Privacy Alert
November 2020

California Privacy Rights: New Amendments, New Regulations, No Signs of Slowing Down

California continues to lead the charge for privacy rights in the United States and shows no signs of slowing down. From the new California Consumer Privacy Act (CCPA) regulations proposed by the attorney general in September to the approval of Proposition 24, the California Privacy Rights Act (CPRA), by California voters, business should expect the trend of new obligations and clarifications to continue at least through the CPRA's effective date of Jan. 1, 2023.

Key Takeaways

- The CPRA's creation of a California Privacy Protection Agency will likely lead to increased enforcement, and the elimination of the 30-day cure period may result in increased fines.
- New rights to limit the use of "sensitive personal information" and to opt out of sharing will require back-end and front-end updates to current compliance programs.
- The prospect of further rulemaking will make it hard for companies to take significant steps toward compliance, as the CCPA rulemaking experience has demonstrated the potential for rulemaking to create significant changes.
- Business-friendly provisions, including the extension of exemptions for employee and business-to-business data and the increased threshold for businesses, provide a silver lining to the prospect of two more years of change and uncertainty.

CPRA: New Definitions, Rights and Obligations

The CPRA amends the CCPA to include new definitions, GDPR-like principles and rights, and additional obligations for businesses that remain in scope.

Change in Scope

- **Definition of "business."** Under the CPRA, in order to be considered a "business," for-profit entities must annually process the personal information of 100,000 California consumers or households (instead of 50,000 California consumers, devices or households under the CCPA), or meet one of the other threshold requirements, which remain unchanged (i.e., $25 million in annual revenue; 50% of annual revenue derived from selling consumers' personal information).
- **Employee and business-to-business exemptions.** The CCPA provided two exemptions for employee and business-to-business data, which will sunset Jan. 1, 2021. The CPRA extends these exemptions for two more years until Jan. 1, 2023.

Attorney Advertising

New Consumer Rights Not Provided Under the Current Law

- **Right to correction.** The CPRA requires businesses to use commercially reasonable efforts to correct inaccurate personal information in response to a verifiable consumer request.
- **Right to limit use/disclosure of sensitive personal information.** The CPRA establishes a new category of sensitive personal information and gives consumers the power to restrict the use of it. Sensitive personal information includes Social Security number, driver's license number, passport number, financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information about sex life or sexual orientation. Specifically, consumers can direct a business to use/share sensitive personal information only for purposes necessary to perform the service or provide the goods requested (subject to limited exceptions, including for the collection or processing of sensitive personal information for security purposes, nonpersonalized (i.e., contextual) advertising, maintaining/servicing accounts, and undertaking activities to verify/maintain the quality of a service).
- **Right to opt out of sharing of personal information for cross-contextual behavioral advertising purposes.** The CPRA expands the opt-out right to include not only "sales" of personal information but also the "sharing" of personal information (which is defined as the transfer or making available of "a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration"). "Cross-contextual behavioral advertising" includes targeted advertising based on prior browsing activity (commonly known as behavioral advertising or interest-based advertising). This differs from the CCPA, as the CCPA does not limit behavioral advertising if it can be done without "selling" personal information. Businesses will need to explain these concepts to consumers.
- **Expanded right to access.** Under the existing CCPA right to access, California consumers can request access to all categories of personal information collected by companies over the previous 12 months. The CPRA will extend that 12-month window indefinitely (beginning Jan. 1, 2022), requiring that businesses provide access to all categories of personal information collected "unless doing so proves impossible or would involve a disproportionate effort."
- **Transparency and opt-out of automated decision-making.** The CPRA directs the California attorney general to develop regulations requiring transparency and opt-out rights for certain automated decision-making and profiling. The CPRA defines profiling as "any form of automated processing of personal information … to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."
- **New exceptions to rights related to deletion.** In addition to the existing exceptions, businesses are not required to comply with a consumer's request to delete if it is reasonably necessary for the business, service provider or contractor to maintain the consumer's personal information in order to fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or help ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary for and proportionate to those purposes.
- **New exception to rights related to access to specific pieces of information.** If the specific pieces of information are data generated by the business to help ensure security or integrity, the business is not required to provide this data in the context of a request for access.

New Obligations for Businesses

- **Increased transparency/notice requirements.** In addition to the transparency requirements set out in the CCPA, the CPRA would require businesses to provide the following information "at or before the point of collection": the categories of sensitive personal information collected and whether they are sold or shared, and the length of time the business intends to retain each category of personal information/sensitive personal information (or, if that is not possible, the criteria that would be used to determine the retention period).

- **Website links.** Businesses will need to update the "Do Not Sell My Personal Information" links to read "Do Not Sell or Share My Personal Information," and a separate link titled "Limit the Use of My Sensitive Personal Information" will also be required. The CPRA does permit a single link if it takes the consumer to a webpage allowing the consumer to both opt out of the sale/sharing of personal information and limit the use of sensitive personal information. Note: a business does not need to provide the links if it complies with automated opt-out signals sent from browsers or other extensions.
- **Loyalty and rewards programs.** The CPRA clarifies that a business is not prohibited from offering loyalty, rewards, premium features, discounts or club card programs. Under the CCPA, a consumer is required to opt in to a financial incentive program. The CPRA imposes a 12-month moratorium on businesses from requesting opt-in consent after a consumer refuses to opt in to a financial incentive program.
- **Collection and purpose limitation.** The CPRA prohibits businesses from collecting more information than needed and from retaining personal information/sensitive personal information for longer than reasonably necessary for the disclosed purpose of collection.
- **Possible risk assessments and audits.** The CPRA directs the California attorney general to issue regulations requiring businesses whose processing presents significant risks to consumer privacy and security (i.e., those that are engaged in "high-risk processing" activities) to perform an annual security audit and submit regular risk assessments to the California Privacy Protection Agency (the new privacy agency established by the CPRA).

Additional Obligations: Third Parties, Service Providers and Contractors

- **New contract requirements**. The CPRA requires that contracts that businesses enter into with third parties, service providers and contractors (a new category of person that receives personal information for specific business purposes) (1) state that personal information is sold or disclosed for limited and specified purposes; (2) require the third party, service provider or contractor to comply with the CPRA and provide at least the level of privacy protection required by the CPRA (and notify the business if it cannot); and (3) allow the business to "take reasonable and appropriate steps" to ensure that the use of personal information by the third party, service provider, or contractor is consistent with the CPRA and to remediate unauthorized uses. The CCPA does not mandate these contractual terms.
- **Direct obligations on service providers and contractors.** The CPRA requires service providers and contractors to assist businesses with their CCPA obligations (including the obligation to comply with consumer rights requests, subject to certain exceptions). Service providers and contractors would also be required to alert businesses when they engage sub-processors and to enter into contracts with those sub-processors that impose the same restrictions that are imposed on the service provider or contractor.

Enforcement and Liability

- **New enforcement agency.** The CPRA creates the California Privacy Protection Agency, an agency dedicated to implementing and enforcing the law by investigating violations and imposing fines. The new enforcement agency would be responsible for rulemaking and would also have the right to audit businesses for compliance with the CPRA.
- **Expanded private right of action.** In addition to the private right of action for breaches of nonencrypted, nonredacted personal information under the CCPA, the CPRA adds a private right of action for unauthorized access or disclosure of an email address and password or security question that would permit access to an account if the business failed to maintain reasonable security.
- **Modified cure period.** The CPRA removes the 30-day cure for general privacy violations of the law, allowing immediate enforcement by the attorney general. The 30-day cure period remains for private rights of action for security breach violations.
- **Limitation of liability.** Businesses are afforded a limitation of liability for violations of the law by service providers, contractors and third parties, with certain conditions.
- **Fines involving children's personal information are tripled.**

What's Next?

- Nov. 11, 2020: Certification of the vote.
- Dec. 2020 – Jan. 2021: Funding and establishment of the California privacy protection agency.
- 2021 – July 1, 2022: CPRA rulemaking (*final regulations must be adopted by July 1, 2022).
- Jan. 1, 2022: Lookback window begins.
- Jan. 1, 2023: CPRA becomes operative.
- July 1, 2023: CPRA enforcement begins.

What Else Should You Watch For?

Last month, the California attorney general released a third round of proposed modifications to the CCPA regulations. The Oct. 12 revisions make substantive changes including adding offline consumer notice requirement, detailing examples of opt-out methods, clarifying the use of authorized agents and amending the notice required based on the ages of children whose information is being collected. Comments were due by Oct. 28, and the regulations will likely go into effect early next year.

The return of offline notice. Businesses that sell personal information are required to provide notice of consumers' right to opt out. The final implementing regulations on Aug. 14 did not include a provision (formerly 999.306 (b)(2)) that required "business[es] that substantially interact[] with consumers offline" to provide notice "by an offline method that facilitates consumer awareness of their right to opt-out." The withdrawn provision listed some examples of acceptable methods, including printing the notice on paper forms used to collect personal information, providing a paper copy of the notice, and posting signs directing consumers to online notices. The removal of former Subdivision (b)(2) was widely seen as giving brick-and-mortar businesses more flexibility to satisfy the notice requirements, including by using online notices. The regulations also provide that businesses that don't operate websites "shall establish, document, and comply with another method by which [they] inform[] consumers of their right to opt-out" that meets the requirements for accessibility, readability and ease of understanding in Subdivision (a)(2).

The proposed amendments add back the requirement that "businesses that collect personal information in the course of interacting with consumers offline" provide notice of consumers' right to opt out. New Subdivision (b)(3) requires that the method of providing notice must be "an offline method that facilitates consumers' awareness of their right to opt-out." The subdivision also provides illustrative examples, including the examples previously included in the withdrawn section, and adds that businesses that collect personal information over the phone "may provide the notice orally during the call where the information is collected."

Easy opt-out procedures. The proposed changes add Subdivision (h) to Section 999.315, governing requests to opt out, requiring that methods for submitting opt-out requests "be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out." This language is in line with the CPRA's restrictions on the use of "dark patterns."

The illustrative examples caution against using confusing language and double negatives; requiring consumers "to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out" or to click through reasons not to opt out; and asking for personal information that is not necessary to implement the opt-out request. Specifically, the opt-out process "shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out."

Authorized agents. Proposed Section 999.326, Subdivision (a) clarifies that businesses interacting with authorized agents may require the agent, rather than the consumer, to provide proof that the consumer gave the agent permission to submit the request. While the proposal shifts the onus for establishing agency to the authorized agent, the businesses may still ask consumers to either directly verify their own identity or directly confirm that they provided the authorized agent permission to submit the request. Businesses may no longer require consumers to give the authorized agent written permission.

Notice regarding children. A proposed amendment to Section 999.332 provides that notice must be given to consumers if a business is subject to either Section 999.330 (Rules Regarding Consumers Under 13 Years of Age) or Section 999.331 (Rules Regarding Consumers 13 to 15 Years of Age), or both of these sections. Currently, the regulation applies only to businesses subject to both sections.

Related Professionals

Jessica B. Lee . . . . . jlee@loeb.com
Susan E. Israel . . . . . sisrael@loeb.com

6517 REV1 12-01-2020