CCPA Update: Final Regulations Submitted but No Changes from Prior Draft

Alysa Z. Hutnik, Aaron J. Burstein, Alexander I. Schneider

June 2, 2020

On June 2, California Attorney General Xavier Becerra announced that he had submitted final CCPA regulations to the Office of Administrative Law (OAL) for review. The final regulations are substantively identical to the second set of modified proposed regulations, which the AG released in March. In addition, the AG issued a Final Statement of Reasons that (1) explains the changes between the first draft and final regulations, and (2) is accompanied by Appendices that respond to each public comment received throughout the rulemaking process – including written comments submitted in response to each draft of proposed regulations and those provided at the four public hearings held in December 2019.

We have described below some of the key provisions of the final regulations, which will impose additional requirements on businesses, service providers, and third parties and data brokers, and likely require the design and implementation of new processes. Whatever hardship the regulations may cause, it is clear that the AG is prioritizing consumer privacy, explaining that the office "has made every effort to limit the burden of the regulations while implementing the CCPA" and does not believe the regulations are "overly onerous or impractical to implement, or that compliance would be overly burdensome or would stifle businesses or innovation."

BUSINESSES

Privacy Policy: Privacy policies will need to identify the categories of personal information disclosed for a business purpose or sold to a third party in the preceding 12 months and provide **on a per category basis** the categories of third parties to whom the information was disclosed or sold. With respect to how a business describes these categories, the AG explained in the response to public comments that "the regulations provide the business with discretion in determining the best way to communicate the required information and … the flexibility to craft the notices and privacy policy in a way that the consumer understands them." This response clarifies that this list of categories need not follow verbatim the list provided in the CCPA's definition of personal information, but should prioritize terms that are meaningful to consumers.

Annual Privacy Policy Disclosures: The regulations will require that businesses that buy, receive for their commercial purposes, sell, or share for commercial purposes the personal information of **10 million or more** California residents in a calendar year disclose the following by July 1, 2021, based on data collected after the regulations take effect:

1. The number of requests to know that the business received, complied with in whole or in part, and denied;

2. The number of requests to delete that the business received, complied with in whole or in part, and denied;

3. The number of requests to opt out that the business received, complied with in whole or in part, and denied; and

4. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

The business may compile and disclose this information for all individuals, but must be able to provide statistics on California residents to the AG on request.

User-Enabled Privacy Controls: Businesses must honor privacy controls that clearly communicate or signal that the consumer intends to opt out of the sale of personal information. When "a global user-enabled privacy control conflicts with a consumer's existing business-specific privacy setting, the business may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific setting." Further, as to do-not-track signals, the AG responded to comments by noting that "the regulations do not prescribe a particular mechanism or technology but is [sic] technology-neutral in support of innovation in privacy services to facilitate consumers' exercise of their right to opt-out." The AG adds that the "regulations do not prohibit a business from responding and respecting a user's [browser] 'do not track' signal…. If a business chooses to treat a 'do not track' signal **as a useful proxy** for communicating a consumer's privacy choices…, the regulations do not prohibit this mechanism. The intention of the regulation was to encourage innovation and development of technological solutions to facilitate and govern the submission of a [sale opt-out] request."

According to the Final Statement of Reasons, the requirement to honor user-enabled privacy controls is "necessary to prevent businesses from subverting or ignoring consumer tools related to their CCPA rights." As support for this point, the FSOR notes that the AG reviewed businesses' disclosures about their responses to DNT signals, which are required under the California Online Privacy Protection Act, and concluded that businesses will very likely ignore or reject a global privacy control if the regulation permits discretionary compliance.

The final regulations also clarify that opt-out requests do not need to be verified.

Financial Incentives: Businesses must obtain opt-in consent before offering a "financial incentive" for the collection, sale, or deletion of personal information. By statute, a financial incentive must be "directly related" to the value provided by the consumer's personal information to the business, and the regulations require that the notice of financial incentive describe, among other things, (1) the incentive and its terms, (2) how consumers who have accepted a financial incentive may opt out, and (3) how the incentive is reasonably related to the value of consumers' data, along with a good-faith estimate of the value of consumers' data, and the method used to calculate that value. (However, in response to comments, the AG stated that the requirement to disclose the method used excludes privileged information as to **why** the business chose a particular method.) The regulations give several examples of how to calculate a financial incentive.

The regulations also clarify that, if the financial incentive is unrelated to the collection, sale, or deletion of personal information (e.g., a "store opening" sale), it does not fall under these financial incentive requirements.

SERVICE PROVIDERS

Internal Use: The regulations require that service providers use the personal information they receive from businesses "to process or maintain personal information on behalf of the business ... and in compliance with the written contract for services required by the CCPA," except in certain narrowly-defined circumstances, such as building or improving the quality of their services. Notably, those internal purposes do **not** include using the personal information for a service provider's own commercial purposes, to build consumer profiles, or to update personal information acquired from another source.

With respect to the concept of matching, the Final Statement of Reasons underscores that the regulation's use of "data" (rather than personal information) in this provision is intentional to "encompass the use of personal information acquired from a business to re-identify de-identified consumer information acquired from another source."

Interest-Based Advertising: In response to comments asking the AG to codify regulations to prevent service providers from using a consumer's personal information "for secondary purposes," the AG explained that it modified Section 999.314(c) "to prohibit service providers from using, retaining, and disclosing personal information outside of directly providing services to the business that has the direct relationship to the consumer." The AG further explained that, as to ads shown on websites, "[t]he CCPA allows a service provider to furnish advertising services to the business that collected personal information from the consumer, and such ads may be shown to the same consumer on behalf of the same business on any website.... Prohibiting a service provider from placing such ads is also unnecessary because the CCPA would not prohibit the business's own marketing department from placing the same ads itself. This provision of advertising services, however, does not relieve the service provider from its obligation to not share the personal information of the consumer with third parties and does not allow the service provider to use the personal information to provide advertising services to other businesses."

Contract Terms: In response to comments, the AG also clarified that neither the CCPA nor the regulations specify any mandatory contract language that must appear in agreements with service providers, so long as the substantive requirements are addressed.

Collection: The regulations and Final Statement of Reasons provide that service providers do not lose their status as service providers merely because they collect consumers' personal information, if that collection is performed at the business's direction and on behalf of that business. In response to comments, the AG also stated that the regulations do not expressly prohibit service providers from combining personal information from multiple sources, provided such combination is consistent with a business purpose and in the context of a contractual relationship. However, the AG warned that, to "the extent that the comment proposes that collective employment of a service provider is permissible, ... such a blanket exception may sweep too broadly and be exploited to thwart the intent of the CCPA."

Subcontractors: The regulations provide that service providers may hire subcontractors, as long as the subcontractors meet all the requirements for a "service provider" set forth in the CCPA and the regulations.

Service Provider vs. Third Party Definition: In response to comments seeking clarity between the terms in Cal. Civ. Code § 1798.140(v) and (w), the AG explained that these provisions create two types of parties that process personal information under a contract with a business: "service providers" and persons who are not "third parties." The AG explained that it was not necessary to change the regulations "because the two different definitions serve related, but different purposes.

The definition of service provider … establishes a role and requirements for sole proprietorships and corporate entities in which the transfer of information from a business to them is not deemed a sale. Relatedly, Civil Code § 1798.140(w)(2)(a) excludes from the definition of sale transfers to persons who meet the requirements in that subsection. If an entity qualifies as a service provider, **it need not also attempt to qualify as a non-third party person under subsection (w)(2)(a)**." This language thus clarifies that a certification with a service provider is not necessary.

Consumer Requests: A service provider that receives a request to know or delete from a consumer must either act on behalf of the business in responding to the request, or inform the consumer that it cannot act on the request because it is a service provider. Service Providers do not need to provide the consumer with contact information for the business, as the AG determined that such a requirement may be overly burdensome, particularly when a service provider provides services for many businesses that may have submitted personal information about the same consumer.

THIRD PARTIES AND DATA BROKERS

Notice at Collection: If a third party or data broker will sell personal information that it did not receive directly from a consumer, it must provide notice of its privacy practices to that consumer. It can satisfy this requirement by registering with the AG as a data broker and providing a link to its privacy policy in such registration.

ODDS AND ENDS

Cookie Banners Not Required: In response to comments seeking clarification on this point, the AG responded that the regulations do "not require a cookie banner, but rather leave[] it to businesses to determine the formats that will best achieve the result in particular environments. In addition, § 999.305(a)(3) provides additional guidance and illustrative examples on making the notice readily available to consumers."

Trade Secret Defense: The AG rejected commenters' requests to eliminate the obligation to provide a good faith estimate of the value of consumers' data due to trade secret concerns, responding that it was unclear how such data or method could be a "trade secret" that "[d]erives independent economic value … from not being generally known to the public" and "[i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy…," or would result in competitive harm. The AG concluded that the potential for harm is mitigated because all similarly situated competitors in California will be bound by the same disclosure requirements, and that neither federal nor state law provide absolute protection for trade secrets.

CPRA: In response to comments requesting that the AG defer regulations until after the CPRA initiative to avoid wasting resources, the AG responded that the "CPRA has not been enacted. If, in the future, statutes are enacted that require modification of the regulations, the OAG will review and modify the regulations as necessary."

***

The Office of Administrative Law now has 30 working days, plus an additional 60 calendar days due to the COVID-19 pandemic, to review the submission and confirm compliance with the California Administrative Procedure Act and corresponding regulations. OAL will then either approve the rulemaking action and file the proposed regulation with the Secretary of State or disapprove the rulemaking action.

The Attorney General has filed a written request for expedited review from OAL, meaning that the

regulations could become effective on July 1, 2020. In support of this request, the AG states that it "is mindful of the challenges imposed by COVID-19 and [the] Executive Order ... granting additional time to finalize proposed regulations," but "respectfully requests that the Office of Administrative Law complete its review within 30 business days, given the statutory mandate for regulations" by July 1. It is unclear whether OAL will grant this request. As of Tuesday evening, the regulations are not yet listed as "under review."

If the request is denied, and the final regulations are filed with the Secretary of State on or before August 31, they will take effect on October 1, 2020. If that filing occurs after August 31, the regulations will not take effect until January 1, 2021.

The immediate next step for companies is to take a close look at the regulations, evaluate what changes they will need to make, and map out a compliance checklist and timeline. Companies should also be mindful about approaching some of these requirements that offer discretion in implementation, and determining whether certain options may pose greater exposure to the company than others. Please contact any of the attorneys in Kelley Drye's Privacy Group if you would like assistance.