Special Alert: California attorney general releases proposed CCPA regulations

October 14, 2019

Last week, the California attorney general released the highly anticipated proposed regulations implementing the California Consumer Privacy Act (CCPA). The CCPA — which was enacted in June 2018 (covered by a Buckley Special Alert), amended several times and with the most recent amendments signed into law on Oct. 11, and is currently set to take effect on Jan. 1, 2020 — directed the California attorney general to issue regulations to further the law's purpose.

The following provides a summary of key points in the proposed regulations:

- **Notice at Collection of Personal Information.** The proposed regulations set forth requirements for the notice at collection of personal information and provide guidance for how to meet this requirement when the information is collected online versus offline. Notably, a business that intends to use a consumer's personal information for a purpose that was not previously disclosed in the notice must directly notify the consumer of this new use and obtain *explicit consent* from the consumer to use it for the new purpose. The regulations also provide specific requirements for a business that does not collect information directly from consumers, but that intends to sell consumers' personal information. Those businesses must either (1) contact the consumer directly to provide notice and a right to opt-out of the sale or (2) contact the source of the personal information to confirm that the source provided the required notice and obtained a signed attestation about the notice.

- **Notice of Right to Opt-Out of Sale of Personal Information.** The proposed regulations provide additional guidance with respect to how businesses should provide the notice of a consumer's right to opt-out of the sale of their personal information. A business that does not sell personal information is exempt from providing a notice of right to opt-out if its privacy policy represents that it does not and will not sell personal information. We note that the attorney general is still designing the sample opt-out button or logo that may be used in addition to posting the notice of right to opt-out.

- **Non-Discrimination.** While the CCPA prohibits a business from discriminating against any consumer for exercising his/her rights under the CCPA, it permits a business to offer (1) financial incentives for the collection, sale, or deletion of personal information and (2) a different price, rate, level, or quality of goods or services to the consumer if that price or difference is "directly related" to the value provided to the consumer by the consumer's data. The proposed regulations provide examples of discriminatory versus non-discriminatory practices, and provide the methods a business must use to calculate the value of the

consumer's data.

- **Notice of Financial Incentive.** The proposed regulations provide guidance regarding how a financial incentive or price or service difference must be explained to the consumer. For example, the notice must include, among other things, an explanation of why the financial incentive or price or service difference is permitted under the CCPA, a good-faith estimate of the value of the consumer's data, and a description of the method the business used to calculate the value of the consumer's data. There are also regulations related to discriminatory practices, including examples of such, and how to calculate the value of consumer data.

- **Privacy Policy**. The proposed regulations provide additional guidance regarding the information that must be included in the CCPA-mandated privacy policy. For example, among other things, the policy must include: (1) instructions and links to the online forms or portals for making verifiable consumer requests to know, to delete, and to opt-out, and (2) the process the business will use to verify the consumer request, including the information that the consumer must provide. Further, a business that buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 4,000,000 or more consumers is required to compile and disclose specific metrics in the privacy policy.

- **Handling Consumer Requests.** The proposed regulations establish methods for how a business must handle the various requests made by consumers. The regulations require businesses to provide two or more designated methods for submitting requests to know and requests to delete, and the businesses must consider how they interact with consumers when determining the methods it will offer consumer for submitting requests. In addition, for deletion requests, there must be a two-step process for online requests to delete where the consumer must: (1) clearly submit the request to delete and (2) separately confirm that the consumer wants their personal information deleted. The proposed regulations also provide separate instructions for businesses that do not interact directly with consumers in its ordinary course of business.

- **Responding to Requests to Know or Delete.** The proposed regulations provide that upon receiving a request to know or delete, the business must confirm receipt of the request and provide the consumer with information on how the business will process the request. Notably, the regulations provide that a business is not required to provide a consumer with specific pieces of personal information if the disclosure creates a "substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." A business is also prohibited from, at any time, disclosing certain enumerated sensitive information, such as a consumer's Social Security number, government-issued identification number, financial account number, or account password. If a business denies a consumer's verified request to know because of an exception to the CCPA, the business must inform the requestor and explain the basis for the denial. For requests to delete, if a business cannot verify the identity of the requestor, the

business may deny the request, inform the requestor that their identity cannot be verified, and must treat the request as a request to opt-out of a sale. A business also may respond to requests for deletion by (1) permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems, (2) de-identifying the personal information, or (3) aggregating the personal information. A business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented.

- **Responding to Requests to Opt-Out**. The proposed regulations provide additional guidance for responding to requests to opt-out, which are not required to be verifiable consumer requests. For example, if a business collects personal information online, the business must treat user-enabled privacy controls (e.g., browser plugins, privacy settings) that communicate a consumer's choice to opt-out as a valid request to opt-out for that browser, device, or consumer (if known). In addition, businesses may present the consumer with the choice to opt-out of certain categories of personal information so long as consumers are offered with a global option to opt-out that is more prominently presented. The regulations also provide that a business must: (1) respond to a request to opt-out no later than 15 days from the date a request is received, (2) notify all third parties to whom it has sold consumer personal information within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information, and (3) notify the consumer when the foregoing has been completed. After a consumer has opted-out, the consumer may request to opt-in to the sale of personal information by way of a two-step process: (1) the consumer must first, clearly request to opt-in, and (2) the consumer must separately confirm their choice to opt-in.

- **Service Providers.** The proposed regulations clarify that a person or entity can be a service provider even if the person or entity provides services to an entity, person, or organization that is not a business. Further, the proposed regulations explicitly prohibit a service provider from using personal information it receives for the purpose of providing services to another person or entity, except that the service provider may combine personal information it receives from one or more entities for which it is a service provider, on behalf of those businesses, to detect security incidents or protect against fraudulent or illegal activity. Entities that may be considered service providers should carefully review the proposed regulations, which provide additional guidance on CCPA compliance.

- **Verifying Consumer Requests.** The proposed regulations require businesses to establish and follow a "reasonable method" for verifying the identity of consumers making requests to know and to delete. The business may consider factors such as, among other things, the type, sensitivity, and value of the personal information collected and maintained to determine the method for verifying identity. While discouraged by the proposed regulations, businesses may request additional information from consumers to verify their identity if it cannot be

established from information already maintained by the business. Any such information must be deleted as soon as practical after processing the request except as required to comply with certain recordkeeping requirements set forth in the proposed regulations. The proposed regulations set forth different standards for verification of non-account holders depending on the requests, ranging from a "reasonable degree of certainty" to a "reasonably high degree of certainty." For example, a "reasonably high degree of certainty" may include matching at least three pieces of personal information that the business had determined to be reliable and obtaining a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request.

Compliance Costs and Commenting on the Proposed Regulations.

The attorney general estimates compliance costs associated with the regulations from 2020 to 2030 will total $467 million to $16,454 million, with compliance costs likely the highest in the first 12 months after the CCPA and regulations take effect. Moreover, the August assessment prepared by a research firm for the California attorney general, estimates the total cost of *initial* compliance with the CCPA will be approximately $55 billion.

The California attorney general will hold four public hearings between Dec. 2 and Dec. 5 on the proposed regulations. Any interested party may submit written comments regarding the proposed comments at a hearing, by mail, or by e-mail. Written comments are due by Dec. 6.

If you have any questions about the CCPA or other related issues, please visit our Privacy, Cyber Risk & Data Security practice page, or contact a Buckley attorney with whom you have worked in the past.