WILMERHALE

California Attorney General Publishes Long-Awaited Proposed Regulations Implementing the CCPA

OCTOBER 15, 2019

By D. Reed Freeman, Jr., Ali A. Jessani and Lydia Lichlyter

On October 10, 2019, California Attorney General Xavier Becerra (the California AG) proposed regulations and issued an explanatory statement, "Initial Statement of Reasons," aimed at clarifying the scope of the California Consumer Privacy Act (CCPA) and meeting his office's statutorily prescribed requirements. Here are the key takeaways from the proposed regulations.

Key Takeaways

Definitions

- Notable terms used in the CCPA that are defined for the first time in the proposed regulations include "financial incentive," "price or service difference" and "affirmative authorization."
- Some important terms that were undefined in the CCPA continue to remain undefined in the proposed regulations, such as "reasonable security" and "specific pieces of personal information."
- The definition of "categories of third parties" includes advertising networks as an example, making clear that the California Attorney General's Office views online and mobile advertising as falling within the scope of the CCPA.

Notices to Consumers

- The CCPA requires businesses to provide consumers notice regarding their various rights, such as a notice, at or before the point of collection, of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used; a detailed privacy policy; notices of the right to delete personal information and the right to opt out of the "sale" of personal information, as defined; and notice when businesses offer a financial incentive to use a consumer's information.
- The proposed regulations delineate the requirements of each of these notices and would require businesses to implement certain readability and presentation standards.

Handling Consumer Requests

- The CCPA requires businesses to provide two or more methods for consumers to submit requests to know and requests to delete.
- The proposed regulations provide examples of appropriate contact methods that businesses could rely on to comply with this obligation. The proposed regulations also would require businesses to confirm receipt within 10 days of a consumer's request to know or request to delete and provide for a maximum of 90 days to respond to such requests. When responding to a request to delete or opt out of sale, a business would be permitted to give a consumer the ability to delete only some of their personal information or opt out from only some sales, as long as the business also provides the consumer with a more prominent option that would allow the consumer to delete all of their collected personal information or opt out of all sales.

Service Providers

- The CCPA distinguishes between obligations that apply to "businesses" and those that apply to "service providers."
- The proposed regulations clarify that a service provider would not be required to comply with a consumer request under the CCPA. The service provider would, however, be required to explain to the consumer the basis for denying the request, convey that the consumer should submit the request directly to the business on whose behalf the service provider is processing the personal information, and provide the contact information of the business, if possible.

Requests to Opt Out

- The CCPA requires businesses to provide consumers with two or more methods by which they can opt out of the sale of their personal information.
- The proposed regulations would require businesses to consider several factors—such as available technology and ease of use by the average consumer—when determining which methods to offer consumers.
- Under the proposed regulations, businesses would be required to act on a request to opt out as soon as feasible, but no later than 15 days from receiving the request. They would further be required to notify within 90 days all third parties to whom the business has "sold" the consumer's personal information and instruct them not to further sell the information.
- The proposed regulations would also require businesses that collect information online to treat user-enabled privacy controls that communicate or signal the consumer's choice to opt out of the sale of their personal information, such as browser privacy settings, as a valid request to opt out. (This is apparently intended to require businesses to respect "Do Not Track" settings, which are not commonly used because there is no industry standard protocol for handling them.)

Training and Record Keeping

- The CCPA is silent on any training or record-keeping requirements.
- The proposed regulations impose record keeping and training as new requirements under the CCPA. Further, all individuals who handle CCPA requests would, under the proposed regulations, need to be informed as to the CCPA's requirements and how to respond to consumer requests under the law. Also, businesses that collect the personal information of over 4 million consumers would have to compute metrics regarding how quickly and how often they respond to consumer requests and post those metrics in their privacy policies.

Requests to Access or Delete Household Information

- The CCPA explicitly applies to personal information collected from "households."

- Along with defining "household," the proposed regulations clarify that upon receiving a request from a consumer who does not have a password-protected account with the business, the business would only have to provide that consumer with aggregate household information and not with specific pieces of information. If all consumers of a household jointly access specific pieces of information for the household or wish to delete all of the household's personal information and the business can verify the identity of each member of the household, then the business would be required to comply with the request.

Verifying Requests

- The CCPA requires businesses to verify consumers' identity prior to responding to consumer requests but was largely silent as to what specific actions businesses needed to take. The proposed regulations provide some specificity in this regard.
- The proposed regulations would impose general rules that all businesses must follow when verifying consumer requests, and distinguish between consumers who have password-protected accounts with the businesses and those who do not.
- Businesses that have password-protected accounts for consumers would be permitted to use those accounts for consumer authentication when responding to requests, while businesses that do not have password-protected accounts for consumers making requests would be required to employ a risk-based approach depending on the type of request being made and the information under consideration.

Special Rules Regarding Minors

- The CCPA prohibits businesses from selling personal information from consumers under the age of 13 unless the consumer's parent or guardian has affirmatively authorized the sale, and it prohibits businesses from selling personal information from consumers ages 13–16 without receiving affirmative authorization from the consumer.
- Under the proposed regulations, businesses that have actual knowledge that they collect or maintain the personal information of children under the age of 16 would be required to establish, document and comply with a reasonable method for obtaining affirmative authorization either from the parent or guardian of the consumer (if the consumer is under 13) or from the consumer themselves. Businesses that *exclusively* target children under 16 and do not sell their personal information without the necessary affirmative authorization would not need to provide consumers with notice of their right to opt out of sale.

Nondiscrimination

- The CCPA prohibits businesses from discriminating against consumers based on the consumers' exercise of any of their rights under the CCPA, but it allows businesses to provide consumers with financial incentives that are based on the value of the business using the consumer's personal information.

- The proposed regulations provide examples of how businesses would be able to properly provide financial incentives without illegally discriminating against consumers.
- The proposed regulations would also require businesses to document a reasonable and good-faith method for valuing consumer information and provide a list of factors that businesses should consider when making this determination.

Public Comment Period and Public Hearings

- As part of the regulatory process, the California AG's Office has opened a public comment period on the proposed regulations, which will include four public hearings on December 2–5, 2019.
- Written comments must be submitted to the California AG (PrivacyRegulations@doj.ca.gov) on or before 5 p.m. Pacific time on December 6, 2019.

The rest of this alert provides the background behind the California AG's proposed rules and summarizes key parts of the California AG's proposed regulations that businesses should pay particular attention to as they prepare for CCPA compliance.

Background

The CCPA was passed on June 28, 2018. As part of the law's original requirements, the California AG was required to promulgate regulations, on or before July 1, 2020, clarifying various parts of the law. Cal. Civ. Code § 1798.185(a). Specifically, the CCPA required the California AG to promulgate regulations that:

- Updated the categories of "personal information" to address changes to technology, data collection practices, obstacles to implementation and privacy concerns;
- Updated the definition of "unique identifiers" to address changes to technology, data collection practices, obstacles to implementation and privacy concerns;
- Added more categories of designated methods that businesses could provide consumers so that they could access their rights under the law;
- Established any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights;
- Established rules and procedures for how consumers could submit a request to opt out of the sale of their personal information and how businesses could properly respond to such a request;
- Developed a uniform opt-out button or logo that all businesses could use on their websites;

- Established rules and procedures for the various notices required under the CCPA; how a consumer could use an authorized agent to obtain information from a business; and how a business could properly verify a consumer's identity when receiving a request.[1]

The CCPA also allowed the California AG to "adopt additional regulations as necessary to further the purposes of [the law]." Cal. Civ. Code § 1798.185(b). The proposed regulations released by the California AG on October 10, 2019, were intended to meet his office's statutory requirements. Of the aforementioned list, the following are topics that the proposed regulations do not address:

- The definition of "personal information";
- The definition of "unique identifiers"; and
- Additional exceptions to the law.

The rest of the topics listed are addressed by the proposed regulations in some form.2 The California AG's office also developed regulations for topics that it did not explicitly need to address according to statutory mandate, including:

- Training and record-keeping requirements;
- How to calculate the value of a consumer's data;
- How a business can manage a request from a consumer to opt in again after the consumer has chosen to opt out; and
- Additions to the content required in privacy policies.

While the proposed regulations provide some useful guidance regarding potential compliance measures, they also further muddy the waters in many respects and continue to leave important questions unanswered. Nevertheless, businesses looking to ensure they are CCPA-compliant prior to the law's effective date of January 1, 2020, will need to take these proposed regulations into consideration, assuming the final version is substantially similar to the California AG's current proposal, but promulgated after January 1, 2020.

The California AG's office will be holding public hearings regarding the proposed regulations from December 2 to December 5 and has set December 6 as the final date for when public comments can be submitted. The California AG will be able to start enforcing the CCPA six months after the final regulations are issued or on July 1, 2020, whichever is sooner. Cal. Civ. Code § 1798.185(c).

Enforcement actions under the CCPA brought by the California AG can lead to fines as high as $2,500 per violation or $7,500 per intentional violation. Cal. Civ. Code § 1798.155(b). The

[1] The CCPA also requires the California AG to adjust the monetary threshold of what qualifies as a "business" under the law in January of every odd-numbered year to reflect any increase in the Consumer Price Index. Cal. Civ. Code § 1798.185(a)(5).
[2] The California AG has not yet developed a uniform logo regarding the right to opt out but has left a placeholder in the regulations for it to be added in a modified version later. See 11 CCR § 999.306(e).

CCPA also confers on consumers a private right of action if their nonencrypted or nonredacted personal information is subject to a data breach as a result of a business's violation of its duty to implement reasonable security procedures and practices. Cal. Civ. Code § 1798.150(a)(1). Damages under the private right of action can be anywhere between $100 and $750 per consumer per violation or actual damages, whichever is greater. Cal. Civ. Code § 1798.150(a)(1)(A).

Summary of Key Provisions

1. Verification Requests

The CCPA requires businesses to respond to verified consumer requests for information, but it does not provide businesses with guidance as to how to properly verify consumers upon receiving such requests. The proposed regulations would create general standards for all verification requests, but also distinguish between the standards that apply in two scenarios: (1) verification requests from password-protected accounts that consumers already have on file with businesses; and (2) requests that come from consumers without accounts.

Generally, the draft regulations would require that all businesses establish, document and comply with a reasonable method for verifying the identity of a consumer making a verified request under the CCPA. 11 CCR § 999.323(a).

When determining the method by which to verify a consumer's identity regarding a request to know, businesses would need take the following steps:

- **Information matching:** To the extent possible, match the identifying information provided by the consumer to the personal information the business already has on file or use a third-party identity verification service.
- **Do not collect sensitive information to verify a request:** Avoid collecting the categories of information listed in Cal. Civ. Code § 1798.81.5(d), unless they are necessary. These categories are:
    - An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
        - Social Security number;
        - Driver's license number or California identification card number;
        - Account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account;
        - Medical information;
        - Health insurance information; and
    - A username or email address in combination with a password or security question and answer that would permit access to an online account.

- **Watch for spoofed requests:** Take a number of factors into consideration, including the sensitivity of the consumer's information and the likelihood that fraudulent or malicious actors would seek the consumer's personal information. 11 CCR § 999.323(b). The consideration of these factors likely needs to be documented as part of the business's showing that it has developed a "reasonable" verification mechanism.

Verifying Requests From Consumers Who Have a Password-Protected Account:

For password-protected accounts, businesses would be allowed to use existing authentication practices to verify a consumer's identity, though they would be required to ensure that consumers reauthenticate themselves prior to disclosing or deleting a consumer's data. 11 CCR §999.324(a).

Verifying Requests From Consumers Who Do Not Have a Password-Protected Account:

For verification requests received from non-account holders, businesses would, under the proposed regulations, be required to comply with the following rules, depending on the specific request from the consumer:

- **For requests to know categories of personal information:** Businesses would be required to ensure that they can identify the consumer with a *reasonable degree of certainty*, which the regulations define as being able to match two or more data points provided by the consumer with the information the business already has on file. 11 CCR § 999.325(b).
- **For requests to know specific pieces of personal information:** Businesses would be required to ensure that they can identify the consumer with a reasonably high degree of certainty, which the regulations define as being able to match three or more data points provided by the consumer with the information the business already has on file and having the consumer sign a declaration, under the penalty of perjury, that the requester is the consumer whose personal information is the subject of the request. 11 CCR § 999.325(c).
- **For requests to delete:** Businesses would be required to ensure that they can identify the consumer with either a reasonably high degree of certainty or a reasonable degree of certainty, depending on the sensitivity and risk of harm related to the information in question. The regulations provide the deletion of family photographs as an example of when identity should be verified with a reasonably high degree of certainty and the deletion of browser history as an example of when identity should be verified with a reasonable degree of certainty. 11 CCR § 999.325(d).

If there is no reasonable method for a business to verify the consumer's identity with regard to the degree of certainty required, the business would be required to so inform the consumer. If a business is generally unable to verify any consumer's identity with the requisite degree of certainty, then it would have to include this fact in its privacy policy. The business would also be required to evaluate and document on a yearly basis whether it can establish such a verification mechanism. 11 CCR § 999.325(f).

2. Training and Record Keeping

The CCPA itself does not include any training or record-keeping requirements, but the proposed regulations do. This is a significant new requirement borrowed from Europe's General Data Protection Regulation.

Under the proposed regulations, businesses would be required to inform all individuals responsible for handling consumer inquiries about the business's privacy practices and the business's compliance with respect to all the requirements of the CCPA and how to handle consumer requests under the law. 11 CCR § 999.317(a). The regulations would also require all businesses to maintain records for at least 24 months of consumer requests made under the CCPA and how the business responded to such requests. 11 CCR § 999.317(b). These requirements will be significant undertakings for businesses, as they will require new employee trainings, new manuals and additional resources devoted to CCPA compliance. Moreover, the proposed training requirement creates additional risk that businesses may be in violation of the CCPA without enhancing consumer protection. Theoretically, a business could comply with all substantive requirements of the CCPA itself and yet still be liable under the law for failing to properly record its activities.

The proposed regulations create additional requirements for larger businesses. Businesses that collect, share or sell the personal information of more than 4 million consumers would have to establish, document and comply with a training policy that ensures all individuals handling CCPA requests understand the law and how to respond to consumer requests. 11 CCR § 999.317(g)(3). They would also have to compute the following metrics for the previous calendar year and include them in their privacy policy:

- The number of requests to know that the business received, complied with in whole or in part, and denied;
- The number of requests to delete that the business received, complied with in whole or in part, and denied;
- The number of requests to opt out that the business received, complied with in whole or in part, and denied; and
- The median number of days within which the business substantively responded to requests to know, requests to delete and requests to opt out. 11 CCR § 999.317(g)(1).

Again, this further increases the risk that businesses can be deemed to be noncompliant with the CCPA for mere procedural violations.

3. Requests to Access or Delete Household Information

The definition of personal information under the CCPA includes information that could be reasonably linked to a household. Cal. Civ. Code § 1798.140(o)(1). The proposed regulations would clarify how businesses should properly respond to requests to know from households while also protecting individual consumer information. 11 CCR § 999.318(a). They state that when a

business receives a request to know or a request to delete from a consumer who does not have a password-protected account, it may only provide that consumer with aggregate household information and not specific pieces of information about the individual members of the household. If, however, all consumers of a household jointly request access to specific pieces of information for the household or wish to delete all household personal information and the business can individually verify all members of the household, then the business would be required to comply with the request. 11 CCR § 999.318(b).

4. Special Rules Regarding Minors

The CCPA has special rules regarding the right to opt out of sale as it applies to minors. It states that businesses must:

- Obtain affirmative authorization from the parents or guardians of consumers under the age of 13 prior to selling those consumers' personal information to third parties; and
- Obtain affirmative authorization from consumers between the ages of 13 and 16 prior to selling their personal information to third parties. Cal. Civ. Code § 1798.120(c).

The proposed regulations would require businesses that have actual knowledge that they collect or maintain the personal information of children under the age of 16 to establish, document and comply with a reasonable method for obtaining affirmative authorization either from the parent or guardian of the consumer (if the consumer is under 13) or from the consumer themselves. 11 CCR § 999.330(a)(1); 11 CCR § 999.331(a)(1). If a business must comply with this portion of the proposed regulations, then it would be required also to include a description of its compliance mechanism in its privacy policy. 11 CCR § 999.332(a). Businesses that exclusively offer their goods or services to consumers 16 years of age and younger and do not sell consumer personal information without the requisite affirmative authorization would not need to provide consumers with a right to opt out of sale of their personal information, including not needing to include a website link on their home page titled "Do Not Sell My Personal Information." 11 CCR § 999.332(b).

5. Nondiscrimination

The CCPA prohibits businesses from discriminating against consumers for exercising their rights under the CCPA, but allows for businesses to provide financial incentives or different prices or services to consumers for collecting, selling or sharing their information if the incentive or differing price or service is reasonably related to the value of the consumer's data. Cal. Civ. Code § 1798.125. The proposed regulations illustrate this distinction. For example, a music streaming service that offers the right to opt out of sale only to its customers who pay a subscription fee and not to its free customers would be considered to be unlawfully discriminating. On the other hand, if a retail store offers discounts to customers on its mailing list, it would not be considered discriminatory if customers on the mailing list continue to receive discounts even after they have exercised some of their rights under the CCPA. 11 CCR § 999.336(c).

The Initial Statement of Reasons offered by the California AG indicate that this section was intended to allow businesses to continue to offer loyalty programs without

being in violation of the CCPA. That said, it is unclear how this would actually apply in practice. The second example offered by the proposed regulations is a situation where the retail store customer would still receive a mailing list discount after exercising some of their rights under the CCPA. If, however, that retail store customer exercised their right to delete all of the information that the retail store had on file about them or even just the piece of information necessary for them to be informed of the discount (like their email address), then that retail store would no longer be able to provide the discount that customer had received prior to exercising their CCPA right. The proposed regulations do not address whether such a situation would constitute unlawful discrimination.

The proposed regulations also address how a business can calculate the value of consumer data. They would require businesses to establish and document a reasonable and good faith method for assigning value to consumers' information and list a number of factors that businesses may take into consideration when making this determination. 11 CCR § 999.337(b).

Conclusion

The California AG's proposed regulations add many more factors for businesses to consider and operationalize as they prepare for CCPA compliance prior to the law's effective date of January 1, 2020. Some additions, such as the ability to provide consumers with the ability to delete only portions of the information they have on file with a business, are welcomed by business and good for consumers. Other provisions, such as the training and record-keeping requirements, will likely prove onerous to business, and do not necessarily provide consumers with any additional privacy protections.

As a reminder, written comments to the proposed regulations are due December 6, 2019. If you have any questions regarding your CCPA compliance program, please feel free to reach out to any of the listed authors.

For more information on this or other CCPA matters, contact:

D. Reed Freeman, Jr. | +1 202 663 6267 | reed.freeman@wilmerhale.com
Ali A. Jessani | +1 202 663 6105 | ali.jessani@wilmerhale.com
Lydia Lichlyter | +1 202 663 6460 | lydia.lichlyter@wilmerhale.com