# Cybersecurity Alert

Akin Gump
STRAUSS HAUER & FELD LLP

## A Business Guide to the Draft CCPA Regulations

10/28/19

**Key Points**:

- The Draft Regulations introduced by the California Attorney General's Office on October 10, 2019 are subject to a public comment period and public hearings that will close on December 6, 2019. Now is the time to act to try to influence the final regulations.
- The Draft Regulations are a mixed bag—they contain some helpful clarifications, include some additional obligations beyond the CCPA's current requirements and leave various ambiguous issues either unaddressed or unresolved.
- The Draft Regulations go beyond the CCPA in several important ways and introduce new requirements, including new recordkeeping requirements for businesses that alone or in combination receive or share records of four million or more California residents.

### 1. Introduction

The California Attorney General's Office (AGO) recently issued its much anticipated draft regulations ("Draft Regulations") for implementation of the California Consumer Privacy Act (CCPA). The AGO also issued a corresponding Initial Statement of Reasons (ISOR) that provides additional explanation. The Draft Regulations are a mixed bag—they contain some helpful clarifications, include some additional obligations beyond the CCPA's current requirements, and leave some ambiguous issues either unaddressed or unresolved. This alert discusses what the Draft Regulations do and do not address and provides practical advice for entities caught in the CCPA's web.

More information on the CCPA can be found in our prior client alerts and publications, including our initial summary of the CCPA, our overview of the September 2018 amendments and our recent article in the Recorder concerning the September 2019 amendments.

The CCPA requires the AGO to adopt regulations to guide businesses in fulfilling their obligations generally, and with regard to seven areas in particular. The Draft Regulations only cover some of those seven areas. The AGO cannot bring an enforcement action until six months after the publication of the final regulations or July


Contact Information

If you have any questions concerning this alert, please contact:

**Natasha G. Kohne**
Partner
nkohne@akingump.com
San Francisco, CA
+1 415.765.9505

**Michelle Reed**
Partner
mreed@akingump.com
Dallas
1 214.969.2713

**Dario J. Frommer**
Partner
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

**Jo-Ellyn Klein**
Senior Counsel
jsklein@akingump.com
Washington, D.C.
1 202.887.4220

**Diana E. Schaffner**
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

**Rachel Kurzweil**
Associate
rkurzweil@akingump.com
Washington, D.C.
1 202.887.4253

1, 2020—whichever is earlier. Given the current schedule, it appears unlikely that AGO enforcement will begin before July 1, 2020.

At the press conference announcing the Draft Regulations, the Attorney General and his staff appeared to imply that they intend to investigate alleged violations that take place between January 1 and July 1, 2020. This seemingly puts businesses on notice of the Attorney General's intention with regard to this interim enforcement period.

The AGO is collecting comments on the Draft Regulations until December 6. It will hold four public hearings as part of that process in Sacramento, December 2; Los Angeles, December 3; San Francisco, December 4; and Fresno, December 5. Thereafter, the AGO will either issue revised regulations or submit the final text of the regulations to the Office of Administrative Law (OAL). The timing and exact process depends, in part, on the AGO's response to comments. The regulations go into effect upon OAL approval.

## 2. Discussion of Proposed Regulations

The Draft Regulations mainly focus on businesses' notice obligations and consumers' rights to request information, delete information or opt-out of the sale of information. They clarify things like businesses' response deadlines and the required contents of privacy notices. New obligations include, among others, that businesses apply "reasonable security measures" to consumer requests. Plenty of ambiguities remain. This alert provides a non-exhaustive overview of key points from the Draft Regulations.

Businesses that have already begun operationalizing the CCPA should carefully review the text of the Draft Regulations. Draft consumer notices, privacy policy inserts and related materials will likely need to be updated. The Draft Regulations also impose additional process requirements that may require modification of planned consent and opt-out systems, including new requirements for two-step opt-in and two-step deletion request mechanisms.

The following chart provides a high-level summary of the Draft Regulations in terms of (1) provisions that clarify or provide helpful operationalization guidance, (2) provisions that outline new requirements beyond the current terms of the CCPA and (3) ambiguous or difficult issues that the Draft Regulations either do not address or leave unresolved.

| Helpful Clarifications | New Requirements | Issues Not Resolved |
|---|---|---|
| • Clear directions on what has to be included in privacy policies and initial notices.<br>• Initial notice may be provided via link to privacy policy posted on website.<br>• Guidance on authorized agents— | • Upon opt-out, must tell third parties to which sold PI not to further sell.<br>• Respond to consumer requests even if deficient.<br>• Use reasonable security measures to protect consumer request process. | • No Do Not Sell logo or button provided.<br>• Agent issues remain.<br>• Household issues remain.<br>• No guidance on "specific pieces of information". |

| Helpful Clarifications | New Requirements | Issues Not Resolved |
|---|---|---|
| written consent, may still verify consumer.<br>• Clear deadlines for responses; same deadlines apply to Request to Know (RTK) and Request to Delete (RTD).<br>• No obligation to provide specific pieces of information if certain risk.<br>• Backup/archived data exempted from deletion requirements until accessed.<br>• Offers of partial deletion permitted, if full option listed.<br>• Businesses can craft own verification method, but guidelines provided.<br>• Service providers required to refer consumers to businesses and provide info.<br>• Appears to limit obligation to provide household data absent certain verification.<br>• Guidance on access issues for those with disabilities.<br>• Clear statement that denying consumer request under valid statutory exception is not discriminatory.<br>• Clear record retention obligations. | • Explain basis for denial of RTK or RTD.<br>• Notice of financial incentives provided online and offline (in store?).<br>• Must provide two-step deletion mechanism.<br>• Discrimination broad, seems beyond CCPA.<br>• Detailed content to include in privacy policies and initial notices.<br>• Cannot use collected information for non-noticed purpose absent notice and opt-in.<br>• May need to say how to designate agent in policies.<br>• Provide webform and request methods.<br>• Minors 13 less than 16, provide two-step opt-in.<br>• Minors less than 13, verify parent/guardian (hard).<br>• Businesses that collect data from 4+ million consumers have new reporting requirements. | • No guidance on “reasonable security” standard.<br>• No guidance on what it means to ensure consumer has “meaningful understanding”.<br>• No draft regulations on three of seven areas: (1) categories of personal information, (2) unique identifiers and (3) exceptions to the law. |

### A. Initial Notice (§ 999.305)

A business may meet its obligation to provide a consumer initial notice at or before the time of collection by including a link to the section of its privacy policy that contains certain content now required by the Draft Regulations.

Under the Draft Regulations, the initial notice provided to consumers at or before the point of collection must include: (1) a list of the categories of personal information about consumers to be collected; (2) for each category of personal information, the business or commercial purpose for which it will be used; (3) if the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" and (4) a link to the business's privacy policy. In order to use collected personal information for a new purpose that was not disclosed in the initial notice, a business must directly notify the consumer of the new use and obtain "***explicit consent***" from the consumer to use the information for that new purpose. The Draft Regulations do not set forth a standard for how businesses may meet the "explicit consent" requirement.

The Draft Regulations clarify a few points with regard to businesses that do not collect information directly from consumers and the notice they must provide. First, such businesses do not have to provide notice at the point of collection (indeed, how could they?). Second, in order to sell personal information received from other entities, such businesses must either: (1) contact the consumer directly to provide notice of the sale and the consumer's opt-out right or (2) contact the source of the personal information and (a) confirm that the source provided notice to the consumer and (b) get the source to provide a signed attestation that it provided notice to the consumer and a copy of such notice. Attestations must be maintained for two years and must be provided to consumers upon request.

Notice must be accessible to consumers with disabilities, meaning, at the least, it should inform a consumer with a disability how to access the notice or policy in an alternative format. Businesses should keep in mind that website accessibility issues are a burgeoning area of attack in consumer litigation.

### B. Privacy Policies (§ 999.308; § 999.317)

The Draft Regulations specify that a business' notice to consumers and its privacy policy should use plain and straightforward language (avoiding legal jargon), draw consumers' attention and be easily readable (including in a mobile version), be available in languages in which the business typically offers translations of other contracts, be accessible to individuals with disabilities and be visible before data is collected.

Although the CCPA refers only to an "online privacy policy," the Draft Regulations expand the scope of the obligation by defining the policy to cover both online and offline practices.

Included in the provisions is detailed information on what a business should include in its privacy policy. This includes, among many others, a list of the categories of personal information it has collected about consumers in the preceding 12 months, and, for each category of personal information collected: (a) the categories of sources from which that information is collected; (b) the business or commercial purpose for which the information was collected and (c) the categories of third parties with whom

the business shares personal information. A business also has to provide descriptions of consumers' rights, instructions for how to exercise those rights and details of the verification process for the same (including the proof consumers need to submit). Under the Draft Regulations, a business must also provide an explanation of how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf. Other information that must appear in the privacy policy includes contact information for a person to receive complaints and the date the business last updated its privacy policy (which must be done annually).

Significantly, the Draft Regulations impose special reporting requirements on businesses that collect personal information, alone or jointly, of four million or more consumers a year. Those businesses are required to report statistics like how many requests to know or requests to delete are denied, the length of time it takes them to respond and similar information.

### C. Request to Know (RTK) (§§ 999.312–999.313)

The Draft Regulations clarify internal inconsistencies in the CCPA regarding the deadlines within which businesses have to respond to consumer requests to know (RTK). Under the Draft Regulations, the following deadlines apply: (1) within 10 days of receipt, a business must provide acknowledgement of receipt; (2) within 45 days of receipt, a business must provide a response or notice of its intention to delay response and (3) if provided timely notice of delay, within 90 days of receipt, provide a response.

Businesses are prohibited from providing certain information in response to a RTK. A business cannot include certain sensitive information in its responses to consumer requests, including a consumer's social security number, government identification number, financial account number, health insurance or medical identification number, account password or security questions and answers. A business is prohibited from providing specific pieces of information to a consumer if it would create "a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." It is not clear what a business would have to establish to meet this "risk to the security" standard.

### D. Request to Delete (RTD) (§§ 999.312–999.313)

The Draft Regulations clarify a number of issues related to consumers' requests to delete (RTD) personal information. A business has to provide a two-step process to consumers to facilitate RTDs: Step 1, the consumer requests deletion; Step 2, the consumer separately confirms deletion. This is apparently to avoid mistaken deletion requests.

The same response timelines required for RTK apply to RTDs. As noted above, upon receiving a RTD, a business must confirm receipt of the request within 10 days and provide information about how the business will process the request. A business must respond to a RTD within 45 days of the receipt of the request, regardless of the time required to verify it.

Deletion does not have to be all or nothing. A business may offer a consumer the option of only deleting a portion of their personal information so long as it also offers the consumer the option of deleting all of the personal information.

Thankfully, a business does not have to delete personal information from backup or archived systems until it accesses the archived material. This saves businesses hassle and high compliance costs. However, it does require longer-term tracking and follow through.

A business complying with a RTD request must inform the consumer that it has deleted the information, disclose that it will maintain a record of the request and specify the manner in which it deleted the personal information. There are three ways to delete information: (1) by permanently erasing the personal information on its existing systems (with the exception of information on archive or back-up systems); (2) by de-identifying the information or (3) by aggregating the information. A business may choose any of these methods.

### E. Request to Opt-Out (§ 999.306; § 999.315)

Under the Draft Regulations, a business must provide two or more designated methods for consumers submitting requests to opt-out of the sale of their personal information, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information” or “Do Not Sell My Info.” Additional acceptable methods for submitting requests include, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail and user-enabled privacy controls (e.g., browser controls). A business must act on a request to opt-out no later than 15 days from the date it receives the request.

A business cannot ask a consumer who has opted-out to opt back into the sale of their personal information for 12 months after the opt-out. Thereafter, a business has to provide a two-step opt-in mechanism to enable consumers who previously opted-out to opt-in to the sale of their personal information: Step 1, the consumer opt-ins; Step 2, the consumer separately confirms opt-in.[1] A business may offer consumers the option of opting out of the sale of certain categories of personal information only, as long as it also provides consumers the option to opt out of all sales.

A business that does not have a website or that primarily interacts with a consumer offline must still provide an opt-out right and notice of the same. This obligation can be met by printing the notice on relevant paper forms, providing a paper copy of the notice or posting a sign. If the business operates a website, it must provide on any paper form a link to the relevant webform to submit a request and a URL for the business’ online privacy policy.

An agent may submit an opt-out request on a consumer’s behalf if the consumer provided the agent written permission to do so and the agent provides proof of the same. A business may still separately verify the consumer’s identity.

Separate from the authorized agent system, the Draft Regulations permit consumers to make opt-out requests via user-enabled privacy controls like browser controls. This new requirement may have far-ranging effects.

When a consumer opts-out, a business is now required to notify all third parties to which it has sold information about that consumer within the prior 90 days (calculated from the date the business receives the opt-out request) of the consumer’s opt-out request and instruct them not to further sell the information. The business must notify the consumer when this is complete.

The Draft Regulations include new requirements for businesses that choose not to post an opt-out notice. These new requirements deserve careful consideration. First, the Draft Regulations provide that a business is exempt from providing the opt-out notice if it does not and will not sell personal information and it states in its privacy policy that it does not and will not sell personal information. Keep in mind that representations in a privacy policy can be weaponized. Regulators and class action plaintiffs have actively pursued companies for alleged misrepresentations in their privacy policies.

Second, a business that later decides to sell personal information collected during a period when it did not post an opt-out notice must deem all consumers' whose information was collected during that period to have opted-out of the sale of their personal information. This may weigh in favor of posting the opt-out notice under certain circumstances.

### F. Household Requests (§ 999.318)

The Draft Regulations provide a definition of "household" and suggest that a business is not required to comply with a request for specific pieces of information related to a household unless it can individually verify the members. This seems to afford some protections but does not go as far as may be required to ensure at-risk populations are protected. Where a household does not have a password-protected account, a business may respond to an RTK or RTD by providing aggregate household information.

### G. Processing and Responding to Consumer Requests (§ 999.312; § 999.313; § 999.317; § 999.323)

Under the Draft Regulations a business needs to follow several requirements related to the general processing of consumer requests. First, a business needs to maintain records of consumer requests and how it responded to those requests for 24 months. A ticket or log form is okay as long as certain information is included and the information is not used for another purpose.

Second, a business is required to implement "reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information." This provision arguably raises the stakes for businesses in combatting fraudulent requests. The AGO provides no guidance on what may qualify as reasonable security measures.

Third, a business is required to respond to a consumer request even if that request is deficient. The business can either: (1) treat the request as properly submitted or (2) provide the consumer specific instructions on how to properly submit a request. Businesses may want to consider adding form instructions on how to submit requests into their request responses.

### H. Nondiscrimination & Financial Incentives (§§ 999.336 – 999.337)

The nondiscrimination provisions in the Draft Regulations deserve special attention. Among other things, the Draft Regulations require that a business inform consumers of the value of their personal information before the consumers make a decision whether to participate in a financial incentive program. A business may use one of eight approved methods of calculating that value. Businesses should consider if an incentive program is worth the potential costs.

In addition to sheer costs, providing the value of data to consumers gives both regulators and civil litigants the ability to put a number to or otherwise support later claims. Indeed, in its ISOR, the AGO noted that this requirement "increases businesses' accountability to the law by disclosing information necessary for the public and the Attorney General to evaluate whether the financial incentive is in fact reasonably related to the value of the data."

To offer an incentive, a business has to provide notice online or in a "physical location where consumers will see it before opting-in to the financial incentive." Thus, businesses that operate both online and physical locations and that offer entry into incentive programs may have to display certain notices in both locations.

### I. Verification of Requests (§§ 999.323 – 999.325)

The Draft Regulations require a business to establish, document and comply with a "reasonable method for verifying" the identity of the requestor. The good news is that the Draft Regulations appear to grant businesses the flexibility they need to craft their own systems. Less helpful is the suggestion that businesses should generally avoid requesting additional information from the consumer for purpose of verification. That is a general recommendation only, however, and the Draft Regulations do contemplate that additional information may be required. The verification method created is supposed to utilize, where possible, information already in a business' systems or to use a third-party identity verification service. Any additional information obtained for verification can be used only for verification purposes and must be deleted thereafter.

The draft regulations state that the stringency of verification can vary depending on the type of information at stake. The following types of information warrant a more stringent verification process: (1) sensitive or valuable personal information; (2) information that poses a higher risk of harm to consumers if accessed or deleted or (3) information that bad actors are more likely to seek. This makes sense and is in line with recent amendments to the CCPA.

The Draft Regulations require that a business should have a certain degree of certainty as to a consumer's identity before complying with a request. The degree of certainty needed, whether "reasonable" or "a reasonably high" degree of certainty, depends on the type of information sought (e.g., providing specific pieces of information in response to a consumer request requires that a business have a reasonably high degree of certainty). Similarly, a business generally may verify the identity of a consumer wishing to use an authorized agent.

Where a business cannot verify a request, it is still required to take certain actions. If a business cannot verify a RTK for specific pieces of information, for example, it is required to treat the request as if the consumer was seeking the disclosure of the categories of personal information. If a business cannot verify a RTD, the business may deny the RTD but must inform the requestor that their identity cannot be verified and treat the request as a request to opt-out.

### J. Service Provider Issues (§ 999.314)

Issues related to service providers continue to pose special complications for businesses. The Draft Regulations clean up a couple of these issues, while complicating or leaving others unresolved.

The Draft Regulations specifically direct that vendors that provide services to entities that do not qualify as "businesses," but for which the vendor would otherwise be a service provider, fall under the CCPA. This is because the CCPA generally defines "businesses" to be for-profit entities.

The CCPA's definition of "service provider" also suggests that the business collects the personal information and provides it to the service provider. It leaves open the question whether an entity could be a service provider if it collected information on behalf of a business directly from a consumer. The Draft Regulations resolve this issue and provide that an entity that collects information directly from consumers at the direction of a business may be a service provider.

Less helpfully, the Draft Regulations provide that a service provider to one or more businesses may not use personal information collected on behalf of one business to benefit the other businesses. This appears to have been intended to forestall the combination of information from different sources. Doing so would now may fall outside permissible business purposes.

Finally, a service provider may be both a service provider and, for information collected or used outside its role as a service provider, a business subject to the CCPA.

#### K. Children's Information (§§ 999.330 – 999.332)

Children's personal information gets heightened attention under the Draft Regulations. For children under 13, the Draft Regulations require a business to establish, document and comply with a reasonable method of verifying that a person authorizing the sale of the child's personal information is the child's parent or guardian. We note that all the suggested methods of compliance are relatively burdensome and include, among others, requiring the parent or guardian to sign a consent form under penalty of perjury and return the form to the business. For minors who are at least 13 and less than 16 years old, a business is required to obtain consent through a two-step process: Step 1, the consumer opts-in; Step 2, the consumer separately confirms that choice.

Business that "exclusively" target offers directly to consumers under age 16 and do not sell the personal information of those minors without "affirmative authorization" do not need to provide notice of the opt-out right. "Affirmative authorization" here means either the parental or guardian consent process (for children under 13) or the two-step consent process (for children at least 13 and less than 16).

### 3. Issues Outstanding

The Draft Regulations either did not address or left unresolved several meaningful issues. Among other things, the AGO has as yet to release its model "Do Not Sell" button or logo. It is difficult for businesses to come to final operational decisions related to that button or logo without seeing the model. The Draft Regulations also fail to define or provide guidance on various terms like "specific pieces of information," "reasonable security" or "meaningful understanding," which effect businesses obligations under the CCPA or the Draft Regulations. Household requests continue to pose issues even with the new definition. The lack of clarity on these and other issues may hamper ongoing efforts to operationalize the CCPA.

## 4. How to Get Involved

Now is the time for businesses to think through the potential impact of the Draft Regulations on their company and to consider commenting on them. Affected businesses can participate in the rulemaking by providing comments about the regulations to the Attorney General. The comment period will remain open until 5:00 p.m. Pacific Time on December 6. There is a short window in which businesses can work alone or with their peers to try and influence the final CCPA regulations. Impacted business can also testify and provide public comment at the four forums scheduled by the Attorney General across the state. Our CCPA team can help businesses consider the practical impact of the Draft Regulations and consider next steps.

[1] A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction and provide instructions.

akingump.com