California Consumer Privacy Act—Still Working Out the Kinks

The California Attorney General issued a second draft of regulations for the California Consumer Privacy Act (CCPA) on February 7, 2020 and issued supplemental draft on February 10, 2020 to address an omission from three days before. The latest iteration of the regulations incorporates public comment received from the original date of issuance in October of 2019, through December 6, 2019, clarifying some of the language from the initial draft but also making several material changes as highlighted below.

- **Clarification is provided for what degree of specificity is required for disclosures of categories.** Specifically, the "Categories of sources" and "Categories of third parties" must be "*described with enough particularity to provide consumers with a meaningful understanding of the type of*" person or entity or third party from or to whom personal information is collected or shared.

- **Guidance is provided that narrows the definition of "personal information."** More specifically, the regulations advise that:

Whether information is "personal information" … 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 example, 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."

This clarification raises questions on what effort would be required by an organization to "reasonably link" an IP address to a consumer or household. It also raises a question on whether businesses may now take the position that certain online and digital advertising activities are not considered a "sale." For example, businesses store data collected from website visitors that they themselves cannot link to any individual (e.g., cookie ID or IP address collected via a tag or pixel employed on their website) – but which they share with analytics and AdTech partners who can. The clarification of whether this data is "personal information" may provide the basis for claiming that no sale occurs by the collecting business because the data shared is not considered to be "personal information."

- **New illustrative examples are provided to help businesses deliver appropriate notices "at the time of collection" of personal data**. The regulations offer examples for what constitutes timely notice for collection of data occurring by telephone, in-person, and mobile applications. Most notably, the guidance clarified that certain mobile application disclosures must be presented in real time. The regulations provide the following example:

When a business collects personal information from a consumer's mobile device for a "purpose that the consumer would not reasonably expect," it shall provide a just-in-time notice containing a summary of the

categories of personal information being collected and a link to the full notice at the time of collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window, when the consumer opens the application on the mobile device.

***Do Not Track (DNT)* is still in effect, but the signals for a *CCPA DNT* still need to be developed.** The updated regulations maintain the requirement to treat DNT-like signals as Do Not Sell (DNS) requests, but recognize that technical steps need to be perfected before this rule can be effectively implemented. The regulations emphasize that signals from user privacy controls must "clearly communicate that a consumer intends to opt-out of the sale of personal information" before they must be treated as DNS requests –yet the regulations also recognize that it is unclear whether any such controls presently exist. The guidance further clarified that these signals must be "global" (e.g., an opt-out cookie placed in a user's browser by one website's cookie management tool may not amount to a DNS signal for other websites.)

- **Service Provider modifications spell out use of customer personal data**. Specifically, service providers may now use customer personal information for internal research and development, with a carve out for certain "high-risk" use cases. The guidance makes it clear a service provider may use customer data to build a better product, provided that use doesn't venture into "building or modifying consumer or household profiles, or cleaning or augmenting data received from another source." The regulations also clarify that a service provider must stop selling data on behalf of a business when a consumer has opted out of the business's sale of their personal information.

- **Loyalty Program administrators receive clarification about what constitutes discrimination of members.** For example, program administrators no longer have to delete the rewards-related personal information of participants who wish to remain in the program but who otherwise want deletion of all their other personal information. This updated guidance allays some previous concerns of organizations with loyalty programs about whether deleting rewards program data - in response to a deletion request (and thus eliminating their rewards) - or not deleting their rewards program data (and effectively treating them differently from non-loyalty members) constituted illegal discrimination under the CCPA. The updated regulations provide that if a loyalty member "submits a request to delete all personal information the business has collected about them, but also informs the business that they want to continue to participate in the loyalty program," the business does not need to also delete the data that is necessary to provide the loyalty program to the consumer.

- **Annual Privacy Notice Disclosures Requirements are Clarified.** Businesses that buy, receive for the business's commercial purposes, sell, or share for commercial purposes, the personal information of over **10 million consumers in a calendar year** must disclose required metrics by July 1 of every calendar year in their privacy policy (or on their website and accessible from a link included in their privacy policy) with some variations depending on how it tracks the data.

- **Clarification is provided for further processing of requests by consumers who cannot be verified.** Specifically, the guidance makes it clear that businesses who sell information may still deny a deletion request when they are unable to verify or authenticate the requestor, but they must also respond by asking the requestor if they wish to opt-out of the sale of their personal information (even if they have not made such request) and provide the requestor with a link to the opt-out.

The deadline to submit written comments to these proposed modifications to the CCPA regulations is February 24, 2020. Michael Best's Privacy & Cybersecurity team will continue to analyze the draft regulations and is available to help you with your questions about how these regulations may impact your business.

Authors

Adrienne Ehrhardt
Partner
asehrhardt@michaelbest.com
T 608.283.0131

Rebecca Gerard
Associate
rlgerard@michaelbest.com
T 312.596.5872

Elizabeth Rogers
Partner
earogers@michaelbest.com
T 512.640.3164

Ryan Sulkin
Partner
rtsulkin@michaelbest.com
T 312.596.5836