

CLIENT ALERT

California Attorney General Releases Proposed Updates to CCPA Regulations

Feb.11.2020

On February 7, 2020, California's Office of the Attorney General (OAG) released proposed revisions to the California Consumer Privacy Act (CCPA) draft regulations of 2019.

The proposed revisions, available [here](#), are substantial and come in response to public comments submitted to the OAG last year. The revisions and a new deadline of February 24, 2020 for additional public comments suggest some sensitivity to concerns raised by industry and policy advocates.

Below is an overview of key proposed revisions that, if adopted, could have a significant impact on companies' compliance efforts. These proposed revisions cover the following topics:

- Definitions
- Notice at Collection of Personal Information
- Notice of Right to Opt-Out of Sale of Personal Information
- Privacy Policies
- Requests to Know and Requests to Delete
- Service Providers
- Special Reporting Requirements

Key Proposed Changes to CCPA Implementing Regulations

I. Definitions

There are a number of proposed revisions to Section 999.301, "Definitions," of the CCPA draft regulations. Highlighted below are key definitions that relate to required consumer disclosures and actions companies must take.

1. **More precise terminology in privacy notices relating to sources of personal information:** The definition of "Categories of sources" from whom personal information is collected has been expanded as follows:

(d) "Categories of sources" means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

2. **Clarity on what a “household” is for purposes of CCPA:** The definition of “Household” has been expanded from people occupying a single dwelling to mean “people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.”
3. **Whether information is personal information depends on the factual circumstances and the technical means at the disposal of businesses:** A new Section 999.302 explains that whether information is “personal information” under CCPA depends on whether the business maintains 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.” For instance, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be “personal information.”

II. Notice to Consumers at Collection of Personal Information:

The new revisions add substantial detail on how businesses may satisfy the core CCPA requirement of providing “Notice at Collection of Personal Information.” Key updates include:

1. **Accessibility:** Clarifying businesses’ obligation to make all notices accessible to disabled consumers. Notices must now be *reasonably* accessible to those with disabilities, with businesses required to “follow generally recognized industry standards, such as Web Content Accessibility Guidelines, version 2.1 as of June 5, 2018, from the World Wide Consortium.”
2. **Mobile app notices:** Describing where to place a notification for a mobile application that collects a users’ information, specifically requiring placing a link on “on the mobile application’s download page and within the application, such as through the application’s settings menu.” The prospect of where to offer the mandated “Notice At or Before Collection” of information is particularly thorny for businesses operating primarily on mobile platforms.
3. **Just-in-time notices:** Adding an additional requirement that businesses present a “just-in-time” notice ahead of any collection of information from a consumer’s mobile device that is for “a purpose that the consumer would not reasonably expect.” The notice must contain a summary of categories of personal information being collected as well as a link to the full “notice at collection”, and cites the example of a flashlight app collecting geolocation data as such an “unexpected” variety of information collected.
4. **No separate purpose disclosure for each category of personal information:** Removing the requirement that “for each category of personal information” the business or commercial purpose(s) of the information’s use be disclosed. That requirement is replaced by a broad requirement to disclose the commercial purpose(s) for the categories of personal information collected generally.
5. **No notice at collection for registered data brokers:** Changing the requirements for businesses that do not collect information directly from consumers such that those businesses do not need to provide a notice at collection to the consumer if they have registered with the Attorney General as data brokers, and included in the registration submission a link to the online privacy policy including instructions on how to submit an opt-out.

III. Notice of Right to Opt-Out of Sale of Personal Information:

The new revisions also include additional information on how businesses that sell personal information are to comply with the requirement to provide a notice of the right to opt-out of the sale of personal information by:

1. **Dropping opt-out disclosure requirements for non-sellers.** If a business does not sell personal information, it may state so in its privacy policy. The proposed revisions explicitly clarify that any business not selling personal information does not need to provide notice of a right to opt-out, just a statement in the relevant privacy policy that it does not sell such information.
2. **Adding an opt-out toggle:** Including, for business that **do** sell personal information, a description of the following authorized opt-out “button or logo” that may be used in addition to the posting of the notice of the right to opt-out.



Businesses may include the above button to the left of the “Do Not Sell My Personal Information” link, and must be the same size as other buttons on the business page. Previous iterations of the proposed regulations and statute itself alluded to an approved “opt-out” button design, but left the actual image for future definition by the OAG.

IV. Privacy Policies:

For privacy policies, the new revisions propose:

No separate disclosure of purposes, third parties, sources for each category of personal information: Removing the requirement that businesses specifically disclose for each category of personal information collected the business or commercial purpose(s) for collecting that category, the categories of third parties with whom it was shared, and the categories of sources from which the category was collected.

Instead, businesses must generally “identify the categories of personal information collected” and the categories “must be described in a manner that provides consumers a meaningful understanding of the information being collected.”

Sellers, however, must still disclose the categories of third parties to whom information was sold or disclosed, for each category of third party.

V. Requests to Know and Requests to Delete:

Concerning consumer requests to know and requests to delete, the revisions propose several crucial clarifications to businesses’ obligations, including the following:

1. **Except for online businesses with a direct user relationship, a toll free number:** Specifying that all businesses must provide two mechanisms for submitting consumer requests, one of which must be a toll-free telephone number, except for businesses that (1) operate exclusively online; and (2) have a direct relationship with the consumer. Those businesses must provide only an email address for the submission of requests.

2. **No two-step process for deletion requests:** Removing the requirement that businesses use a two-step process involving a separate confirmation for online requests to delete. While businesses may do so at the businesses' discretion, mandatory use of the practice is dropped in the proposed revision.
3. **Response deadline clarifications:** Modifying the time limits for businesses to confirm the receipt of requests to know and requests to delete and for responding to those requests. Under the revised regulations, businesses have **10 business days** for the confirmation of such requests and **45 calendar days** to respond, respectively.
4. **No need to search for personal information in certain circumstances:** Proposing a set of four requirements businesses must meet in order to avoid the requirement that they search for personal information upon receiving a request to know or request to delete. Businesses may refrain from responding if:
 - a. The business does not maintain the personal information in a searchable or reasonably accessible format;
 - b. The business maintains the personal information solely for legal or compliance purposes;
 - c. The business does not sell the personal information and does not use it for any commercial purpose; and
 - d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
5. **No need to specify deletion method:** Removing the requirement that businesses inform consumers of the means by which requests to delete were responded to (by permanent erasure, de-identification, or aggregation of the consumer's data). Instead, businesses have an obligation to inform consumers whether a request to delete has been complied with, but not the specific mechanism by which it was done.

VI. Service Providers:

The proposed revisions propose a number of important changes regarding service providers:

1. **Service provider permitted uses of personal information:** Most critically, the revisions offer a list of "permitted uses" of personal information that they receive from businesses in order to provide services, including:
 - Performing the services;
 - To retain and employ another service provider as a subcontractor subject to same limitations;
 - To build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source;
 - To detect data security incidents, or protect against fraudulent or illegal activity;
 - For the purposes given in Section 1798.145(a)(1)-(4), which are to:
 - Comply with federal, state, or local laws;
 - Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
 - Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
 - Exercise or defend legal claims.

Allowing service providers to use information "for internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or

augmenting data acquired from another source” is a major clarification from the earlier proposed regulations and a significant reduction in CCPA risk for many service providers.

2. **Changing service provider obligations regarding requests received:** Service providers that receive requests to know or delete from consumers must either “act on the behalf of the business” or “inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.” Under the proposed revisions, the obligation to inform the denied requestor of the business’ contact information has been removed.

VII: Special Reporting Requirements

The original proposed regulations included annual reporting requirements for any business that “buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers” in a calendar year.

These requirements included an obligation to compile the following metrics annually:

- a. The number of requests to know that the business received, complied with in whole or in part, and denied;
- b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
- c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
- d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

Among other changes, the proposed revisions increase the minimum threshold number from 4,000,000 consumers to 10,000,000 consumers, and require the disclosures be made annually on July 1. This increase should relieve some companies’ obligations because they no longer meet the minimum threshold number of consumers required.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kristin J. Madigan, CIPP/US

Partner – San Francisco

Phone: +1 415.365.7233

Email: kmadigan@crowell.com

Jeffrey L. Poston

Partner – Washington, D.C.

Phone: +1 202.624.2775

Email: jposton@crowell.com

Paul M. Rosen

Partner – Los Angeles, Washington, D.C.

Phone: +1 213.443.5577, +1 202.624.2500

Email: prosen@crowell.com

Jarno Vanto, CIPP/E, CIPP/US

Partner – New York

Phone: +1 212.803.4025

Email: jvanto@crowell.com

Lee Matheson, CIPP/US/E/A, CIPM, PCIP

Associate – Washington, D.C.

Phone: +1 202.654.6728

Email: lmatheson@crowell.com