# PUBLICATION

## California Privacy Regulations Released: Guidance and the Addition of New Requirements

**Authors: Alexander Frank Koskey, III**
**October 14, 2019**

**On October 10, the California Attorney General issued its proposed regulations for the California Consumer Privacy Act (CCPA). The long-anticipated regulations are intended to provide guidance to businesses for how to comply with the CCPA, which has a January 1, 2020 effective date. While the proposed regulations do provide clarification to businesses for implementing consumer rights under the CCPA, the regulations also dictate new requirements not found in the CCPA. Notably, the regulations specify additional detail for what must be included in consumer notices and privacy policies, establish additional security requirements for verifying consumer requests, and require businesses to acknowledge a consumer's browser settings when receiving personal information.**

The written comment period closes on December 6, 2019 at 5:00 pm. The final regulations will be issued in the spring of 2020 and the Attorney General will begin enforcement on July 1, 2020. With just over two months until the CCPA goes into effect, businesses have limited time to react to the proposed regulations. Therefore, it is critical that businesses perform a comprehensive evaluation of their privacy processes, implement protocols for responding to consumer requests, and align privacy functions across multiple departments to ensure compliance with the CCPA. Organizations must understand, this is not just about writing a clear privacy notice; it is about understanding the information created, obtained, and shared as well as operationalizing certain changes to the methods currently being used. The overview below is a "high level" overview and we expect to release additional alerts over the next few weeks; however, as you will note by reviewing the information below, time is of the essence and there are a significant number of tasks businesses will need to undertake quickly.

### Notices to Consumers and Your Privacy Policy

The CCPA requires businesses to issue an initial notice outlining the categories of personal information to be collected from a consumer (Notice at Collection) and a notice of a consumer's right to opt out of the sale of personal information to third parties (Notice of Right to Opt Out of Sale). However, in addition to stating that all notices must use plain language and avoid technical jargon, the proposed regulations go beyond the initial requirements of the CCPA for what is mandated for such notices.

**Notice at Collection.** The Notice at Collection must be provided to the customer at or before the time of collecting any personal information. It must include: (1) a list of the categories of personal information to be collected; (2) the business or commercial purpose for which the personal information will be used; (3) the link to the "Do Not Sell My Personal Information" page; and (4) a link to the business's privacy policy. The addition of a purpose limitation requirement is akin to the European law (General Data Protection Regulation "GDPR") and means that a business may not use personal information for any purpose other than what is disclosed in the Notice at Collection.

**Notice of Right to Opt Out of Sale.** The proposed regulations state that the Notice of Right to Opt Out of Sale must be posted on the webpage, which you are directed to after clicking on the "Do Not Sell My Personal Information" button. The notice must include a description of the consumer's right to opt out of the sale of their personal information by the business along with a form which can be submitted online to opt out. Remember,

the use of the word "sell" does not have the plain meaning it has in everyday language and organizations must make sure they have an understanding of whether their disclosures to third parties could be considered a "sale" as defined by the CCPA.

**Responding to Right to Opt Out Requests.** If a business receives a request to opt out from a consumer, a business is required to act on the request within 15 days from the date of receipt. A business is also required to notify all third parties with which it has sold personal information of the consumer within the previous 90 days of the request to opt out and instruct the third party not to further sell the information. A business is required to notify the consumer when this has been completed. Notably, a request to opt out is the only consumer request that does not have to be a verifiable request.

**New Privacy Policy Requirements.** Privacy policies are about to get a lot longer. Specifically, in identifying each category of personal information that will be collected from a consumer, a privacy policy must also identify the categories of sources from which the information was collected, the business or commercial purpose for which the information was collected, and the categories of third parties with whom the business shares personal information. The privacy policy must also outline the method by which a consumer may designate an authorized agent to make a request on the consumer's behalf. These new requirements will undoubtedly require businesses to review existing policies and evaluate steps for compliance.

**"Do Not Sell My Personal Information" Button.** Unfortunately, the proposed regulations did not provide a sample "Do Not Sell My Personal Information" button to be included on a business's website. The Attorney General noted that a sample button will be added in a modified version of the regulations after public feedback on its design.

**Businesses Must Pay Attention to Browser Settings.** One surprise introduced by the proposed regulations is that a consumer's browser plug-ins and privacy settings can be considered a valid communication for the consumer to exercise its right to opt out of the sale of personal information. There are many unanswered questions concerning this new requirement. Notably, whether a change in the browser settings by the consumer at a later date can serve to reverse a previous decision to opt out. Nonetheless, businesses will now need to recognize such settings form a consumer's device and work to implement methods to avoid the risk of missing a consumer's opt-out designation.

**Exemptions for Businesses Who Do Not Sell.** If a business does not and will not sell personal information, the proposed regulations provide that the business is not required to include a "Do Not Sell My Personal Information" button on its website and does not have to provide a Notice of Right to Opt Out to Consumers. A business claiming the exemption must also state in its privacy policy that it does not and will not sell personal information.

**Opting In After Opting Out**. The CCPA was silent on how a consumer could opt in to the sale of their personal information after previously opting out. The proposed regulations provide for a two-step process where a consumer must clearly submit the request to opt in and then separately confirm the choice to opt in. This is similar to the two-step process for authorizing a Request to Delete.

**Online vs. Offline Distinction.** Although the vast majority of information will be collected from consumers online, the proposed regulations require a business to establish procedures for notice where personal information is collected offline. So, by example, businesses must also now inform customers when obtaining phone numbers or email addresses at a point of sale in a brick and mortar store. This new requirement includes providing notices on printed forms or posting prominent signage directing consumers to a web address where such notices can be found.

## Consumer's Right to Know and Right to Delete Requests

Two of the core principles of the CCPA are a consumer's right to request that a business disclose the personal information the business has about the consumer (Request to Know) and the consumer's right to request deletion of that personal information (Request to Delete). The proposed regulations provide specific details for responding to such requests, the methods which businesses must put in place for receiving such requests, and what information can be disclosed by a business to a consumer.

**Deadlines to Acknowledge and Respond to Requests.** For each Request to Know or Request to Delete received, a business must: (1) confirm receipt of the request from the consumer within ten days of receipt and (2) respond to the request within 45 days from the date the request is received. An additional 45 days to respond is available, for a total of 90 days, but a business must provide notice to the consumer with an explanation for why it will take longer to respond to the request. The tight timeframe to acknowledge these requests makes it imperative that a business develop a process well in advance to comply with this requirement. If a business denies a request, it must inform the consumer that it will not comply and describe the basis for the denial.

**Methods of Submitting Requests.** A business must have at least two methods in place for consumers to submit these requests, one of which must include the method in which the business primarily interacts with the consumer. In most cases, this will involve providing a link or form available through the business's website. Although recent amendments passed by the legislature have eliminated the requirement to have a toll-free telephone number as a method for submitting a request, other acceptance methods include submitting a form in person or through the mail. If a Request to Know is properly submitted and verified, the business must respond based on the personal information collected over the previous 12 months.

**Two-Step Process for Requests to Delete.** A two-step process is required for a Request to Delete. The consumer must submit the request *and* separately confirm that they want their personal information deleted. The additional step of confirmation is intended to prevent any accidental requests from proceeding with irrevocable deletion.

**Not All Information Can Be Provided.** In balancing the consumer's right to know against the potential harm that could result from inappropriate disclosure, the regulations prohibit the disclosure of certain types of information. This includes a consumer's social security number, driver's license or government identification number, financial account numbers, health insurance numbers, account passwords, and/or security questions and answers.

## Verification of Consumer Requests

After much dilemma from the public regarding what would constitute a "verifiable consumer request" under the CCPA, the Attorney General's regulations set forth general verification requirements for businesses. While balancing the potential risk of harm to consumers if information fell into the wrong hands, the proposed regulations introduced new security requirements for verification.

**"Reasonable Method" Standard.** The regulations require that a business shall establish a "reasonable method" for verifying the identity of a person making a Request to Know or Request to Delete. This requires the business to match the information provided by the consumer to the personal information maintained by the business or the use of a third-party identity verification service.

**Factors to Consider for Verification.** In evaluating what is a "reasonable method" for verifying requests, the regulations established various factors to be considered by a business. This includes: (1) the sensitivity of the information requested; (2) the risk of harm to the consumer from unauthorized access or deletion; (3) the likelihood that malicious actors would seek the personal information; and (4) the manner in which the business

generally interacts with the consumer. The regulations highlight that a business should generally avoid requesting additional personal information from the consumer in order to verify the request.

**Use of Authorized Agents.** A consumer is permitted to use an "authorized agent" to submit a Request to Know or Request to Delete on the consumer's behalf. If a business receives a request from an authorized agent, the business may require that the consumer: (1) provide written permission to the authorized agent to make the request and (2) verify their own identity directly with the business.

**Password Protected / Non-Password Protected Accounts.** The proposed regulations streamlined the verification process for password protected accounts stating that a business may verify a consumer's identity through existing authentication practices for the consumer's account. If the request is made from a non-password protected account, then the business is required to verify the identity of the consumer through a "reasonable degree of certainty." For a request for categories of information, this requires a business to match at least two data points provided by the consumer to two data points maintained by a business. For a request for specific pieces of personal information, a business must match three data points and receive a signed declaration that the requestor is the consumer whose personal information is the subject of the request.

**Unverified Requests to Delete Are Considered Requests to Opt Out.** If a business is unable to verify the identity for a Request to Delete, the proposed regulations require that the business deny the request and treat it as a Request to Opt Out of Sale.

## Miscellaneous Provisions

**Consent for Sale of Minor Information.** If a business is collecting personal information from a child under the age of 13, it must receive consent from the child's parent or guardian affirmatively authorizing the sale of that personal information. The regulations set forth various methods for verifying that the person providing the consent is the child's parent or guardian including a consent form, calling a toll-free number, or checking government identification. For children over 13 years old, the business must implement a two-step process to confirm the choice to authorize the sale of personal information. Businesses will need to marry the regulations with current compliance with federal requirements.

**Businesses Must Quantify the Value of Consumer Data.** A business is required to provide a notice to consumers for any financial incentive offered in exchange for the retention or sale of personal information. This is in relation to the CCPA's prohibition on discriminatory practices against a consumer for exercising any rights under the CCPA. Any such notice must include an estimate of the actual value the business places on the consumer's data and a description of the method used by the business to calculate the value of the data.

**Service Provider Confusion.** Contrary to the actual language of the CCPA, the proposed regulations require service providers to respond to consumer requests by providing the specific basis for denying the request. Service providers are also required to direct consumers to submit any requests directly to the business.

**Record-Keeping Requirements.** Businesses are required to retain records of all consumer requests, including all responses by the business to the consumer, for at least 24 months. The record-keeping requirements are more onerous for businesses which buy or sell personal information of four million or more California consumers.

## Conclusion

The Attorney General's regulations have provided the roadmap to businesses for how to comply with the CCPA. However, it will not be an easy road to travel. CCPA compliance continues to be a moving target and the added requirements from the regulations mean that businesses will need to go back to the drawing board to evaluate compliance mechanisms. The Attorney General has implied that, even though his office won't

begin enforcement until July 1, 2020, businesses can be held accountable for noncompliance as of January 1, 2020. Therefore, all businesses which are subject to the CCPA must focus on it immediately to ensure compliance.

For any questions regarding these issues or any other cybersecurity or data privacy-related matters, please contact Alex Koskey or Alisa Chestler.