Data Privacy and Cybersecurity

California Attorney General Issues Proposed CCPA Guidelines

By: David P. Saunders

On October 10, 2019, the California Attorney General surprised many by issuing 24 pages of proposed regulations implementing the California Consumer Privacy Act of 2018 (CCPA). After reviewing the proposed regulations, they have left many in the industry shaking their heads. Absent from the proposed regulations is much of the clarity that industry participants were hoping for. In its place are additional obligations that not only risk confusing consumers, but that likely will pose administrative and logistical challenges.

Public comment on the proposed regulations is open through 5:00 pm PST on December 6, 2019. Interested parties can submit comments by e-mail to PrivacyRegulations@doj.ca.gov or by mailing comments to the Privacy Regulations Coordinator, California Office of the Attorney General, 300 South Spring Street, First Floor, Los Angeles, CA 90013. Additionally, the Attorney General will be holding four public hearings on the new proposed regulations, the schedule of which is available here**.**

In the meantime, let us examine the proposed regulations.

Companies Left to Wonder on Key Topics

Because this alert focuses on what *is* in the proposed regulations, we will highlight here only two of what we consider to be the biggest omissions from the proposed regulations: *First*, the regulations do nothing to address the scope of the definition of the terms "sell," "selling," "sale," or "sold" in the CCPA. Many had hoped that the Attorney General would produce regulations that exempted certain ordinary-course transactions between a company and its vendors. However, the proposed regulations do not address the definition at all, leaving in place CCPA's broad definition. *Second*, the proposed regulations do not offer any guidance as to how businesses are to calculate the $25 million "annual gross revenues" trigger for the CCPA. Absent any further guidance, the conservative approach continues to be to treat the threshold as a global calculation.

More Work Necessary for Companies to Comply with CCPA

Below we highlight some of the noteworthy aspects of the proposed regulations. Given the granularity of the proposed regulations, we have not attempted to summarize every aspect, and therefore encourage companies to read the proposed regulations thoroughly.

CCPA Notices Generally

No surprise that the proposed regulations require that the CCPA privacy notices published by companies must be in plain language, easily understood and available for those with disabilities. Perhaps more surprising, however, is the requirement that "[i]f the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall *directly notify the consumer* of this new use and *obtain explicit consent from the consumer* to use it for this new purpose." (999.305(a)(3)) (emphasis added). In other words, companies must receive opt-in consent from consumers to use their personal information if a company decides to use it in a way not originally disclosed.

The proposed regulations also require that "for each category of personal information, the business or commercial purpose(s) for which it will be used" must be disclosed. This means that the California Attorney General anticipates privacy disclosures to look more like GDPR privacy notices than the typical

American-form privacy notice where the "what is collected" section is divorced from the "how we use your data" section. Now, for *each* category of information collected, a business must specify the purpose for which the information is collected. That will be a change for many companies that were not impacted by GDPR.

The final proposed regulations related to privacy notices govern businesses that do not collect personal information directly from a consumer. For those companies, the proposed regulations provide that before a company that indirectly receives consumer personal information can sell that information, the company must: (1) contact the consumer directly and provide CCPA notices; or (2) contact the source of the personal information and (a) confirm that the source provided CCPA notices to the consumer and (b) "obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice." In short, parties that indirectly receive personal information now must develop a form attestation that would permit them to ultimately transfer the personal information to another.

Verifiable Consumer Requests

Summarized below are the disclosures companies are required to make with respect to each CCPA consumer right:

Request Type	Disclosures Required
Right to know about information collected, disclosed or sold	• Summary of the right • Instructions for submitting request • Process the business will use to verify the consumer request • List of personal information collected • For each category, provide the sources from which the information was collected, the business purpose for collection and the categories of third parties with whom the information is shared • State whether the business has sold any personal information (and if so, the categories) • State affirmatively whether the business sells personal information of minors under 16 years of age without affirmative authorization
Right to Request deletion	• Summary of the right • Instructions for submitting request • Process the business will use to verify the consumer request
Right to opt-out	• Summary of the right • A web form by which the consumer can submit their request • Instructions for submitting the opt-out • "Proof required when a consumer uses an authorized agent to exercise their right to opt-out" • A link or the URL to the business' privacy policy
Right to non-discrimination	• Summarize the right
Authorized agents	• Explain how a consumer can designate an authorized agent in an acceptable manner
Contact for additional information	• Must be provided

Throughout the proposed regulations is the suggestion that certain CCPA disclosures (*e.g.,* opt-out rights) link to a company's privacy policy. It appears that the California Attorney General is contemplating that businesses would provide multiple-different stand-alone disclosures to consumers in order to comply with CCPA. Whereas many companies had been folding CCPA requirements into their existing privacy policies, the proposed regulations appear to suggest that the CCPA disclosures should exist apart from a company's otherwise-existing privacy policies.

Request to Delete

New in the proposed regulations is the requirement that when a consumer makes an online request for deletion of their information, a company must engage in a two-step process. First, the consumer must "clearly submit the request," and then "separately confirm they want their personal information deleted." In the event that a company cannot verify the identity of the consumer making the request to delete, the proposed regulations provide that the company should instead treat the request as one to opt-out of the sale of information.

One saving grace for businesses is that the proposed regulations make clear that companies do *not* need to immediately delete personal information from archived or backup systems upon receipt of a request to delete. Instead, the information from those systems must be deleted when the "archived or backup system is next accessed or used." While this carve out is not perfect – what does it mean when an archived or backed up system is "next accessed or used"? – the proposed regulation at least demonstrates some understanding of the immense burden that would be put on businesses if they had to immediately delete information from archived systems.

Requests to Know

The proposed regulations create two data-disclosure safe harbors in which companies can refuse to provide certain information to consumers who submit a verifiable consumer request. First, the proposed regulations state that a business "shall not provide a consumer with specific pieces of personal information if the disclosure creates 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." The proposed regulations offer no guidance, however, as to when this threshold might be met. Second, the proposed regulations prohibit a business from disclosing in response to a request to know, a consumer's: social security number, driver's license number or other government ID number, financial account number, health or medical insurance or identification numbers, account password or security questions and answers.

Opt-Out Rights

The proposed regulations provide that "a consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out." Thus, if a business decides to sell personal information after collecting it from some consumers, those consumers will be considered to have opted-out, and will have to go through the affirmative opt-in procedures discussed below. The proposed regulations also create something of an automatic opt-out, allowing businesses to rely on a consumer's use of enabled web privacy controls as the equivalent of an opt-out request. Under the proposed regulations, the opt-out request *need not be* made in the form of a verified consumer request. However, a business can chose to verify the opt-out request *if* it has some reason to believe the request is fraudulent.

The regulations add an additional deadline and requirement to the opt-out process as well. Specifically, companies have to act on the opt-out request within 15 days. Additionally, companies must notify any company to which information was sold in the 90 days leading up to the request of the opt-out.

Opt-In Rights

In the event that a consumer who previously opted out of the sale of their information decides, for some reason, to opt-in to the sale of their information, companies must engage in a two-step process to confirm the change. First, a consumer must request to opt-in. Second, the consumer must separately confirm their desire to opt-in. In the event that a consumer previously opted-out of the sale of their information, but a transaction requires the sale of their personal information, the business interacting with the consumer can provide instructions to the consumer on how to opt back in. It is worth noting that the notion that a transition "requires" the sale of personal information is another indicator of the breadth of the term "sale" under CCPA; it includes much more than the vernacular of the term "sale."

Financial Incentives

Beyond merely describing the incentives that a business will offer consumers for not opting out of the sale of personal information, the proposed regulations require that a company provide "an explanation of why the financial incentive or price or service difference is permitted under the CCPA" including both a good faith estimate of the value of the consumer's data *and* a description of the method the business used to calculate the value of the data. Perhaps realizing the dynamic nature of the value of a consumer's personal information, the proposed regulations include a list of seven specific ways in which a business could choose to value consumer data ranging from marginal value from the sale of the information to the expense of the provision of financial incentives or price differences offered by companies.

Service Providers

The proposed regulations expand the definition of "service providers" in two significant ways. First, if a company meets the definition of "service provider" in the CCPA, but does work for a company that is *not* a business under the CCPA, the proposed regulations provide that the company is *still* considered a "service provider" under CCPA. Meaning that even if the principal company is not covered by CCPA, the *service provider* could still be covered with respect to the same personal information. For example, a processor of personal information for a business that has annual gross revenues of $24 million, and thus is not a "business" under CCPA. The processor would nonetheless be a "service provider" for purposes of CCPA. Second, the proposed regulations expand the definition of "service provider" to encompass not just entities that process or to whom personal information is disclosed, but also any company that collects personal information on behalf of a CCPA-covered business.

The Process of Verifying Consumer Requests

Required under the proposed regulations, companies have to develop documented processes for verifying a consumer request. Those policies must take into account, among other things, the type of information, the potential risk of harm if the information were disclosed in an unauthorized fashion, the likelihood of fraudulent or bad actors seeking the information, whether the verification process is sufficiently robust, the manner in which the business interacts with a consumer and the use of technology to assist in the verification.

One shortcut to verifying a consumer request is that companies can rely on password-protected accounts with consumers as a verification method. In other words, if someone logs into their password-protected account with the company and then submits a CCPA request, then unless the company has some reason to believe the activity is fraudulent or malicious, the act of logging in with the password would be sufficient for a company to verify the consumer's identity.

For companies that do not maintain password-protected accounts, the proposed regulations offer two approaches. For requests to know categories of personal information, companies should verify the consumer by "matching at least two data points provided by the consumer with data points maintained by the business." For a request to know specific pieces of information, companies should verify the consumer by matching at least *three* data points. And for deletion requests, the company must decide based on the nature of the request whether to match at least two or three data points. In performing this

matching, the proposed regulations caution that businesses should avoid collecting (for the first time) information such as social security numbers, driver's license or government ID numbers, medication information, account information and other sensitive data.

Record and Reporting Requirements

Throughout the proposed regulations, the California Attorney General imposes an obligation on companies to retain certain documentation regarding CCPA compliance from consumer requests to documentation of compliance for some period of time; often two years. The proposed regulations also, however, create an affirmative reporting requirement for businesses that "alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the personal information of" four million or more consumers.

Companies that do so must compile metrics related to (1) the number of requests to know that the business received, complied with and denied; (2) the number of requests to delete the business received, complied with and denied; (3) the number of requests to opt-out received, complied with and denied; and (4) the median number of days within which the business substantively responded to each request. These metrics then must be reported either in a company's privacy policy or otherwise posted on the company website with a link to the separate page in the privacy policy.

Data Collection from Minors

Under the proposed regulations, businesses must establish – in addition to the requirements of The Children's Online Privacy Protection Act – a method for documenting the affirmative consent by a parent to permit the sale of the information of someone under the age of 13. For minors 13 to 16 years of age, businesses must inform the child of the right to opt-out and the process for doing so. Finally, where a business does not sell the information of a person under the age of 16 without affirmative authorization, that company need *not* provide a notice of the right to opt-out to the consumer because the authorization is treated as an opt-in.

* * *

Overall, like the CCPA when it was first passed, there is still a lot of work that needs to be done before the proposed regulations can be finalized. As a result, the public comment period for these regulations will be important. Regardless, with the publication of the proposed regulations, the last piece of the CCPA puzzle for 2020 is coming into focus.

Contact Us

David P. Saunders

dsaunders@jenner.com | Download V-Card