Published on *The National Law Review* https://natlawreview.com

Proposed CCPA Regulations: The Attorney General's Expectations for Businesses Subject to the CCPA

Article By:

Michael G. Morgan

Daniel F. Gottlieb

Edward G. Zacharias

On October 10, 2019, the California Attorney General released proposed regulations to implement the California Consumer Privacy Act (CCPA), including substantial new requirements not included in the CCPA. Here we offer a comprehensive summary of the proposed requirements and identify key next steps to address the requirements.

In Depth

On October 10, 2019, California Attorney General Xavier Becerra (Attorney General) released proposed regulations (Proposed Regulations) to implement the California Consumer Privacy Act (CCPA). The Proposed Regulations establish procedures to facilitate consumers' rights under the CCPA. During his press conference announcing the Proposed Regulations, the Attorney General identified four areas of focus in the Proposed Regulations: choice, control, transparency and innovation.

Stakeholders may submit comments to the Attorney General orally or in writing at one of four public hearings or submit written comments to the Attorney General by December 6, 2019, at 5:00 pm Pacific Time.

The Attorney General will amend the Proposed Regulations to reflect the CCPA amendments Governor Gavin Newsom signed into law on October 11, 2019. The Attorney General anticipates issuing final CCPA regulations by the CCPA's July 1, 2020, deadline, at which point the CCPA authorizes the Attorney General to begin enforcing the CCPA and the final regulations.

The Proposed Regulations provide five main components intended to address the four areas of focus: notice to consumers, business practices for handling consumer requests, verification of requests, special rules regarding minors and non-discrimination. Although not final, the Proposed Regulations provide useful direction to businesses seeking to implement CCPA-compliant policies and procedures prior to the January 1, 2020 effective date of the CCPA. The following sections of

this *On the Subject* discuss each major component in more detail and provide our recommended next steps for businesses subject to the CCPA.

Notice to Consumers

The CCPA requires businesses to provide notice to California consumers in several different circumstances. The Proposed Regulations direct businesses on how to provide consumers with the following required notices:

- Notice at or before the collection of personal information;
- Notice of the right to opt out of the sale of personal information;
- Notice of financial incentives (in the context of financial incentive programs); and
- A privacy policy with a comprehensive description of the business's online and offline privacy practices.

Each notice must use plain language that avoids technical or legal jargon, and be in a readable and printable format, available in the languages in which the business ordinarily communicates with others, and accessible to consumers with disabilities. Businesses that handle personal information offline must still comply with notice obligations and may present the various notices in paper form or post prominent signage directing consumers to the web address where the notices can be found.

Notice at Collection. The CCPA requires businesses to give consumers notice of the categories of personal information to be collected and the purposes for which the categories of personal information will be used at or before the collection of personal information. The Proposed Regulations require a business to present this notice in a way that an average consumer will understand, and include the business purpose for the use of the personal information, a "Do Not Sell My Info" link if the business sells personal information, and a link to the business's privacy policy.

Notice of Right to Opt Out. For businesses that sell personal information, the notice of the right to opt out must include a description of consumers' right to opt out of sale of their personal information, a web form by which consumers can submit requests to opt out online, instructions for any other method consumers can use to request to opt out, any proof required when consumers use an agent to exercise the right to opt out, and a link to the business's privacy policy. Notably, the Proposed Regulations would require any business that does not need to provide this notice to affirmatively state that it "does not and will not sell personal information" in its privacy policy.

Notice of Financial Incentive Program. If a business offers consumers compensation for the right to sell personal information or another financial incentive, it must provide a notice to consumers that contains:

- A summary of the financial incentive;
- A description of the material terms of the financial incentive;
- An explanation of how the consumer can opt in or withdraw from the financial incentive; and

- An explanation of why the financial incentive is permitted under the CCPA and does not violate the non-discrimination principles.

Privacy Policy. The CCPA requires a business to maintain a privacy policy that provides consumers a comprehensive description of its online and offline privacy practices. Under the Proposed Regulations, the privacy policy must contain many detailed provisions notifying consumers of, among other things:

- The personal information being collected, disclosed and/or sold about them;
- Their CCPA rights of access, deletion, opt out and non-discrimination;
- If the business does not sell personal information and will accordingly not be providing an opt-out notice, a statement that the business "does not and will not sell personal information";
- How they can designate an agent to make a CCPA request on their behalf; and
- Specific metrics about consumer requests (but only if the business buys, receives or sells the personal information of 4 million California consumers or more).

Business Practices for Handling Consumer Requests

Requests to Know and Delete Personal Information. The Proposed Regulations require businesses to provide certain methods for consumers to submit requests to know (Requests to Know) about the collection, disclosure or sale of their personal information and to delete the personal information. Businesses must provide two or more designated methods for these types of requests, including a toll-free telephone number and a way for consumers to submit requests online. Upon receipt of a Request to Know or delete personal information, businesses must confirm receipt of the request within 10 days and respond to the request within 45 days. The 45-day period begins on the day the business receives the request, not when the business verifies the request. If the business cannot verify the identity of the consumer, the business must inform the individual that it cannot verify the request. If the business denies these requests, it must inform the consumer the basis for the denial. All personal information must be transmitted securely, and all deleted information must be permanently erased, de-identified or aggregated.

If a service provider (processing personal information on behalf of a business) receives and denies a Request to Know or delete from a consumer regarding the personal information, the service provider must inform the consumer to submit the request directly to the business and provide contact information for the business.

When handling Requests to Know or delete household personal information, businesses may respond with respect to aggregate household information, and may only provide or delete specific pieces of household information if the business verifies a request comes from all members of the household.

Requests to Opt Out and Opt Back In. A business must provide two or more designated methods for submitting requests to opt out, including a "Do Not Sell My Info" link on its website homepage or the download or landing page of a mobile application. In addition, the Proposed Regulations require

that businesses treat user-enabled privacy controls that communicate or signal the consumer's choice to opt out of the sale as a valid request to opt out. Requests to opt out do not have to be a verifiable consumer request, but businesses may deny a request they reasonably believe to be fraudulent.

Businesses must comply with requests to opt out within 15 days of the request, and must notify the relevant third parties within 90 days (and then confirm with the consumer) that the personal information will no longer be sold. The Proposed Regulations do not describe how third parties must be notified. Requests to opt back in to the sale of personal information must go through a two-step process where the consumer must clearly state the request to opt in and then separately confirm the choice to opt in.

Training and Record-Keeping. A business must train all its employees and other individuals responsible for handling consumer requests on the requirements of the CCPA and the final regulations. Businesses must also maintain records of consumer requests for at least 24 months. These records cannot be used for any other purpose.

If a business annually buys, receives, sells or shares for commercial purposes the personal information of 4 million or more California consumers, it must comply with additional record-keeping requirements and disclose this information in its privacy policy. The additional records include: the number of Requests to Know and delete it received, complied with and denied; the number of opt-out requests it received, complied with and denied; and the median number of days it took for the business to substantively respond to Requests to Know, delete and opt out.

Verification of Requests

Verification Method Factors. The Proposed Regulations require businesses to establish, document and comply with reasonable methods for verifying that a person making a Request to Know or delete personal information about a consumer is in fact the consumer. In determining the method by which the business will verify the consumer's identity, the Proposed Regulations require the business, whenever feasible, to match the identifying information provided by the consumer to the personal information of the consumer that the business already maintains or use a third-party identity verification service. Businesses must consider the following factors when determining the identity verification method:

- The type, sensitivity and value of the personal information collected;
- The risk of harm to the consumer posed by unauthorized access or deletion;
- The likelihood that fraudulent or malicious actors would seek the personal information;
- whether the personal information the consumer must provide in order to verify their identity is easily spoofed or fabricated;
- The manner in which the business interacts with the consumer; and
- Available technology for verification.

The Proposed Regulations also require businesses to implement reasonable security measures to

detect fraudulent identity-verification activity.

Verification Requirements. If a business maintains a password-protected account with the consumer, it may use existing authentication practices of the account for verification purposes.

If a consumer does not have or cannot access a password-protected account with the business, the business must verify the consumer's identity with varying degrees of certainty, depending on what information is involved in the request. For Requests to Know ***categories*** of information, the business must verify the consumer's identity to a "reasonable degree of certainty," which may include matching at least two data points provided by the consumer with the data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer. For example, the business may request that the consumer provide a credit card's security code and identify a recent purchase made with that card.

For Requests to Know ***specific pieces*** of personal information, the business must verify the consumer's identity with a "reasonably high degree of certainty," which may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the businesses combined with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses must keep these signed declarations as part of their record-keeping obligations.

For requests to delete, the business must consider the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion when deciding between a reasonable degree or reasonably high degree of certainty. In circumstances where the business has no reasonable method to verify the requestor's identity with the required degree of certainty, the business must inform the requestor of this fact and explain why it has no reasonable method to verify the requestor's identity.

When a consumer uses an authorized agent to submit requests, the business may require the consumer to provide the authorized agent with written permission to do so and verify their own identity directly with the business.

Special Rules Regarding Minors

Under 13 Years Old. For minors under 13 years old, a business must establish methods for ensuring that the person affirmatively authorizing the sale of personal information about the minor is indeed the child's parent or guardian. These methods can include:

- Providing a consent form to be signed by the parent or guarding under penalty of perjury;
- Requiring the parent or guardian to use a payment system that notifies the parent (or other payment card holder) after each monetary transaction;
- Having the parent or guardian call a toll-free number or connect via video-conference or connect in person with trained personnel; or
- Checking the parent or guardian's government-issued identification and deleting that identification promptly after verification is complete.

Between 13 and 16 Years Old. Businesses must establish procedures for minors between 13 and 16 years old for them to affirmatively opt in to the sale of their personal information, and also to opt out of such sale. Minors between 13 and 16 years old do not require a parent or guardian to opt in or opt out of the sale of personal information.

Non-Discrimination and Financial Incentive Programs

Businesses may offer financial incentive programs with differences in price or service so long as the difference is reasonably related to the value of the consumer's data, and not because of the consumer's exercise of their privacy rights. The Proposed Regulations provide good-faith methods of calculating and documenting the value of the consumer's data, including, but not limited to, the revenue generated by, or expenses related to, the business from the sale, collection or retention of the consumer's personal information.

Next Steps

Businesses regulated by the CCPA should consider the following next steps in response to the Proposed Regulations:

- The Attorney General invited interested parties to continue providing comments as his office moves to finalize the Regulations. Contact one of the authors of this *On the Subject* or your regular McDermott lawyer if you are interested in submitting comments.

- Businesses uncertain about the applicability of the "sale" opt-out right under the CCPA should evaluate or re-evaluate their position in light of the new requirement that businesses that do not sell personal information expressly state this fact in their privacy policy. This new proposed requirement would materially change the risk analysis under the opt-out right by introducing additional liability for deceptive privacy policy statements.

- The Proposed Regulations' privacy notice provisions add to the existing privacy notice requirements in the CCPA, resulting in a maze of overlapping notice requirements. Businesses should conduct gap analyses with their current privacy notices and begin drafting language that would comply with these new proposed requirements.

- Businesses should continue their data mapping efforts to better understand how their California data is collected, processed, stored and disclosed, which will help facilitate the efforts to comply with rights granted to consumers under the CCPA and the Proposed Regulations.

- The Proposed Regulations provide a framework for businesses to develop consumer request verification procedures in alignment with the specific requirements of both the Proposed Regulations and the businesses' data handling procedures. Businesses should review or begin drafting verification procedures, including the creation of any webpages, telephone services or email accounts that may be needed.

National Law Review, Volume IX, Number 290

Source URL:https://natlawreview.com/article/proposed-ccpa-regulations-attorney-general-s-expectations-businesses-subject-to-ccpa