ALERT MEMORANDUM

California AG Proposes Second Round of Modifications to CCPA Regulations

March 16, 2020

On Wednesday, March 11, 2020, the California Attorney General released a second set of modifications (the "March Revisions") to the proposed regulations implementing the California Consumer Privacy Act of 2018 (the "CCPA"), including substantive changes to both the initial draft regulations issued in October (the "Initial Regulations") and the revisions published Friday, February 7, 2020 (as supplemented on Monday, February 10, 2020, the "February Revisions"). (We previously analyzed the CCPA here, the legislative amendments here, the Initial Regulations here, and the February Revisions here.) While the March Revisions address several of the issues raised by stakeholders commenting upon the February Revisions, there are many issues that remain unaddressed. Another round of modifications to the regulations may be issued following the conclusion of the public comment period on March 27, 2020.

This alert memorandum highlights certain notable changes to the proposed regulations, particularly with respect to service providers, requirements for privacy policies and other notices to consumers, and the processing of CCPA consumer rights requests.

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

WASHINGTON, D.C.

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

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

NEW YORK

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

Service Providers' Use of Personal Information Clarified

The March Revisions again alter the treatment of service providers under the CCPA, one of the topics most commonly addressed by industry commenters following the issuance of the February Revisions.

— Service Provider's Use of Personal Information on Behalf of Third Parties. One material change brought by the February Revisions was an expansion of the permissible uses of personal information collected by a service provider in the course of providing services to a business. In contrast to the Initial Regulations, which prohibited the use of such information by a service provider for the purpose of providing services to others, the February Revisions detailed five categories of permissible use of such information, notably including to "perform the services specified in the written contract with the business that provided the personal information." Following the issuance of the February Revisions, many stakeholders commented that this language left open the interpretation that service providers are free to use personal information collected in the course of providing services to one business in order to provide the same services to other businesses, so long as the contract with the first business does not prohibit the provision of such services to such other businesses. This interpretation was, however, arguably inconsistent with the statute's definition of "service provider."

  The March Revisions clarify that use of personal information by service providers to service third parties is not permitted. Rather, the permissible use in the context of providing services is limited to processing or maintaining personal information "on behalf of the business that provided such information or that directed the service provider to collect the personal information" and in compliance with the written contract.

  At the same time, the March Revisions slightly expand the permissible internal use of personal information by the service provider. The February Revisions had allowed service providers to use the personal information internally to build or improve the quality of its services but not to build or modify household or consumer profiles. The March Revisions would allow such profile building so long as it is not used to provide services to another business.

— Ambiguity in a Service Provider's Role in Data Hygiene and Analytics Remains. One of the hotly debated provisions introduced in the February Revisions was one that prohibited service providers from building or improving their services by "cleaning or augmenting data acquired from another source." Many commenters noted that this language was vague, and requested that it either be clarified or removed to avoid inadvertently preventing pro-consumer data hygiene functions, such as refining address databases used to deliver goods to consumers, or otherwise permissible analytics functions. The March Revisions replaced the ambiguous word "cleaning" with the similarly undefined term "correcting" but took no other steps to clarify when such analytics and data hygiene functions may be performed.

Personal Information Definition Guidance Removed

— Personal Information Classification Is Not Reliant on Whether the Collecting Business Maintains the Information in a Manner that Allows Identification. The March Revisions removed entirely guidance introduced in the February Revisions that restricted the scope of the definition of "personal information" to information that is maintained by a business in a manner that meets the requirements for the definition of personal information under the CCPA. In other words, meeting the definition depended on whether the collecting business maintains the information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." The

guidance had specifically identified IP addresses as an example of information that may not be personal information if the collecting business "does not" and "could not reasonably" link the IP address to any particular consumer or household.

While many commenters applauded the California Attorney General for the guidance, numerous prominent privacy advocates argued for its deletion. Those critics voiced concerns that the provision was contrary to legislative intent (as demonstrated by the rejection of proposed amendments with similar effect) and created a substantial loophole, given that such information may be transferred or even sold to other businesses who could match it to a consumer or household and yet the seller of the personal information would escape the provisions of the CCPA entirely (including the notice and opt-out provisions). Following the March Revisions, a business has to treat as "personal information" any information that could be reasonably linked by anyone, whether the business or third parties, with a particular consumer or household.

Consumer Request Responses and Mechanisms Modified

— User-Enabled Controls that Indicate Consumer Intent are Requests to Opt-Out. The Initial Regulations required businesses to treat any user-enabled privacy control, such as a browser plugin or privacy setting, as a signal that the consumer using such a control wishes to opt out of the sale of personal information. The February Revisions seemed to relax this requirement, stating that user-enabled privacy controls developed in accordance with the regulations must *clearly* communicate or signal such an intent and should require consumers to affirmatively exercise their choice (and must not be designed with any pre-selected settings).

Industry reaction to this revision was split. Some commenters voiced support for this limitation on controls recognized as requests to opt-out, while others advocated for revisions that would designate a broader set of controls as opt-out requests, including "Do Not Track" privacy settings. The March Revisions represent a compromise approach. The provisions retain the requirement that privacy controls must clearly indicate an intent to opt out but do not require consumers to "affirmatively select" their choice, nor do they prohibit the use of pre-selected settings in order for such controls to constitute a request to opt-out. Notably, the March Revisions do not address other commenters' requests for clarification of related issues, such as the definition of "global privacy controls" or the interaction between global opt-out mechanisms and business- or website-specific privacy settings.

— Enhanced Responses to Requests to Know Biometric and Other Sensitive Data. The February Revisions added certain biometric data to a list of types of information that a business should not disclose in response to a request to know. While some commenters lauded this exemption as a much-needed consumer protection measure limiting the risk of identity theft and fraud, prominent commenters raised concerns that this type of restriction would effectively exempt several particularly sensitive personal data sets from consumer's right to know (e.g., social security numbers, health insurance information or medical identification numbers). In particular, the addition of biometric information as an exempt category was met with protests.

The March Revisions adopted the approach suggested by Californians for Consumer Privacy, specifying that businesses must still inform consumers with sufficient particularity of the categories of biometric and other sensitive information collected (e.g., biometric data including a fingerprint scan), but without disclosing the sensitive data itself.

— All Denied Requests to Delete Trigger an Opt-Out Offer. Under the Initial Regulations, businesses were required to treat a request to delete that could not be verified as a request to opt-out of sale, which is subject to less stringent identity verification requirements. The February Revisions

replaced this requirement with a provision requiring businesses that sell personal information to ask consumers if they would like to opt out of sale of their personal information and include a notice of the right to opt-out. There was some ambiguity, however, as to whether this requirement was triggered by all requests to delete or only those requests for which the business cannot verify the identity of the requestor. The March Revisions apply this obligation when (i) a business denies a consumer's request to delete (for any reason, not only as a result of an inability to verify the requestor's identity), (ii) the business sells personal information, and (iii) the consumer has not already made a request to opt-out.

— Deletion of Proposed Opt-Out Logo. The Initial Regulations promised to provide in later versions an optional image for businesses that sell personal information to include alongside the required opt-out link on their website. The February Revisions included a proposed image (an "opt-out button") and required that when the opt-out button is used, it must appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link and "be approximately the same size as other buttons on the business's webpage." Following an outpouring of criticism of the design, implementation, and utility of the proposed image, the entire provision was removed in the March Revisions.

Amendments Relating to Privacy Policies and Notices to Consumers

The CCPA requires businesses to make certain disclosures in their privacy policies, notices to consumers at or before the point of collection of personal information (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 February Revisions imposed certain new disclosure obligations not included in the text of the statute or the Initial Regulations but also relaxed or removed entirely other obligations that appeared in the Initial Regulations. The March Revisions walk back some of these changes while also imposing limited additional disclosure requirements on businesses that engage in the sale of personal information of minors.

Privacy Policies

— Disclosure of Sources and Purposes of Collection of Personal Information. For each category of personal information collected in the preceding 12 months, the Initial Regulations required businesses' privacy policies to state the category of sources from which, and the business or commercial purpose for which, such information was collected. This requirement was removed in the February Revisions, creating ambiguity as to the intended effect of the change since a general disclosure of sources and purposes appears to be required under Section 1798.110(c) of the statute. The March Revisions clarify that businesses have an obligation to provide source and purpose information in the privacy policy but need not map such information against each category of personal information collected in the past 12 months.

— Sale of Personal Information of Minors. The Initial Regulations and February Revisions imposed certain additional obligations not found in the statute upon businesses that sell the personal information of minors under the age of 16, including privacy policy disclosure obligations and requirements to implement opt-in mechanisms for such sales. As suggested by one of the comment letters, the March Revisions expand such privacy policy disclosure obligations by requiring any business that has actual knowledge that it sells the personal information of minors under age 16 to describe in the privacy policy the processes for minors (or their parent or guardian for minors under age 13) to opt in to such sale and the processes to subsequently opt out of such sale. The March Revisions could also be read to require a description in the privacy policy of the methods by which the business will verify that a person submitting a request to know or request to delete the personal information of a child under 13 is the parent or guardian of that child, though it is not clear that this is the intent.

Notice at Collection

— Employee Collection Notices. Businesses benefit from a temporary exemption for employment-related personal information under most provisions of the CCPA, which is currently scheduled to sunset on January 1, 2021. A notable exception is the notice at collection, which must still be given to employees, contractors, and job applicants at or prior to the point of collection of their personal information. The February Revisions introduced language allowing a business to link to a specialized employment-related privacy policy in notices at collection relating to employment information, rather than its general privacy policy. Perhaps in response to isolated comments claiming that even this reduced notice obligation is not justified by the language of the CCPA's exemption, the March Revisions eliminate the obligation for businesses to provide a link to any form of privacy policy in the notice at collection given in connection with the collection of employment-related information.

— Indirect Collection and Data Brokers. The Initial Regulations contained two provisions relevant to businesses that do not collect information directly from consumers: first, an exemption to the requirement to provide a notice at collection; and second, a restriction on selling such personal information without obtaining either direct consent from the consumer or a signed attestation from the information's source that sufficient notice was given at collection. The February Revisions removed both provisions, substituting instead an exemption from the requirement to give a notice at collection which benefits only a business that registers with the California Attorney General as a data broker and includes in its data broker registration submission a link to its privacy policy containing instructions on how consumers can submit opt-out requests. The March Revisions address concerns from many commenters (who protested that the structure from the February Revisions failed to contemplate situations in which the provision of a notice at collection by businesses that do not collect personal information directly from consumers but that are not data brokers would remain impractical) by providing an exemption to the notice at collection requirement for businesses with respect to personal information they collect indirectly, provided they do not sell it.

Other Modifications

— No Fees for Authorized Agents. The February Revisions added a restriction preventing businesses from charging consumers for identity verification. As an example, the February Revisions stated that "a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization." Comments were split on this provision. Some wanted this provision narrowed so as not to discourage notarization or to clarify that businesses *may* charge authorized agents (which may include for-profit companies set up for this purpose). Others applauded the provision and wanted clarification that businesses also may not charge authorized agents. The March Revisions extend the restriction on charging fees for identity verification to explicitly include authorized agents but do not reference authorized agents in the provided example.

— Value of Consumer Data Restricted to U.S. Persons. The CCPA prohibits businesses from discriminating against consumers for the exercise of their rights thereunder but explicitly allows businesses to charge a consumer a different price or rate, or provide a different level or quality of goods or services, if that difference is reasonably related to the value provided to the business by the consumer's data. The Initial Regulations required businesses who offer financial incentives or price or service differences to use and document a reasonable and good faith method for calculating the value of the consumer's data. The February Revisions provided additional guidance that, for the purpose of calculating the value of consumer data, a business may consider the value of the data

of all natural persons and not just consumers. Seemingly in response to a commenter concerned that businesses may use this to grossly understate how much they earn selling consumers' information (because the value of a consumer in certain countries may be much lower than the value of one in the United States), the March Revisions amend this provision to state that businesses may consider the value to the business of the data of all natural persons "in the United States."

Unanswered Questions and Next Steps

Consumer advocacy groups and industry associations have been outspoken and active participants in shaping of the CCPA and its implementing regulations. With the March Revisions, the California Attorney General demonstrated the importance of this interplay between regulators and the various stakeholders by incorporating new provisions, clarifying areas of disagreement, and walking back proposals that, based on the received comments, were unjustified or impractical. However, areas of ambiguity and uncertainty remain. The California Attorney General will be accepting comments on the March Revisions through March 27, 2020, which may prompt additional revisions in advance of the issuance of the final regulations. Enforcement of the CCPA begins July 1.

…

CLEARY GOTTLIEB