

## Understanding What the Revised Draft CCPA Regulations Mean for Business

### Key Points

- The California Attorney General Office (AGO) issued revised proposed regulations (Version 2) regarding the California Consumer Privacy Act on February 7, 2020. The AGO will collect comments on the revised regulations until February 25, 2020.
- Version 2 includes many changes and appears to respond to comments received on the prior version. Issues addressed in Version 2 include permitted uses of personal information by service providers, the appearance of the “Do Not Sell” logo, notice requirements for apps and more.
- There is still no clear indication of when the final regulations will be released. Given the issues that remain in Version 2, businesses should consider submitting comments.

### I. Introduction

On February 7, 2020, the AGO released revised proposed regulations related to the California Consumer Privacy Act (CCPA) (Version 2). These are not the final regulations. Version 2 varies considerably from the initial proposed regulations (Version 1), undercutting statements by the Attorney General ([here](#)) that there was likely to be little change between Version 1 and the final regulations. Below, we analyze the changes.

The CCPA charges the AGO with promulgating regulations to implement the CCPA. The AGO issued its first version of proposed regulations (Version 1) in October 2019, which we analyzed [here](#). Comments submitted during the following public comment period highlighted a variety of practical issues with Version 1. Many of the changes in Version 2 appear to address comments received during the initial comment period.

It is not clear when the AGO will issue final CCPA regulations. The public comment period for Version 2 will close on February 25. The timing and exact process for finalizing the CCPA regulations will depend, in part, on the AGO’s response to the comments on Version 2. It could issue revised regulations or submit the final text of its proposed regulations to the Office of Administrative Law, which must approve the regulations before they take effect. Information on the rulemaking process can be found [here](#).

### Contact Information:

**Natasha Kohne**

Partner  
[nkohne@akingump.com](mailto:nkohne@akingump.com)  
San Francisco  
+1 415.765.9505

**Michelle Reed**

Partner  
[mreed@akingump.com](mailto:mreed@akingump.com)  
Dallas  
+1 214.969.2713

**Dario Frommer**

Partner  
[dfrommer@akingump.com](mailto:dfrommer@akingump.com)  
Los Angeles  
+1 213.254.1270

**Jo-Ellyn Klein**

Senior Counsel  
[jsklein@akingump.com](mailto:jsklein@akingump.com)  
Washington, DC  
+1 202.887.4220

**Diana Schaffner**

Counsel  
[dschaffner@akingump.com](mailto:dschaffner@akingump.com)  
San Francisco  
+1 415.765.9507

## II. Discussion of Revised Draft

Version 2 includes a number of important changes. As we did with the prior Version 1, below we provide a chart with a high-level summary of: (1) provisions that clarify or provide helpful operationalization guidance, (2) provisions that outline new requirements beyond the current terms of the CCPA or raise other issues, and (3) ambiguous or difficult issues that Version 2 either does not address or leaves unresolved.

Helpful Clarifications	New Requirements / Complications	Issues Not Resolved
<ul style="list-style-type: none"> <li>• Provides guidance on meaning of personal information (PI).</li> <li>• Narrows definition of household and restricts household requests.</li> <li>• Aligns use of PI for non-notified purposes with Federal Trade Commission (FTC) “material difference” standard.</li> <li>• Provides guidance on how to meet online accessibility requirements.</li> <li>• Clarifies collecting employment-related information is a business purpose.</li> <li>• Fixes opt-in error for 13-16-year-old bracket.</li> <li>• Clarifies financial incentive notice only required if actually offering incentive.</li> <li>• Limits statements required to include in privacy policy re sale of PI generally and sale of minors’ PI.</li> <li>• Makes two-step deletion request process is optional.</li> </ul>	<ul style="list-style-type: none"> <li>• Requires just-in-time notice for apps in certain circumstances.</li> <li>• Removes security exception to response to request to know.</li> <li>• Indicates that oral notice can/should be provided where appropriate.</li> <li>• Requires instructions on how to use agents.</li> <li>• Imposes “reasonable security” requirement on CCPA records.</li> <li>• Limits use and sharing of information collected to comply with CCPA.</li> <li>• Prohibits charging fees for verification.</li> <li>• Imposes security and other limits on agents.</li> <li>• Data brokers must provide opt-out mechanism in privacy policy and provide link to the same in registration with state to take advantage of exception to notice requirement in Sec. 1798.115(d).</li> </ul>	<ul style="list-style-type: none"> <li>• No guidance on “specific pieces of information.”</li> <li>• No guidance on “reasonable security” standard.</li> <li>• No guidance on what it means to ensure consumers have a “meaningful understanding.”</li> <li>• No draft regulations on three of seven mandated areas: (1) categories of personal information, (2) unique identifiers, and (3) exceptions to the law.</li> <li>• No guidance on how to provide accessible offline materials.</li> </ul>

<ul style="list-style-type: none"> <li>• State denial of CCPA request is not discriminatory if in accordance with CCPA/regs.</li> </ul>		
---	--	--

**A. Definitions (§ 999.301)**

Version 2 revises and/or adds several important definitions. Below, we walk through key changes. Text in red indicates text that was added to the proposed regulations in Version 2.

- **Personal Information** - Clarifies that whether information is “personal information,” depends, in part, on how the information is maintained. Information is not “personal information” unless it is maintained 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” California resident or household. It provides that IP addresses, for example, do not qualify as personal information if the IP addresses are not linked and could not reasonably be linked to a particular consumer or household. This guidance may have significant implications for business and could ease compliance costs.
- **Household** - Narrows the definition of “household” to mean people who (1) live at the same address, (2) share a common device or receive the same service from the business, and (3) are identified by the business as sharing the same account or unique identifier. This appears likely to help address some of the safety concerns raised by the prior definition, which categorized all people occupying a single dwelling as a “household.” Other revisions in Version 2, together with the revised definition, appear geared toward limiting the ability of one member of a household to gather information on other members without the other members’ knowledge.
- **Employment-Related Information** - Adds a new definition for “**employment-related information**” that aligns with the employee exemption in Section 1798.145 and provides that the collection of employment-related information is a “**business purpose**.” This latter point provides a path to permit sharing employment-related information with service providers and may become more important should the employee exemption expire.
- **Request to Know** - Specifies that a “request to know” is a request that a business disclose personal information it “has **collected**” about the consumer, not just personal information that the business has on the consumer.
- **Authorized Agent** - Specifies that an “authorized agent” must be, among other things, registered with the California Secretary of State “**to conduct business**” in California. The lack of this specification in Version 1 had led to some confusion.
- **Price or Service Difference** - Targets the definition of “price or service difference” to mean a difference “**related to the disclosure, deletion, or sale of personal information**.” This appears to limit the applicability of the related provisions in a manner that better aligns with legislative intent behind the non-discrimination provisions.
- **Fixes for Minors** - Provides that a “request to opt-in” is necessary from “**a minor at least 13 and less than 16** years of age.” This change fixes a gap in Version 1 that did not account for the need to seek opt-in consent from consumers in the 13 to 16

bracket. Version 2 also clarifies that “verification” includes verifying that a request submitted for a minor under 13 was submitted by the minor’s parent or legal guardian.

## **B. Accessibility Requirements that Apply Across Sections**

Version 2, like Version 1, requires businesses to ensure that notices at collection, opt-out notices, privacy policies and responses to consumer requests meet certain accessibility requirements. There were two helpful changes in Version 2 related to this issue. First, businesses are only required to provide copies of such materials (notices, privacy policies and responses) in languages in which they usually provide similar information to “consumers in California.”

Second, Version 2 provides businesses guidance on how to meet the requirement that they provide *online* materials (notices, privacy policies and responses) to consumers in a manner that is accessible to consumers with disabilities. It provides that they can do so by “follow[ing] generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium.” With regard to offline materials, businesses still have to provide information on how a consumer with a disability may access the notice in an alternative format. No details are included as to what formats would meet this offline requirement.

## **C. Notice Requirements**

### **1. Notice at Collection (§ 999.305)**

Version 2 clarifies how a business may provide notice at collection through revised examples. It indicates that notice at collection may be provided through a “conspicuous link” to the notice at collection posted on (a) the “introductory page of the business’s website and all webpages where personal information is collected”; or, if the business collects personal information through a mobile app, (b) in the app download page and within the app (e.g., in the settings menu). These changes align the examples with the definition of “homepage” in Section 1798.140(l), without requiring businesses to cross-reference that definition to understand the examples (as was required with Version 1).

The revisions also permit a business to provide oral notice if personal information is collected in person or over the phone. Other provisions provide that a business may confirm receipt of a consumer request on a phone call. Given these revisions, businesses may consider revising call recording warnings to include CCPA statements once the regulations are final.

Version 2 adds a new requirement to provide “just-in-time notice” when a business “collects personal information from a consumer’s mobile device for a purpose the consumer would not reasonably expect.” That notice has to include a summary of the categories of personal information collected and a link to the full notice at collection. Determining whether a consumer should “reasonably expect” the collection appears to be open to interpretation.

The revisions modify the standard that controls whether a business may use personal information for a purpose not listed in the original notice at collection. In line with FTC guidance, Version 2 provides that personal information may not be used for a “materially different” purpose than the purposes about which the consumers were

originally provided notice at collection. The prior draft imposed a less practical standard that would have prohibited use without opt-in consent for “any purpose other than disclosed in the notice at collection.” This may help companies whittle the “purposes” section of their privacy policies.

Version 2 replaces a provision that had previously enabled a company that did not collect personal information directly from consumers to sell that information under specific, difficult circumstances with a provision focused on registered data brokers. This simplifies compliance for registered data brokers, but removes a potential means of compliance for companies that do not collect personal information directly from consumers and are not registered data brokers. The provision enables a data broker registered under California’s data broker law (Cal. Civ. Code § 1799.99.80) to avoid providing notice at collection if it included opt-out information in its privacy policy filed with the state. This appears to simplify data brokers’ compliance with Section 1798.115(d).<sup>1</sup>

The revisions allow for sensible modifications to the notice at collection provided to employees, including permitting businesses to provide a link to an employee-specific privacy policy (rather than the consumer privacy policy) and removing the need to post a “Do Not Sell” link in the employee notice.

## 2. Notice of Opt-Out Right/”Do Not Sell” (§ 999.306)

Version 2 eliminates the requirement that a business treat a consumer whose personal information is collected while the notice of right to opt-out is not posted as having validly submitted an opt-out request. Instead, Version 2 prohibits a business from selling the personal information it collected during the time the business did not have a notice of right to opt-out posted unless it obtains affirmative, opt-in consent.

The revisions also remove some content from the opt-out notice. A business, for example, will no longer have to include a link to the business’s privacy policy, or specify what proof a consumer has to provide to use an authorized agent.

Version 2 finally provides an optional model opt-out button. That button may be provided in addition to, but not in lieu, of a “Do Not Sell” link.



## 3. Notice of Financial Incentive/Difference in Service (§ 999.307)

Version 2 modifies the purpose of the financial incentive notice to explain “**the material terms of a** financial incentive or price or service difference,” and provides that notice is only required when a “business **is offering**” an incentive or difference (not when it *may* offer the same). The revisions clarify that a business that does not offer incentives or differences does not have to provide a relevant notice.

### D. Privacy Policy (§ 999.308)

The revisions modify the requirements for privacy policies in a few ways. Version 2 removes the need to specify for each category of personal information collected the

sources, purposes and categories of third parties with which the information was shared. This may help declutter some CCPA sections. It also helpfully limits the requirement that a business include a statement regarding the sale of minor's personal information to only those businesses that have "actual knowledge that [they] sell[] the personal information" of minors. Similarly, businesses are only required to state whether they sell personal information, rather than whether they sell or *will* sell personal information.

The revisions also modify the information that has to be included in the privacy policy regarding a request to delete. Version 2 provides that a business only has to explain that a consumer has a right to request deletion of personal information collected by the business. It expressly eliminates the need to explain that a consumer has a right to delete personal information "maintained" by the business.

Version 2 does include a couple of additional obligations. It requires that for each category of personal information, a business must provide the categories of third parties to which the information was disclosed or sold. The revisions also clarify that businesses are expected to "provide instructions on how an authorized agent" can make a request on their behalf. Version 1 had required that a business explain how a consumer can designate an agent.

## **E. Requests to Know and Requests to Delete**

### **1. Methods for Submission of Requests to Know or to Delete (§ 999.312)**

Version 2 makes several changes to methods of submission for requests to know and to delete. It eliminates the requirement that if a business does not interact directly with consumers, at least one method for submission of either type of request be online. Businesses must consider "the methods by which [they] primarily interact[] with consumers" when deciding what methods to provide for submitting either requests to know or to delete.

- **Requests to Know:** Version 2 eliminates the requirement that a business operating a website includes an interactive webform to enable submission of a request to know. A toll-free number is still required. It also implements a legislative change to enable businesses that operate exclusively online and have a direct relationship with consumers to provide an email address for submitting requests to know.
- **Requests to Delete:** Version 2 makes optional the use of the two-step process to request to delete personal information included as a requirement in Version 1.

### **2. Responding to Requests to Know and Requests to Delete (§ 999.313)**

Version 2 made several changes applicable to responses to both requests to know and requests to delete. It permits a business to provide confirmation of receipt in the same manner that the request was submitted. For oral conversations, confirmation may be provided in the same oral conversation in which a request is submitted. Version 2 also enables a business to deny a request to know or to delete if it cannot verify the consumer within 45 calendar days. Additional changes applicable to particular request types are detailed below.

- **Updated Deadlines:** Version 2 changes certain deadlines by modifying the required time period to be in either calendar or business days. A business: (1) has

to confirm receipt of a request to know or to delete “within 10 **business** days”; (2) has to respond to a request to know or to delete “within 45 **calendar** days”; and (3) may extend its time to respond to requests to know or to delete by an additional “45 **calendar** days” or a total of “90 **calendar** days.”

- **Requests to Know:** Version 2 eliminates the security exception that previously enabled a business to avoid providing a response to a request to know if disclosure of specific pieces of information “create[d] a substantial, articulable, and unreasonable risk” to certain security. It prohibits a business from providing in response to a request to know “**unique biometric data**,” in addition to other information already listed in Version 1. The revisions add a new exception for information that is maintained solely for legal or compliance purposes and is not otherwise used or disclosed. Version 2 provides that a business is not required to search for personal information in response to a request to know if the following are true: (1) it does not maintain the personal information in a searchable or reasonably accessible format; (2) it maintains the personal information solely for legal or compliance purposes; (3) it does not sell the personal information and does not use it for commercial purposes; and (4) it describes the categories of records that may contain personal information that it did not search.
- **Requests to Delete:** Version 2 eliminates the need to treat a request to delete that cannot be verified as an opt-out request. Instead, a business that sells personal information may ask the consumer if they would like to opt-out and provide the opt-out notice or a link to the same. It also removes the need to specify how the personal information was deleted when providing a response to a request to delete. A business must tell consumers whether it complied with the request when it responds. Businesses may retain records of requests to delete in order to ensure the information remains deleted, but they are required to inform consumers if they do so. Version 2 clarifies that personal information stored on archived or back-up systems does not need to be deleted unless the data in those systems is restored to an active system or is accessed or used for a sale, disclosure or commercial purpose.

#### **F. Service Providers (§ 999.314)**

The revisions to the service provider provisions do a number of helpful things. Version 2 provides clear terms for when a service provider may retain, use or disclose personal information obtained in the course of providing services, including: (1) for its own internal use to build or improve its services, as long as it does not “**build[] or modify[] household or consumer profiles, or clean[] or augment[] data acquired from another source**”; and (2) to retain another service provider as a subcontractor, if the subcontractor meets the requirements for a service provider. The revisions do not define “build,” “modify,” “clean,” “augment” or other terms key to applying this provision. It also requires service providers either to respond to consumer requests on behalf of a business or to respond that they cannot because they are not the business.

#### **G. Requests to Opt-Out (§ 999.315)/Opt-In (§ 999.316)**

Version 2 requires that the method for submitting requests to opt-out must be easy for consumers to execute and require minimal steps to enable consumer opt-out. The method cannot be designed to subvert or impair the consumer’s decision to opt-out. A business has to comply with a request to opt-out as soon as feasible, “but no later than 15 **business** days from the date the business receives the request.”

The revisions require, as did Version 1, that a business treat global privacy controls as a valid opt-out request. Version 2 further provides that any privacy control has to require the consumer to affirmatively select their choice to opt-out and cannot use pre-selected settings. When a global privacy control conflicts with a consumer's business-specific privacy setting or their participation in a financial incentive program, the global privacy control wins. However, a business may then inform the consumer of the conflict and give the consumer the option to confirm the business-specific settings or their participation in the financial incentive program. Although these revisions do not fully address industry concerns, they do at least give businesses the option of following up with consumers to confirm an opt-out is intended.

Version 2 narrows a business's notice obligations should a consumer opt-out of sales. Under Version 1, a business had to notify all third parties to which it sold the personal information in the 90 days prior to the business's receipt of the opt-out request. Under Version 2, a business only has to notify those third parties to which it sold the consumer's personal information after the consumer submitted their request, but before the business complied with the request. It must also direct those third parties not to sell the information.

Helpfully, the revisions also permit a business to ask a consumer who previously opted-out to opt-in if the consumer initiates a transaction or attempts to use a product or service that requires the sale of the consumer's personal information. The business has to inform the consumer of the requirement.

#### **H. Training and Record-Keeping (§ 999.317)**

Version 2 imposes certain reporting requirements on businesses that buy, sell or share/receive for commercial purposes the personal information of 10,000,000 or more California residents in a calendar year. This should reduce the overall applicability of this section. The revisions also require businesses to implement and maintain reasonable security procedures in maintaining records required by the CCPA, prohibit use of such records for any purpose aside from compliance with the CCPA and prohibit sharing information maintained for recordkeeping purposes with a third party.

#### **I. Requests to Access or Delete Household Information (§ 999.318)**

The revisions include important changes to the process for requesting access to or deleting household information. Industry advocates have repeatedly raised security concerns with regard to this issue. Version 2 adds a joint verification requirement that must be met before specific pieces of personal information may be provided or household information deleted, unless the requester has the password for the household's password-protected account with the business. To meet the requirement: (1) all consumers of the household must jointly submit the request; (2) the business must individually verify all the members of the household; and (3) the business must verify that each member making the request is currently a member of the household. When household members are under 13, a business must obtain verifiable parental or guardian consent.

#### **J. Verification of Requests (§§ 999.323, 999.325)**

Businesses are generally prohibited from charging fees to verify requests to know or to delete. For nonaccount holders, a business must deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor. A business that does not have a reasonable means of verification for nonaccount



holders must state so and explain in its privacy policies. It is then required to reevaluate annually whether a method can be established.

#### **K. Authorized Agents (§ 999.326)**

Version 2 enables a business to require a consumer seeking to use an authorized agent, among other things, to require the consumer to confirm with the business directly that the consumer provided the agent permission to submit the request. It also imposes obligations on agents, including requiring agents to implement and maintain reasonable security to protect consumer information. Version 2 prohibits agents from using personal information for any purpose other than fulfilling the consumer's requests, for verification, or for fraud prevention.

#### **L. Minors (§ 999.330)**

The revisions specify that businesses that have actual knowledge that they “sell” personal information of minors have to obtain opt-in consent from those at least 13 and less than 16 years of age. Similarly, Version 2 requires businesses that “sell” the personal information of children to have a reasonable method for determining whether the person affirmatively authorizing the sale is the parent or guardian of that child. Both of these revisions bring the regulations more in line with the CCPA. The revisions add a new requirement that businesses have a reasonable method for determining whether a person submitting a request to know or to delete the personal information of a child under 13 is the parent or guardian of that child.

#### **M. Discriminatory Practices (§ 999.336)**

Version 2 prohibits businesses from providing a financial incentive or difference in services if they cannot calculate a good-faith estimate of the value of the consumer's data or show the reasonable relation of the incentive or service difference to the value of the data. The revisions clarify that a business's denial of a request to know, delete, or opt-out is not discriminatory if it abides by the CCPA. The revisions also provide that a price or service difference that is the direct result of compliance with federal law is not discriminatory.

#### **N. Calculating the Value of Consumer Data (§ 999.337)**

The revisions give a business the ability to “consider” one of several proposed methods for calculating the value of consumer data. Version 1 had made use of these methods mandatory. Version 2 also enables a business to consider the value of data of all natural persons, not just California residents, for the purpose of calculating the value of consumer data.

### **III. Conclusion**

Businesses should consider the potential impact of Version 2 on their particular industries and needs and consider submitting comments on the revised proposed regulations. The comment period will remain open until 5:00 p.m. on February 25. This may be the last opportunity businesses have to comment on some of these provisions before the regulations take effect. Our CCPA team can help businesses consider the practical impact of the revisions and consider next steps.

<sup>1</sup> Section 1798.115(d) prohibits a third party from selling personal information about a consumer sold to it by a business unless the consumer receives explicit notice and an opportunity to exercise the right to opt-out.