CCPA 2.0 May Be Heading to California's November 2020 Ballot: What Employers Need to Know

Insights
5.20.20

In 2018, the California legislature enacted the California Consumer Privacy Act ("CCPA"), which went into effect on January 1, 2020 but was amended six times before it even took effect. Concerned that amendments have weakened the CCPA and that consumers still do not understand how their personal information is being used by businesses, proponents of the CCPA have proposed a ballot initiative for the November 2020 ballot titled the California Privacy Rights Act of 2020 ("CPRA")—colloquially known as CCPA 2.0.

The CPRA currently has over 930,000 signatures which are pending signature verification. The California Secretary of State needs to confirm 623,212 valid signatures for the initiative to qualify for the November 2020 ballot. The CPRA can continue to be circulated for additional signatures until June 15, 2020. While a limited sampling of signatures thus far shows only 75% of signatures are actually valid, this percentage would still be sufficient to meet the threshold to get the CPRA on this fall's ballot.

While this blog post discusses the CCPA and CPRA as though they are two separate laws, the CPRA would amend the CCPA rather than be a completely separate law. If the CPRA passes, businesses would need to re-evaluate whether the CPRA (and CCPA) still applies to them under adjusted criteria. Businesses that are currently compliant with the CCPA will need to evaluate what steps they need to take to be ready for the CPRA.

CPRA Would Change the Criteria for Covered Businesses
Currently, the CCPA applies to for-profit businesses that (a) do business in California, (b) collect the personal information of consumers (including employees), and (c) satisfy any one of three additional criteria. The CPRA would tweak those additional criteria:

- Changes to Criterion 1: The CPRA clarifies that the criterion of a business having a gross annual revenue in excess of $25 million is based on the annual gross revenue as of January 1 of the prior calendar year. This provides some clarification to businesses near that threshold who were unclear on how to determine if the CCPA applied to them. It also potentially creates a loophole in which businesses in their first year of operation will not have the CPRA apply to them.
- Changes to Criterion 2: The business alone or in combination annually buys, sells, or shares the personal information of 100,000 or more consumers or households. This doubles the threshold

of consumers or households from the CCPA to determine whether a business would qualify under this criterion, while also no longer including devices along with consumers or households. Devices was a problematic consideration when a single person can own multiple devices (such as a smart phone and a computer), meaning that a person or household could be counted multiple times to meet the threshold number.

- Changes to Criterion 3: The CPRA now includes businesses that derive 50% or more of their annual revenues from selling or sharing consumer personal information—the CCPA only included selling personal information.

"Sharing" is one of the recurring changes made by the CPRA. Like selling under the CCPA, sharing is a term of art that is not used in the commonly understood sense. Sharing applies to sharing information for "cross-context behavioral advertising" (i.e., targeted advertising), whether or not for monetary or other valuable consideration.

In addition, the CPRA—like the CCPA—would apply to businesses (including non-profit businesses) that are controlled by and share common branding with a covered business. Where the CPRA expands on the CCPA is that the controlled or controlling entity must also share consumers' personal information—a requirement which does not exist in the CCPA.

The CPRA further adds in two new potential covered business. First, joint ventures or partnerships composed of businesses in which each business has at least a 40% interest. Second, a person that does business in California and is not otherwise covered by the CPRA can voluntarily certify to the California Privacy Protection Agency (a new agency which would be created under the CPRA and is discussed below) that it is in compliance with the CPRA and agrees to be bound by the CPRA.

When Would Businesses Have to Comply with the CPRA?

The CPRA contains good news and bad news for employers. The good news: an exemption in the CPRA for employers would go into effect before the CCPA exemption for employers is scheduled to end on January 1, 2021. This exemption would apply to all provisions of the CPRA except for (1) disclosure of the categories of personal information collected about employees and job applicants and the business purposes for which the information is used and (2) the need to take reasonable security measures to protect applicant and employee personal information. These two exceptions already exist under the CCPA although, as will be discussed below, the CPRA would tweak the information necessary to be included in the disclosure notice. As such, even currently CCPA-compliant employers would need to update their disclosure notices.

The bad news: this exemption has a sunset date of January 1, 2023, which is hardly the permanent reprieve that employers were hoping for.

Further bad news for employers: like the CCPA, this exemption applies only to the extent that the person's information is used by the business "solely within the context of" that person's role within the business, having an emergency contact on file, or administering benefits. While at first blush

this would seem broad, it leaves open the door that information collected could be outside of the exemptions and thus subject to all the provisions of the CCPA. For example, would information collected about employees to further a business's objectives in hiring a diverse workforce be solely within the context of an employee's role within the business and thus subject to this exemption? Employers cannot know for sure, and they will need to wait and see what the regulations promulgated by the Attorney General say on issues like this.

For businesses wanting to know about when the CPRA becomes operative outside of the employment context, the CPRA becomes operative on January 1, 2023 (like for employers) and applies to personal information collected by a business on or after January 1, 2022. Some provisions of the CPRA are slated to become operative sooner, but they do not affect businesses' compliance obligations. This would give businesses a little over a year to prepare for the changes that would be required under the CPRA. This would not excuse businesses with complying with the CCPA until the CPRA becomes operative.

The CPRA Would Create Additional Protections for Sensitive Personal Information

The CCPA has a broad definition of personal information that potentially covers all information that employers collect, maintain, or share about job applicants, employees, and their family members or household. The CPRA creates a separate category for "sensitive personal information," many of the categories of information which may be contained in an employee's personnel file, medical file (including FMLA/CFRA documentation), or in other documentation that employers maintain. These categories include:

- Personal information that reveals a consumer's social security, driver's license, state identification card, or passport number;
- A consumer's precise geolocation;
- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, e-mail, or text messages, unless the business is the intended recipient of the communication;
- A consumer's genetic data;
- The processing of biometric information for the purpose of uniquely identifying an employee;
- Personal information collected and analyzed concerning a consumer's health;
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Sensitive personal information that is publicly available is not considered sensitive information under the CPRA.

The CPRA would create additional rights for consumers to limit the use and disclosure of such personal information. Consumers would have the right to direct a business to limit its use of

collected sensitive personal information to that necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services, or to perform specific other services authorized by the CPRA. In other words, unlike for other personal information collected, consumers are not limited to the two options of either allowing the business to proceed with how it uses the personal information or delete the personal information—there is now a third option.

The CPRA Would Create Additional Limitations on Collection and Use of Personal Information, Including Sensitive Personal Information

Under the CPRA, businesses would need to provide notice to consumers of both the categories of personal information and sensitive personal information collected and the purposes for which they are collected or used. Businesses would need to carefully consider the business purposes included in the notice: **businesses would be barred from retaining personal information or sensitive personal information for longer than is necessary for the disclosed purposes**.

To that end, businesses will need to consider carefully the purposes they list in the notice and ensure that they consider any statutes of limitations for claims that may be brought by consumers. Employers in particular will want to be mindful of ensuring that they retain employee information that might be necessary to defend against lawsuits that may be brought by current or former employees. While the statute of limitations is the last day a lawsuit can be filed, a business may not receive notice of the lawsuit until after that date. In the disclosure statement, businesses need to state the length of time they intend to retain each category of personal information or sensitive personal information. They can, if a specific time limit is not possible to ascertain, list the criteria used to determine such period. Employers would likely want to use criteria rather than a defined retention period.

The CPRA would also create a proportionality requirement: the collection, use, retention, and sharing of a consumer's personal information must be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected . . ." Businesses would need to be aware of what information they are collecting and be able to justify the use and collection of that information.

Additionally, the CPRA would create a requirement that businesses inform consumers which categories of personal information or sensitive information are being sold or shared—something that is not required under the CCPA. The CPRA would also allow consumers to opt out of the sharing of their personal information, in addition to opting out of the selling of personal information already permitted under the CCPA.

The CPRA Would Create New Requirements on Businesses' Relationships with Third-Parties

Under the CPRA, businesses that collect a consumer's personal information and sell that personal information, share it with a third-party, or disclose it to a service provider or contractor would need to modify their agreements with those third-parties to meet additional requirements under the

CPRA. While employers are unlikely to be selling employee information, many employers disclose employee personal information and sensitive personal information when they use service providers for functions such as payroll, human resources, and benefits administration.

Some of the contractual requirements are sure to create future headaches for employers. Specifically, one provision grants businesses the rights to take reasonable and appropriate steps to help ensure that third-party services providers, or contractors use personal information in a manner consistent with the business's obligations. Since businesses have that right, that leaves open the question of whether businesses could be liable under the CPRA for not exercising that right—and what constitutes reasonable and appropriate steps.

However, other changes to the CPRA would be sure to be a boon to businesses that are concerned about how to ensure their service providers assist them in complying with their CCPA obligations. Service providers now must cooperate with businesses in responding to verifiable consumer requests to delete personal information. This includes that such service providers (and any other third-parties to whom personal information has been sold or shared) must delete—and direct their own service providers and contractors to delete—personal information.

The CPRA Would Create a Right for Consumers to Correct Inaccurate Personal Information

The CPRA would give consumers the right to request that a business that maintains inaccurate information about the consumer correct such information upon a verifiable request. This change is likely to be of concern to employers, as employees may attempt to use this section to change negative performance evaluations and remove discipline from their personnel files. The particulars of how consumers can request corrections, including exceptions for requests to which a response is impossible or would involve a disproportionate effort and how concerns regarding the accuracy of the information may be resolved, will be left to the Attorney General to resolve through the adoption of regulations.

The CPRA Would Create a California Privacy Protection Agency

The California Privacy Protection Agency would have the authority to investigate any violations of the CPRA, including the right to investigate possible violations on its own initiative even in the absence of a complaint. If the California Privacy Protection Agency were to decide that there was probably cause that a violation of the CPRA occurred, it would be able to hold hearings, subpoena witnesses and take evidence, bring administrative actions, and assess administrative fines. The California Privacy Protection Agency would have five years to bring an action.

Once established, the California Privacy Protection Agency would also assume rule making responsibility from the Attorney General.

Additional Odds and Ends Businesses Need to Know About the CPRA

The CPRA contains several additional provisions that businesses should be aware of. First, the CPRA defines consent to be an "informed and unambiguous indication of a consumer's wishes . . . such as by a statement or by a clear affirmative action." The consent definition specifies that

"[a]cceptance of general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent." As such, employers would want to ensure that the CPRA policies are provided to employees separate from any employee handbook, and that employers get a separate signature consenting to the policy.

Second, the CPRA would make it explicit that businesses cannot retaliate against an employee, applicant, or independent contractor for exercising their rights under the CPRA. Employers can expect that the plaintiffs' bar will use this provision to state claims for wrongful termination in violation of public policy and retaliation under Labor Code § 1102.5.

Third, the CCPA limits requests for disclosure of personal information to a 12-month period. In contrast, the CPRA would allow consumers to ask for the disclosure of personal information for greater than 12-months, although only applying to personal information collected on or after January 1, 2022.

Next Steps for Employers

Businesses do not need to take steps to comply with the CPRA unless and until the CPRA is passed by a majority of the voters in November 2020. However, businesses should keep an eye on the CPRA to see if it qualifies for the November 2020 ballot and, if it does qualify, whether it passes with the voters.

If you have not taken steps to comply with the CCPA yet, it is not too late to take steps to bring yourself into compliance. The California Attorney General will start bringing enforcement actions under the CCPA on July 1, 2020. As the CPRA indicates, privacy considerations are not going to go away. Moreover, if the CPRA does not pass, employers will need to plan to be fully compliant with all provisions of the CCPA by January 1, 2021. That will be a hard deadline to meet if employers do not start to take the steps necessary for compliance prior to the November election.

Fisher Phillips serves as outside employment counsel for thousands of employers across the country. We are presently advising many California employers and national clients that do business in California on preparing for the CCPA. For advice on California privacy law, feel free to contact any attorney in any of our five California offices.

Related People

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Service Focus

Privacy and Cyber