out. The Revised Regulations have added language clarifying that a privacy control

"developed in accordance with these regulations" must *clearly* communicate or signal that a consumer intends to opt-out of the sale of personal information and that opt-out consent must be exercised *affirmatively* by a consumer (and not designed with any pre-selected settings). While the drafting is somewhat unclear, this requirement could be read to limit the scope of privacy controls which must be treated as signals to opt-out.

Helpful Clarifications Relating to Consumer Requests

— Submitting Requests to Know. The Revised Regulations eliminate the inconsistency between the original regulations and the CCPA regarding whether companies that operate solely online and have direct relationships with consumers are required to provide a toll-free number (they are not). The Revised Regulations explicitly state that such companies are only required to provide an email address for submitting requests to know (which is still inconsistent with the section of the CCPA that states that any business that maintains an internet website must make its website available to consumers to submit requests).

— Opting In After an Opt-Out. The Revised Regulations clarify that if a consumer who has opted out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of such personal information, the business may inform the consumer of the option to opt back in.

— Verification for Non-Accountholders. The Revised Regulations provide revised examples for compliant methods of verifying the identity of individuals without accounts who make a consumer request. The revised illustrative examples state that a retail business may require a consumer to identify items they recently purchased from the store or the dollar amount of the most recent purchase to verify such a consumer's identity (rather than requesting the consumer's name and credit card number, which was provided as an example of a compliant verification process in the original regulations). The Revised Regulations also provide guidance on how a business that collects information through a mobile application that does not require the creation of an account may verify the identity of a non-accountholder who claims to be associated with the non-name identifying information collected through the application.

— Household Information. The Revised Regulations helpfully narrow the definition of "household" and clarify businesses' disclosure and deletion obligations with respect to household information. A household is now defined as a person or group of people who reside at the same address, share a common device or the same service provided by a business, and are identified by the business as sharing the same group account or group identifier. Under the Revised Regulations, businesses must not comply with a request to know specific pieces of personal information about a household or a request to delete household information where a household does not have a password-protected account with the business, unless (i) all consumers of the household jointly make the request, (ii) the business individually verifies all members of the household, and (iii) the business verifies that each member making the request is currently a member of the household. Businesses that enable consumers to set up a password-protected account may use their existing business practices to address requests coming from a consumer with respect to household data.

Amendments Relating to Privacy Policies and Notices to Consumers

The CCPA requires businesses to make certain disclosures in their privacy policies, notices to consumers from whom they are collecting personal information at or before the point of collection (the "notice at collection"), and notices to consumers regarding the right to opt-out of the sale of personal information (the "opt-out notice"). The Revised Regulations impose certain new disclosure obligations

not included in the CCPA or the initial draft of the regulations, but also relax or remove entirely other obligations that appeared in the original regulations.

Privacy Policies

- Disclosure of Sources and Purposes of Collection of Personal Information. The original draft of the proposed regulations required businesses' privacy policies to state, for each category of personal information collected in the preceding 12 months, the source from which such information was collected and the business or commercial purpose for which such information was collected. This requirement has been removed in the Revised Regulations, which do not explicitly require disclosure of sources or purposes in businesses' privacy policies at all. There is some ambiguity as to the intended effect of the change to the Revised Regulations, as a general disclosure of the sources and purposes appears to be required under the statute.

Notices at Collection

- Disclosure of Uses of Personal Information. The Revised Regulations appear to remove the requirement that the disclosure in the notice at collection of the business or commercial purposes for which categories of personal information will be used be mapped to each specific category of personal information being collected.
- Indirect Collection and Data Brokers. The original regulations contained an exemption to the requirement to provide a notice at collection for businesses that do not collect information directly from consumers, provided that such businesses do not sell such personal information unless they received either direct consent from the consumer or a signed attestation from the information's source that sufficient notice was given at collection. The Revised Regulations change this exemption such that it benefits only a business that registers with the Attorney General as a data broker and includes in its data broker registration submission a link to an online privacy policy that includes a mechanism by which a consumer can submit a request to opt-out. Under the Revised Regulations, businesses that benefit from the exemption no longer face restrictions regarding the sale of information indirectly collected.

  Given the narrowing of this indirect collection exemption, it is no longer clear how a business that indirectly collects personal information but does not properly register as a data broker or fit within the service provider exemption can comply with the notice at collection obligation with respect to information collected from another business.
- Form of Notice. The Revised Regulations also clarify that notice at collection may be given in a manner consistent with the nature of the interaction (e.g. oral notice is acceptable when collection is in person or over the phone).

Opt-Out Notices

- Opt-Out Notice Exemption. The Revised Regulations do not require a business to provide an opt-out notice if it accurately asserts in its privacy policy that it does not sell personal information. Contrary to the original draft regulations, businesses are not required to represent in their privacy policies that they *will* not in the future sell personal information in order to benefit from this exemption.

Other Items of Note

— Definition of Personal Information. The Revised Regulations include guidance restricting the scope of the definition of "personal information" to information that is maintained by a business in such a manner that enables it to meet the requirements in the definition under the CCPA. For example, while an IP address can constitute personal information in certain circumstances, an IP address that a business collects but does not link

(and could not reasonably be linked) to any particular consumer or household would not constitute personal information.

— Non-Discrimination. The Revised Regulations clarify that financial incentives or price or service differences are discriminatory if a business is unable to calculate a "good-faith estimate of the value" of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the data, provide an updated list of factors to be considered when estimating the value of the consumer's data, and require the value of the consumer's data and an explanation of how the financial incentive or price or service difference is reasonably related to the value of the data to be explicitly included in the notice of financial incentive. Further, the Revised Regulations provide additional examples that distinguish discriminatory and non-discriminatory incentive programs.

— Record-Keeping Obligations. The initial draft of the regulations required businesses that annually buy, receive or share for commercial purposes or sell the personal information of at least four million consumers to make additional disclosures in their privacy policies or on their websites relating to their receipt of and response to requests to know, delete, and opt-out in the previous calendar year. The Revised Regulations increase this threshold from four million to ten million consumers per calendar year and clarify that the disclosure obligations apply on an annual basis.

Next Steps

The Attorney General will be accepting comments on the Revised Regulations through February 25, 2020. It is still not clear when final regulations will be issued, but the Attorney General has made clear that enforcement efforts may commence July 1.

…

CLEARY GOTTLIEB