April 30, 2021
Volume XI, Number 120

Login

THE
NATIONAL LAW REVIEW

er Privacy Act Effective January 1: UPDATE

nan & Dicker LLP

Tuesday, December 3, 2019

The California Consumer Privacy Act of 2018 (CCPA) is scheduled to go into effect on January 1, 2020. Applauded by many consumers and privacy advocates, the sweeping legislation places onerous new requirements and

Amendments

On October 11, 2019, California Governor Gavin Newsom signed five CCPA amendments (AB 25, 874, 1146, 1355 and 1564) as well as an amendment to California's data breach law (AB 1130). While noteworthy, these amendments leave most of the core aspects of the law intact. In short:

- AB 25 temporarily excludes employment (and similar) information from many of CCPA's requirements until January 1, 2021, a particularly noteworthy amendment for business-to-business companies that do not otherwise interact with personal information of California consumers. However, the exemption does **not** apply to 1798.100(b), which means that businesses with California resident employees, job applicants, owners, officers, contractors, directors or medical staff members still must provide notice to those California residents that the business is collecting personal information at or before the point of collection, and inform those individuals of the categories of personal information to be collected, why it is being collected, and how it is going to be used. The exemption likewise does **not** apply to the private right of action that CCPA affords to consumers when their personal information is breached, meaning employees will have cause of action against their employers in the event of a data breach.
- AB 874 gets rid of the prior conditions regarding what constitutes "publicly available information" and clarifies that "personal information" does *not* include de-identified or aggregate consumer information.
- AB 1146 exempts from the "right to opt out" vehicle and ownership data retained or shared for the purpose of vehicle repair covered by a vehicle warranty or a recall, and exempts from the "right to request deletion" personal information necessary to fulfill the terms of a written warranty or product recall.
- AB 1355 allows for differential treatment of a consumer that is reasonably related to the value provided to the business by the consumer's data, and clarifies that a business's privacy policy must disclose *the right* to request specific pieces of information in general, and the categories of personal information sold for each *category* of third party, rather than "each third party."
- AB 1564 modifies the methods that a business must make available to consumers for submitting requests to exempt businesses that operate exclusively online from the requirement to maintain a toll-free phone number.
- AB 1130 revises the definition of personal information to include unique biometric data and tax identification numbers, passport numbers, military identification numbers, and unique identification numbers issued on a government document. It also authorizes a notice of a breach involving biometric data to include instructions on how to notify other entities that used the same type of biometric data to no longer rely on the data for authentication purposes.

Proposed Regulations

On October 10, 2019, the California Attorney General released the long-awaited draft regulations for the CCPA. While the proposed regulations provide businesses with some practical guidance on how the Attorney General interprets and will enforce key provisions of the CCPA, they do not provide the clarity many businesses desired. In fact, the regulations also create additional substantive legal requirements, including:

- New disclosure requirements for privacy policies regarding methods for submitting requests to exercise rights under the CCPA
- New disclosure requirements for businesses that collect personal information from more than four million consumers
- Businesses must acknowledge the receipt of consumer requests within 10 days

- Businesses must obtain consumer consent to use personal information for a use not disclosed at the time of collection.

The draft regulations contain five main components, three of which are particularly significant for businesses to ensure compliance with the CCPA: (1) notices to consumers, (2) handling consumer requests and (3) verification requirements. The following provides an overview of the key provisions of the draft regulations.

Notice to Consumers

Article 2 of the draft regulations (pages 3 through 10) provides additional detail regarding certain notices that must be provided to consumers, including notice of the categories of personal information to be collected and the purposes for which it will be used, the right to opt out of sale of personal information, and financial incentives a business may offer in exchange for consumers' personal information.

All notices given to consumers must comply with the following requirements:

- Easy to read and understandable to the average consumer
- Avoid technical or legal jargon
- Be in a noticeable and readable format, including on smaller screens, if applicable
- Be available in all languages in which the business provides contracts, disclaimers, sale announcements and other information to consumers
- Be accessible to consumers with disabilities, or at a minimum provide information on how a consumer with a disability can access the notice in an alternative format
- Include all required information, or a link to the section of the privacy policy that contains the required information.

Notice at Collection Categories of Personal Information Collected and Purpose (§ 998.305).
At or before the time of collection, businesses must inform consumers of the categories of personal information to be collected and the business or commercial purpose for which it will be used. In addition, a business that sells personal information must provide a link titled "Do Not Sell My Personal Information" that links to a notice of the consumer's right to opt out. A business must provide a new notice if it intends to collect additional categories of information not included in the original notice. Going even further, the regulations require a business that plans to use the information for a previously undisclosed purpose to send out a new notice and obtain explicit consent from the consumer to use the information for the new purpose.

Notably, the proposed regulations eliminate a business's obligation to provide notice if the entity does *not* collect information directly from a consumer. However, if a business will resell personal information, it must either contact the consumer directly to provide notice and an opt-out opportunity or contact the source of the information to obtain a signed attestation confirming the source provided a compliant notice and obtain an example of the notice.

Notice of Right to Opt Out of Sale of Personal Information (§ 998.306)

As noted above, a business that sells personal information must provide a "Do Not Sell My Personal Information Link" at or before the time of collection, which leads the consumer to an opt-out notice. The opt-out notice must contain a description of the right to opt out, the webform to be used in submitting a request to opt out, instructions for any other method by which the consumer may submit their request, any proof required when a consumer uses an authorized agent to exercise their right to opt out, and a link to the business's privacy policy. A

Notice of Financial Incentive (§ 998.307)

A business offering a financial incentive in exchange for the retention or sale of a consumer's personal information must provide notice and explain such incentive so that the consumer may make an informed decision on whether to participate. The notice must include a succinct summary of the incentive offered, a description of the material terms of the incentive, an explanation of how the consumer can opt in to the incentive, notification of the consumer's right to withdraw from the incentive at any time and how to exercise that right, and an explanation of why the incentive is permitted by CCPA, *i.e.,* a good-faith estimate of the value of the consumer data to the business, and a description of the method used by the business to calculate the value of the data.

Privacy Policy Content & Format (§ 999.308)

The proposed regulations would permit a privacy policy to substitute for detailed notices mentioned above so long as the privacy policy contains all of the content required for those notices and the relevant portions of the privacy policy are available at the required time for each notice. In any event, the privacy policy must be posted online through a conspicuous link using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application.

The privacy policy must include, among other things, the following information:

- An explanation of the consumer's right to know personal information collected, right to request deletion, right to opt out of sale and right to non-discrimination
- **Instructions for submitting consumer requests for disclosure and deletion, the process for verifying those requests including what information will be required, and how to designate an authorized agent to make such requests on a consumer's behalf (note: these requirements go beyond the text of the CCPA)**
- The categories of personal information the business has collected, disclosed or sold in the prior 12 months, as well as the sources of the information, purposes for collecting it and categories of third parties with which that information is shared
- Statement of whether the business sells the personal information of minors under 16 years of age without affirmative authorization
- A contact for questions or concerns about the privacy polices using a method normally used by the business to interact with consumers
- The date on which the privacy policy was last updated.

As noted above, the proposed regulations introduce privacy disclosures that go beyond those identified in the text of the CCPA. In addition to those emphasized above, another new privacy policy disclosure applies to entities that collect the personal information of four million or more consumers. Such entities must disclose certain metrics concerning the number of consumer requests received and average response time.

Handling Consumer Requests

In Article 3, the proposed regulations provide detailed guidance on how consumers must be able to exercise their rights to know, deletion and opt-out requests, and how businesses must respond to those requests, including two new timing requirements that are not present in the CCPA. This section also introduces obligations for business's training and recordkeeping with respect to consumer requests.

Methods for Submitting Requests (§ 999.312, § 999.315)

Currently, the proposed regulations conflict with one of the newly passed amendments by requiring all businesses to provide a toll-free number. As noted in Section 1 above, AB 1564 exempts businesses that operate exclusively online from the requirement to maintain a toll-free phone number. The proposed amendments almost certainly will be amended to reflect AB 1564. In any event, a business that operates a website must make available to consumers an interactive webform for submitting a request to know.

The proposed regulations further require a business that receives a request to know or deletion via a method that is not one of the designated methods to either treat the request as if it had been submitted in accordance with the business's designated manner or provide the consumer with specific direction on how to submit the request.

For requests to opt out of the sale of personal information, businesses are again required to provide two or more designated methods for submitting requests, including, at a minimum, an "interactive webform" accessible via a "clear and conspicuous link titled 'Do Not Sell My Personal Information,' or 'Do Not Sell My Info'" on its website or mobile application.

Responding to Consumer Requests (§ 999.313, § 999.315)

To start, the proposed regulations introduce several new timing requirements with respect to businesses' response to consumer requests. First, within 10 days of receiving a request for information or deletion, a business must confirm receipt and explain to the consumer the procedures for identity verification and request processing as well as when the consumer can expect to receive a substantive response. Second, a business must respond to a consumer's request to opt out of a sale of personal information within 15 days from date of receipt.

- **Requests to Know.** The proposed regulations address security concerns surrounding responding to a consumer's request to know. For example, if a business is unable to verify a consumer's identity, the business "shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity." Instead, the business must treat the request as a request for categories of information, with its weaker verification standard. Additionally, under the proposed regulations, covered businesses cannot disclose sensitive data - such as Social Security numbers, driver's license or other government ID numbers; financial account numbers; health insurance or medical identification numbers; account passwords or security questions and answers - in their response to a consumer request for specific pieces of personal information.

  The regulations also make clear that businesses must provide an individualized response to requests to know *categories* of personal information collected, categories of sources and/or categories of third parties rather than rely on general statements in the business's privacy policy. However, if its response would be the same for all consumers, the business may refer consumers to the privacy policy, provided that the privacy policy contains all information required to be in a response to a request to know categories of information collected and disclosed.

- **Requests to Delete.** The regulations provide much-needed clarity concerning how a business can respond to deletion requests by allowing a business to choose between one of the following options: (1) permanent erasure from existing systems with the exception of archived or backup systems, (2) de-identification of personal information or (3) aggregation of the personal information. Significantly, the regulations allow a business to delay deleting personal information on archived or backup systems until the system is next accessed or used. A business may deny a consumer's deletion request if it is unable to verify the consumer's identity, although it must inform the consumer of the reason and then, importantly, treat the deletion request as a request to opt out of sale.

- **Requests to Opt Out of Sale.** Most notably, the regulations impose an obligation not found in the CCPA by requiring businesses that sell personal information to forward any opt-out requests to any third parties to

but cannot sell it. The regulations further make clear that an opt-out request need not be a verifiable consumer request, although businesses can refuse to comply with requests if they have a "good faith, reasonable, and documented belief" that the request is fraudulent and inform the requestor of that belief.

If a consumer wishes to opt back in to the sale of personal information, businesses must employ a two-step process whereby the consumer makes an initial opt-in request, then separately confirms the choice.

Service Providers (§ 999.314)

The regulations seemingly contradict the CCPA, which states that service providers do not need to reply to a consumer rights request, by requiring service providers to provide a basis for denying such requests and inform the consumer that it should submit requests directly to the business for which the service provider processes the information. The regulations also clarify that an entity may be a service provider where it is collecting information of consumers as directed by another entity.

Training & Recordkeeping (§ 999.317)

This section outlines specific training and recordkeeping requirements that demonstrate a business's compliance with consumer requests. Specifically, the proposed regulations require that the individuals tasked with handling inquiries related to a business's privacy practice or CCPA compliance be trained in all aspects of the CCPA, including the proposed regulations and how to direct consumers to exercise their rights under the CCPA and regulations.

To demonstrate compliance with the CCPA, the proposed regulations also specify recordkeeping requirements, where required documentation should not be used for any other purpose. Generally, covered businesses must document all CCPA-related consumer requests received and all responses to such requests for at least 24 months. This recordkeeping can be in various formats (including ticket or log form) but must include the following:

- The date of request
- The nature of the request (*e.g.*, know, deletion, opt-out)
- The manner in which the request was made (*e.g.*, in person, online)
- The date of the business's response
- The nature of the response (*e.g.*, complied, denied, partially denied)
- If denied, the reason for denying the request.

Verification of Requests

Perhaps the most helpful guidance of the proposed regulations, Article 4 provides detailed verification guidance for businesses receiving consumer requests under the CCPA.

To begin, Article 4 requires a covered business to develop a written verification plan that documents the methods the business will use to verify the identities of individuals who submit requests to know or delete personal information. Generally speaking, the proposed regulations explain that the rigor of the method for verification should reflect the sensitivity of the information requested. To that end, the proposed regulations provide some general guidelines businesses should consider when implementing verification procedures, including:

- Matching the identifying information provided by the consumer to the personal information already maintained by the business where feasible, and avoid collecting new personal information during the verification process

to the consumer from unauthorized access or deletion, or likelihood that the request is fraudulent or malicious.

Verification for Password-Protected Accounts (§ 998.324)

Where a business maintains a password-protected account with the consumer, the proposed regulations allow the business to verify the consumer's identity through the business's existing authentication practices for the consumer's account, but must require the consumer to re-authenticate themselves in another manner consistent with the type, sensitivity and value of the information to the consumer. However, if the business suspects fraudulent activity, it must require additional verification.

Verification for Non-accountholders (§ 998.325)

- **Requests to Know.** The regulations provide that a more rigorous verification process should apply to more sensitive information. That is, businesses should not release sensitive information without being highly certain about the identity of the individual requesting the information. For example, verification procedures for requests to know *categories* of personal information need obtain only a "reasonable degree of certainty," which "may include matching at least two data points provided by a consumer" with reliable data points maintained by the business.

  Requests for *specific pieces* of personal information, on the other hand, require businesses to verify the identity of the consumer with a "reasonably high degree of certainty." The regulations provide an example of what may constitute a "reasonably high degree of certainty": (a) matching three pieces of personal information provided by the consumer with personal information maintained by the business, along with (b) obtaining a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. (Businesses are to maintain all such signed declarations as part of their recordkeeping responsibilities.)

- **Requests to Delete.** For deletion requests, businesses are to use either a "reasonable" or "high" degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by any unauthorized deletion. As an example, the regulations explain that a request to delete family photographs would require a "high" level of certainty, as opposed to a request to delete browsing history, which would require a "reasonable" level of certainty.

  Where a business concludes that there is "no reasonable method" by which it can verify the identity of the consumer to the degree of certainty required, the business must say so in response to the request. If the business will never have a reasonable method to verify consumer requests, it must explain why it has no reasonable method by which it can verify the identity of the requestor in its privacy policy. Meaning, if a business only collects certain limited technical information about site visitors and it is unable to match such information to particular individual consumers, it may state so in its privacy policy and in response to consumer requests under the CCPA. The business must revisit this conclusion on a yearly basis.

- **Authorized Agents.** The regulations do not provide detailed guidance on levels of verification required from authorized agents. Rather, absent the agent having a valid proof of attorney, the regulations simply state that a business may require a consumer to verify their identity directly with the business, even when it wants to use an authorized agent. Businesses can further require agents to present written proof of authorization and may deny the agent's request if they fail to do so.

Key Takeaways

businesses should begin comparing their current compliance programs against the proposed regulations and five amendments to determine whether their programs are in compliance with CCPA requirements, or if updates are needed. Most notably, businesses without a written verification procedure or CCPA-specific training policies must evaluate the procedures and training necessary under the attorney general's guidance, and begin drafting compliant policies and procedures that can be adjusted and adapted easily as the CCPA remains in flux.

The regulations are not final. The attorney general scheduled public hearings on December 2 (Sacramento), December 3 (Los Angeles), December 4 (San Francisco) and December 5 (Fresno) to hear comments. Written comments will be accepted by the attorney general until 5:00 p.m. PT on December 6, 2019. Interested parties may submit written comments via email to PrivacyRegulations@doj.ca.gov or by mail to Privacy Regulations Coordinator, California Office of the Attorney General, 300 South Spring Street, First Floor, Los Angeles, CA 90013.

The final regulations are expected to be released in early 2020 and will be enforced by the Office of the Attorney General beginning in July 2020.

National Law Review, Volume IX, Number 337

TRENDING LEGAL ANALYSIS

5 Ways Lawyers Can Help Car Accident Victims
By Bader Scott Injury Lawyers

Health Care Employers: Whistleblowing, Retaliation Risks Are On the Rise – Diagnosing Health Care [PODCAST]
By Epstein Becker & Green, P.C.