CPRA Update: How to Prepare for Privacy Compliance as an Employer

Alysa Z. Hutnik, Alexander I. Schneider

June 20, 2021

Last year's voter guide to California Proposition 24, the California Privacy Rights Act (CPRA), included a stark argument against enacting the privacy ballot initiative because it did not go far enough to protect employee privacy. "Currently, employers can obtain all kinds of personal information about their workers and even job applicants," the argument against Proposition 24 written by Californians for Privacy Now stated. "Proposition 24 allows employers to continue secretly gathering this information for more years to come…"

The message did not stick. Voters overwhelmingly enacted the CPRA, apparently judging that its provisions – including those that apply to employers – were worth an additional two-year waiting period. The effective date of the new law is January 1, 2023.

As companies build their roadmap to CPRA compliance, that assessment should also take into account planning for employee and job applicant privacy changes. The new law imposes first in the nation obligations that grant employees and job applicants new rights to access, correct, delete, and opt out of the sale or sharing of their personal information. The law also prohibits discriminating against employees or job applicants who lodge privacy rights requests.

In this post, we provide an overview of topics that employers should know as the sunset of the employer exception to CCPA approaches.

Why Would CCPA Apply to Employers?

The California Consumer Privacy Act of 2018 (CCPA), which became effective on January 1, 2020, originally applied to employers. The law defines a "consumer" as a natural person who is a California resident. This includes employees, job applicants, contractors, or other staff of a business.

In 2019, the California legislature amended the CCPA with a stopgap measure – for one year, the CCPA would not apply to employers. The measure, AB 25, said that personal information collected by a business in the course of the person acting as an employee, job applicant, or contractor in connection with the consumer's employee, job applicant, or contractor role is exempt from the CCPA. Also exempt is emergency contact information or information necessary to administer benefits.

Last year, California voters extended the employer exemption for another two years to January 1, 2023 in the CPRA ballot initiative.

What Employers are Covered by California Privacy Law?

If a business is covered by the CCPA for consumer data, it is covered for employee data. Starting in

January 2023, the CPRA thresholds for coverage are as follows:

- Annual gross revenues in excess of $25 million in the preceding calendar year,
- Buys, sells, or share personal information of 100,000 or more California consumers or households, or
- Derives 50 percent or more of its annual revenues from selling or sharing California consumers' personal information.

Some employers may be eligible for certain exemptions that are applicable to already-regulated information that they hold about their employees. For example, credit information that employers routinely collect to assess employment eligibility may be subject to an exception, because the information is already covered under federal fair credit reporting laws.

Also, employers that have existing obligations as business associates under the Health Insurance Portability and Accountability Act (HIPAA) may also be exempt with respect to any medical, protected health information (PHI), or covered benefits information that they maintain, use, or disclose.

In general, employers are also not required to comply with CPRA obligations that conflict with other federal, state, or local laws or legal obligations, or restrict an employer's ability to exercise or defend legal claims. For example, affirmative legal obligations to gather and maintain certain information, such as EEO-1 reports or compensation-related information may directly conflict with CPRA.

What Constitutes Employee Personal Information?

The definition of employee "personal information" includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular employee.

This may include name, contact information, identifiers, protected classifications (like gender, race, or sexual orientation), financial or medical information, account log in, religious or philosophical beliefs, union membership, commercial information, biometric information, internet or electronic network activity information, geolocation data, audio, electronic, visual, thermal, olfactory, or similar information, professional or employment-related information, education information, and inferences drawn from any of this information about the employee.

The contents of an employee's mail, email, and text messages constitutes sensitive personal information, a sub-category of personal information, unless the employer is the intended recipient of the communication.

What Obligations Apply Starting in January 2023?

All CPRA obligations apply. These include:

- **Notice:** Employees will be required to provide a comprehensive notice of their collection of personal information from employees, job applicants, and contractors, including description of the categories of personal information collected, the purposes of collection, details on disclosure of personal information, and information about retention of personal information.
- **Right to access:** Provide employees with a right to access categories of personal information and specific pieces of personal information. This includes any inferences drawn from personal

information to create a profile reflecting the employee's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- **Right to correct:** Provide employees with the right to correct their personal information using commercially reasonable efforts.
- **Right to delete:** Provide employees the right to delete their personal information. However, numerous statutory exemptions may apply, including allowing an employer to retain personal information reasonably anticipated by the employee within the context of an ongoing relationship with the employer, to perform a contract between the employee and employer, or to comply with a legal obligation.
- **Right to restrict uses of sensitive personal information:** Sensitive personal information includes a social security number, account log in, financial information, geolocation, racial or ethnic origin, religious beliefs, sexual orientation, health information, biometrics, and the contents of employee communications unless the employer is the intended recipient of the communication. Starting in January 2023, an employee may be able to direct an employer to limit certain uses of sensitive personal information for specific business purposes, as well as to direct an employer to limit disclosure of sensitive personal information, absent a qualifying exemption.
- **Right to opt out:** Provide employees the right to opt out of the sale of personal information to third parties. The term "sale" is a broad term, and includes disclosing employee information to business partners, vendors, and contractors absent a written agreement containing specific terms restricting the third party's use of that data, or a qualifying exemption.

Certain obligations are subject to change depending on action expected in the coming year from the newly constituted California Privacy Protection Agency.

What Steps Should Employers Take to Prepare?

Given the complexity of HR data and systems, as well as the sensitivity of employee data generally, it is not too early for employers to prepare for CPRA. Such efforts might include, for example:

- **Privacy Stakeholders:** Determine the legal, HR, and technology support (internal resources or external technology solutions) responsible for the efforts necessary to build a privacy compliance program and respond to privacy rights requests.
- **Data Mapping:** Understand the information that the business collects, the categorization of data (whether personal information or sensitive personal information), the location of the data, and the steps to access, correct, or delete the data. A major part of this effort should also include determining which data practices identified are subject to applicable exemptions from CPRA.
- **Contract Review:** Review partner contracts to correctly classify service providers and contractors from third parties, and that the contracts include the necessary restrictions depending on the classification. This effort might prioritize those partners that present more risk to the company, whether due to the nature of the processing, type, or volume of data in scope. Updating these contracts, however, might wait until there is more insight on the forthcoming CPRA regulations by the California Privacy Protection Agency (CalPPA) as to necessary terms, although the CCPA regulations are instructive.

- **Response Procedures:** Develop procedures for responding to employee requests, including managing sensitive requests while maintaining personal information as confidential and accessible to internal personnel only on a need-to-know basis.
- **Retention Policy:** Develop and document a retention policy that complies with applicable employer data retention obligations.
- **Notice:** Draft an employee privacy policy that complies with new statutory obligations under CPRA, as well as forthcoming regulations by the CalPPA.

Do Any of These Obligations Apply Now?

Employers may have an obligation to provide a notice at or before collection of personal information that details the categories of personal information that they collect and the purposes for which personal information will be used.

However, due to an apparent drafting error in the CPRA ballot initiative, this privacy notice obligation is muddled by a textbook case of unclear statutory construction.

Here's what happened. Originally, AB 25 required employers to provide a privacy notice to employees. However, the CPRA ballot initiative from last year changed a critical code section reference in an apparent drafting error. In so doing, the CPRA ballot initiative left unclear whether the employer privacy notice is required.

AB 25 said that employers would be required to provide a privacy notice based on Cal. Civ. Code 1798.100***(b)***. The CPRA ballot initiative changed the reference to Cal. Civ. Code 1798.100***(a)***. It is possible that the drafters intended to point to subsection (a) because in the CPRA ballot initiative this code section also requires a privacy notice. But the CPRA ballot initiative version of the code section is not actually the law until January 1, 2023.

That's a problem because under current law (effective until December 31, 2022), Cal. Civ. Code 1798.100***(a)*** talks about a different topic entirely – giving consumers the right to request that a business disclose the categories and specific pieces of personal information the business has collected about a consumer.

What is a reasonable interpretation in light of this problem? When it comes to statutory interpretation of ballot initiatives, courts generally say that the drafter's intent does not matter. In California, usually a court first looks at the language of the statute. If the language is not ambiguous, the court presumes the voters intended the meaning apparent from the language. If the language is ambiguous, then courts usually look at the ballot initiative voter materials for clues on how voters made their decision.

It is easy to see why a court might agree that the language is ambiguous. The employer exception clearly does not provide a right of employees to access their personal information until January 1, 2023. Giving full effect to 1798.100(a) would be hampered by the fact that the CCPA's core instructions on how to provide access to personal information and what to provide are subject to the employer exemption.

This brings us back to the ballot initiative materials provided to voters. The arguments against proposition 24 from Californians for Privacy Now warn that employers will be able to secretly gather personal information "for more years to come." Clearly, there is no recognition in the ballot initiative materials of any interim employee rights.

Bottom line? The law right now is unclear, and so, as a practical matter, it's a best practice (and required in a few other states) to publish a privacy notice for employees and job applicants.

Final Question: Do Employers Have Privacy Obligations in Other States?

There are no other states that have enacted CPRA-style comprehensive privacy laws that apply to employees; for example, Virginia and Colorado explicitly exempted the employment context without a sunset. But there are some states, such as Connecticut, that do require some form of privacy notice to employees. There are also two-party consent requirements in a number of states that are applicable to recording calls, as well laws that require disclosure about electronic monitoring.

Conclusion

The best way to address navigating these developments is to plan ahead with a compliance roadmap leading to 2023. Figure out what resources you'll need, including what types of internal and external support will be critical for success. Given the complexities involved, thoughtful (and realistic) preparation is a must.

* * *

Subscribe here to Kelley Drye's Ad Law Access blog and here for our Ad Law News and Views newsletter. Visit the Advertising and Privacy Law Resource Center for update information on key legal topics relevant to advertising and marketing, privacy, data security, and consumer product safety and labeling.

Kelley Drye attorneys and industry experts provide timely insights on legal and regulatory issues that impact your business. Our thought leaders keep you updated through advisories and articles, blogs, newsletters, podcasts and resource centers. Sign up here to receive our email communications tailored to your interests.

Follow us on LinkedIn and Twitter for the latest updates.