Published on *The National Law Review* https://natlawreview.com

# California Consumer Privacy Act: FAQs for Employers

Article By:

Jason C. Gavejian

Joseph J. Lazzarotti

Nathan W. Austin

Mary T. Costigan

Data privacy and security regulation is growing rapidly around the world, including in the United States. In addition to strengthening the requirements to secure personal data, individuals are being given an increasing array of rights concerning the collection, use, disclosure, sale, and processing of their personal information. Meanwhile, organizations' growing appetite for more data, and more types of data, persists, despite mounting security risks and concerns about permissible use. The recently enacted California Consumer Privacy Act (CCPA) is intended to address some of these risks and concerns.

The CCPA, which becomes effective on January 1, 2020, is in some ways the most expansive privacy law currently in the United States. Organizations familiar with the European Union's General Data Protection Regulation (GDPR), which became effective on May 25, 2018, certainly will understand CCPA's implications. Perhaps the best known comprehensive privacy and security regime globally, GDPR solidified and expanded a prior set of guidelines/directives and granted individuals certain rights with respect to their personal data, such as the right of access, the right of erasure (popularly known as the "right to be forgotten"), and the right to restrict the processing of personal data. In addition to mandating security for personal data, GDPR requires that individuals be notified of such things as the purpose and legal basis for processing their personal data, the categories of recipients of that data, and if the data has been breached. Many of these same principles are present in the CCPA.

The CCPA is certain to affect businesses across the U.S. and globally, and spur similar legislation in other states. In January 2019, a group of senators in Washington state, for example, introduced the "Washington Privacy Act," SB 5376 (WPA). That bill would establish GDPR-like requirements on businesses that collect personal information related to Washington residents. In addition to requirements for notice, and consumer rights such as access, deletion, and rectification, the WPA would impose restrictions on use of automatic profiling and facial recognition.

With the CCPA's effective date fast approaching, regulations being prepared by California Attorney

General Xavier Becerra's office, and considering that certain provisions may reach back prior to the effective date, businesses need to begin preparing as soon as possible. These FAQs are intended to call attention to some of the pressing issues relating to the CCPA's application to employee personal information, and highlight action items that can help businesses' compliance efforts.

## 1. What businesses does the CCPA apply to?

The CCPA will apply to any entity that does business in the State of California and satisfies one or more of the following: (i) annual gross revenue in excess of $25 million, (ii) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices, or (iii) derives 50 percent or more of its annual revenues from selling consumers' personal information.

Regulations may clarify one or all of these prongs, but some small businesses will not be able to escape the CCPA's reach. The law is trying to reach businesses with significant amounts of data, and that could very well be smaller companies. Additionally, businesses with small operations in California that meet one of these requirements will have significant privacy obligations with respect to those operations.

## 2. Does the CCPA apply to employment data?

The application of the CCPA to employee data remains an open question. On its face, the CCPA appears to apply only to California "consumers." However, the CCPA's definition of consumer (a California resident), combined with California's longstanding practice of protecting individual privacy rights, suggests that the CCPA also may extend to the personal information of California residents maintained as part of the employment relationship. If so, this would include residents of California who are job applicants, full- or part-time employees, temporary workers, interns, volunteers, independent contractors, and even such persons' dependent(s) or beneficiary(ies). For purposes of these FAQs, we refer to these individuals as "Workforce Members."

The definition of "consumer" states: "a natural person who is a California resident." 1798.140(g). That definition is not qualified by requiring such natural persons to be purchasing goods or services from businesses subject to the CCPA. It includes all persons who are residents in California. Additionally, one of the examples for what constitutes "personal information" under the law is "[p]rofessional or employment-related information." 1798.140(o).

On the other hand, the name of the law itself, and the fact that the law does not mention employers or employees, suggests that the legislature intended to protect the personal information of California residents in their role as consumers, and not employees (or Workforce Members). Additionally, prohibited discriminatory acts under the law include (i) denying goods or services, or providing a different level or quality of the goods and services, to the consumer, (ii) charging different prices or rates for goods or services, or (iii) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. Unlike what one might expect for a law protecting Workforce Members, the CCPA does not include acts that relate to the employer-employee relationship.

So, perhaps the CCPA's reference to professional or employment-related information intended to reach such data not in the hands of employers, but businesses handling such data for commercial purposes (such as a recruiting business). But, the CCPA has already been amended once. When

those amendments were being considered, there was an effort to exclude employees from the CCPA's reach. Those amendments, passed as SB 1121, made no change to the definition of "consumer" or any other change that would indicate an intention to exclude Workforce Members personal information from protection under that law.

Employers will have to wait and see whether there will be any additional amendments, or whether the Attorney General will clarify the issue through regulation. Currently, Attorney General Becerra is in the middle of six rulemaking workshops around the state in order to assist his office in formulating those regulations. Employers should watch these developments closely, but they also should consider taking some preliminary steps in order to be prepared to comply.

The remainder of this article assumes that the CCPA will be found to apply to Workforce Members data.

## 3. What is personal information under the CCPA?

The CCPA defines personal information broadly to include information that can identify, relate to, describe, be associated with, or be reasonably linked directly or indirectly to a particular consumer or household. This might be a name, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number or passport number, biometric information, bank account number or any other financial information, geolocation data, audio, electronic, or visual information, employment-related information, certain education information, or medical or health insurance information. It also may include inferences drawn from any such information used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

In the employment context, personal information is likely to be present in:

- A job application, resume, or CV;
- An employment contract or independent contractor agreement;
- A performance review or disciplinary record;
- A photo used for an identification badge or organizational chart, marketing, or website;
- Biometric data used for timekeeping or facility access;
- Backup files;
- Information from company devices or vehicles, including geolocation data;
- Browsing history or search history;
- Information used for payroll processing and benefits administration;
- Internal or external contact information maintained in the electronic onboarding, HRIS system, or Active Directory; or
- Information captured from video, audio, systems, or other forms of monitoring or surveillance.

Personal information also might include data collected about Workforce Members as part of an organization's human capital analytics or talent management programs. As noted above, the law applies to information used to create a profile about a natural person who is a California resident that would reflect such person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. For organizations that use sophisticated analytics programs to assist their human resources department in recruiting and developing the best talent, CCPA could create some compliance challenges.

The CCPA does not apply in certain situations, some of which may be relevant in an employment context. For example, the CCPA does not apply to medical information governed by the Confidentiality of Medical Information Act (CMIA) or protected health information collected by a covered entity or business associates governed by the privacy, security, and breach notification rules of HIPAA/HITECH. Thus, the CCPA is unlikely to apply to a Workforce Member's personal information accessed, created, or maintained in connection with the employer's group health plan. Likewise, medical information that an employer receives in connection with an Family and Medical Leave Act certification, Americans with Disabilities Act reasonable accommodation, workers' compensation claims, and so on, likely would not be subject to CCPA to the extent it is covered under the CMIA. *See* Cal. Civ. Code Sec. 56.20.

## 4. If the CCPA applies to certain employers and their Workforce Member data, would it apply to personal information collected in connection with the administration of employee benefits?

Yes, but perhaps not to all of those employee benefits. If the CCPA applies to Workforce Member data, and considering the broad definition of personal information discussed above, data involved in the administration of employee benefits generally would be within the scope of that definition. However, the CCPA provides specific exemptions that may exclude certain benefit plan data from its reach; namely, plans subject to the HIPAA privacy and security regulations (such as medical plans, dental plans, and health flexible spending arrangements).

There are, of course, may other kinds of employee benefits, such as pension and 401(k) plans, life and disability insurance plans, tuition assistance programs, employee discount programs, wellness program, transportation fringe benefit programs, and others. However, some of these employee benefits may involve plans that are subject to the Employee Retirement Income Security Act of 1974 (ERISA), which preempts certain state laws to the extent those laws relate to ERISA-covered employee benefit plans. A complete discussion of ERISA preemption is beyond the scope of this article, but a significant purpose behind it is to promote uniform administration of benefit plans nationally, avoiding a state-by-state approach. The application of the CCPA, and similar laws in other states likely to follow, certainly would complicate the national administration of such plans.

## 5. What rights would a Workforce Member have?

A Workforce Member would be entitled to each of the rights set forth in the CCPA. For example, under the CCPA, Workforce Members would have the right to request that a business, including an employer, disclose or provide access to personal information it has collected about the Workforce Member, the business or commercial purposes for using the information, and the third parties with whom the business shares the information. For many employers, meeting these obligations may not be too difficult. Employers generally will know the data they collect about their Workforce Members, why they collect it, and the third parties to whom they share the information. However, some employers may be using Workforce Member data in ways that they would prefer not to announce to their workforce or be available to their competitors. For instance, certain talent management strategies or other uses of information could be indicative of future business decisions such as layoffs or expansions into new markets.

Workforce Members also would be able to request deletion of their personal information and opt-out of the sale of their personal information to third parties. While most employers are probably not selling Workforce Member data, having to delete Workforce Members' personal information could be

a significant challenge. Being in a position to carry out this obligation requires knowing where the data is to be deleted. It also means knowing which vendors maintain the data so they could delete it as well. Thus, some kind of inventory or data mapping exercise would be needed to track the data and answer some basic questions such as what data is maintained, why it is maintained, and where it is. Knowing why the data is being maintained is important because employers would be able to push back on deletion requests if the employer, for example, has a legal obligation to retain it. In short, employers may need more sophisticated data governance practices in order to manage this and other rights concerning the data that Workforce Members may have under the CCPA and similar laws.

The rights under the CCPA also include the right to receive notice of the business's personal information collection and processing activities before or at the point of collection, as well as notice of the Workforce Member's rights. Similar notices may need to be made on the businesses' website(s) and online privacy notices. These notices are intended to help ensure individuals are aware of how their personal information is being processed, as well as the rights they have to control their personal information. Employers will have to carefully consider these notices, balancing efforts to ensure they are compliant, but also avoiding creating an administrative burden.

## 6. What obligations do the notice and rights provisions of the CCPA place on businesses?

As discussed above, under the CCPA, covered businesses, including employers, will need to provide notice to Workforce Members that includes the types of personal information collected by the business and how it is used; the Workforce Member's right to access that personal information; the right to delete the information; the right to know the third parties with whom it is shared; and the right to object to its sale to third parties, if applicable.

The CCPA also demands that covered businesses take steps to enable consumers to exercise these rights. Thus, for example, covered businesses will be obligated to make available two or more mechanisms for submitting requests for information required to be disclosed under the CCPA, including, at a minimum, a toll-free telephone number and, if the business maintains an internet web site, a web site address. When requests for information are made under the CCPA, businesses generally must respond to verifiable Workforce Member requests within 45 days. That period may be extended as long as the Workforce Member is notified within the first 45-day period. The response must cover the 12-month period preceding the receipt of the request. Responses must be in writing and the business is not required to respond to more than two requests for the same Workforce Member during a 12-month period. The CCPA requires that the employees designated to handle the responses to these requests receive training.

## 7. Can a Workforce Member agree to waive his or her rights?

No. The CCPA specifically prohibits any contractual provision or agreement that attempts to waive or limit the CCPA's rights, including the right to remedy or enforcement. As a result, any attempt to limit a Workforce Member's rights, whether by employment contract, agreement, or policy, would be unenforceable.

## 8. Where is Workforce Member personal information typically stored by organizations?

Protections under the CCPA apply to personal information regardless of its format. Thus, when thinking of where to look, employers should look broadly. For example, Workforce Member personal information can be stored in multiple locations, such as: a business's electronic onboarding system, HRIS system or Active Directory; file shares or backup files; in benefits or training records; in file cabinets or on a copy machine's hard drive; a manager's "desk copy"; or with third party services providers, such as a payroll processor or travel agency. It is imperative that covered businesses review, assess, and understand their existing data storage practices.

## 9. Does the CCPA require specific security safeguards to protect Workforce Member personal information?

The CCPA's focus is on privacy of personal information and extending greater control to individuals concerning their data. However, security is an element of privacy and while the CCPA does not expressly require the implementation of specific security measures, it notes a business's duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." To do so, organizations typically would need to conduct a risk assessment that reviews the types and sensitivity of its Workforce Members' personal information, as well as the risks to the security and privacy of this information. If California employers have questions about specific safeguards for maintaining security, they can refer to the California Attorney General's February 2016 Data Breach Report, which discusses best practices for data safeguarding. Employers should be aware similar frameworks are mandates in other states, such as Colorado, Massachusetts, and Oregon.

## 10. Can a covered business be sued for violating the CCPA?

The CCPA authorizes a private cause of action against a covered business for damages resulting from a failure to implement appropriate security safeguards which result in a data breach. The definition of personal information for this purpose is much narrower than the general definition of personal information under the CCPA. Here, the CCPA incorporates much of the definition of personal information under the California breach notification law. *See* Cal Civ. Code Section 1798.81.5(d)(1)(A). What should be troubling for covered businesses is that, if successful, a plaintiff can recover damages in an amount not less than $100 and not greater than $750 per incident or actual damages, whichever is greater, as well as injunctive or declaratory relief and any other relief the court deems proper. Thus, in addition to notifications a covered business may have under the state's breach notification law, class action lawsuits brought pursuant to this provision of the CCPA could be very costly.

Before a Workforce Member would be able to bring a lawsuit following an employer's data breach, he or she must provide the employer 30 days' written notice identifying the specific provisions of the CCPA that were violated. If cure is possible, and if within the 30 days the employer actually cures the noticed violation and provides an express written statement that the violations have been cured and that no further violations shall occur, the Workforce Member would not be able to pursue the action for individual statutory damages or classwide statutory damages. The Workforce Member still could seek actual pecuniary damages suffered as a result of the alleged violations.

### 11. What happens to Workforce Member personal information if the business is acquired?

Workforce Member personal information may be part of business assets that are transferred to a third party in the course of a merger, acquisition, or bankruptcy when the third party assumes control of all

or part of the business. This type of transfer is not deemed a sale of personal information for the purposes of the CCPA. Notwithstanding, if the third party materially alters how it uses or discloses the Workforce Member's personal information and that use or disclosure is a materially inconsistent with the notice provided to the Workforce Member at the time of collection, the third party must provide the Workforce Members with prior notice of the changed practices.

## 12. Does the CCPA apply if a Workforce Member is no longer a resident of California?

In the event a Workforce Member moves or is transferred to a location outside of California, depending on the facts, the Workforce Member may no longer be a resident of California and his or her personal information will no longer be protected by the CCPA. Notwithstanding, the Workforce Member's personal information may be protected by other laws and the organization may still have the same, or even heightened, obligations to safeguard the Workforce Member's data. Employers should consider this and similar issues when drafting notices for employees concerning their rights under the CCPA. For example, if a notice extends rights to an "employee" and not an "employee who is a California resident," a transfer that would change the person's residency may not change the rights extended in that notice.

## 13. How does the CCPA interact with federal, state, or local laws?

The CCPA specifies that its obligations are a matter of statewide concern in California and supersede and preempt all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or local agency regarding the collection and sale of a consumer's personal information by a business.

However, the CCPA also specifies that its obligations shall not restrict a business's ability to comply with federal, state, local laws, or regulations. In addition, while the CCPA is drafted to supplement federal and state law, it shall not apply if it is preempted by or in conflict with federal law, the United States Constitution, or the California Constitution. To determine which laws or regulations will govern, an organization will need to identify all the purposes for which Workforce Member information is collected, processed, and retained. For example, the federal Fair Labor Standards Act (FLSA) expressly requires the retention of employee identifying information for a specified period of time. These requirements would preempt the employee Workforce Member's ability under the CCPA to request deletion of certain personal information that must be retained to satisfy compliance under FLSA. Similarly, as discussed above, ERISA includes certain recordkeeping requirements relating to an employer's employee benefit plans. Specifically, section 209 requires that an employer maintain employee records sufficient to determine benefits. Again, an employee Workforce Member's request for deletion of certain personal information may be information subject to ERISA retention requirements. In such a case, the employer's obligations under CCPA would yield to ERISA's requirement.

## Recommended Action

While it is presently unclear whether the CCPA will apply to Workforce Member personal information, the question has been raised and efforts to remove Workforce Member data from the CCPA's reach have thus far been rejected. Regulations from the California Attorney General's office may provide some clarity on this point. It is also reasonable to believe further guidance or amendments from the California legislature may be forthcoming. In the interim, there are several steps an employer can

take to better position itself for potential compliance obligations.

1. Monitor the status of the CCPA to ensure the organization is aware of additional amendments and the regulations that will be issued.

2. Begin staging resources to be able to identify and map the Workforce Member personal information in the organization's possession or under the organization's control. All successful compliance activity is built upon knowledge of what information is collected, who it is collected from, how it is collected, why it is collected, all purposes for which it is used, all locations where it is stored, and any third party with whom it is shared. Of course, the organization may already have obligations to safeguard personal information, which may include deleting information that is no longer needed. To meet such requirements, the organization needs to answer many of the same questions.

3. Review and identify existing or needed organizational and technical procedures to facilitate compliance with Workplace Member rights under CCPA. These should include:

- Developing or identifying at least two mechanisms for permitting Workforce Members to exercise their rights to request information on what the business collects, the purposes for which it is used, the third parties with whom it is shared (such as a payroll processor). Mechanisms can include an email address, postal address, website link, phone number, and so on.
- Developing or identifying internal mechanisms that could be made available to respond to an employee's exercise of access rights, including verifying their identity, responding within the mandated timeframe, and documenting the request and response.
- Developing or identifying an internal mechanism for deleting a Workforce Member's personal information on request. This will include determining whether any state or federal laws preempt the deletion and notifying third parties with whom the organization has shared the information (such as payroll processors and IT vendors) to delete the information.
- If applicable, developing or identifying an internal mechanism to track third parties to whom Workforce Member personal information is sold in order to comply with the Workforce Member's request to opt out of that sale.
- Developing or identifying procedures for handling Workforce Member personal information upon separation from employment. This includes identifying what state and federal laws address record retention and destruction and how they interact with the CCPA and an organization's operational needs.

4. Review or create a data retention schedule that reflects the types of data the organization maintains. The obligation to safeguard data, both under the CCPA and Cal. Civ. Code 1798.81.5, is a significant reason to reduce the amount of personal information retained after it is no longer necessary for the purpose for which it was collected. Consider operational and regulatory retention requirements such as those imposed by FLSA and ERISA.

5. Identify whether the organization's standard employment contracts or employee manual or handbook should be updated to include notice of collection and processing activities, as well as Workforce Member access and deletion rights. The organization also may need to convey similar information in other places, such as its intranet, business website, website privacy policy, and consumer rights notice.

6. Begin identifying the staff who would be responsible for handling employee access rights and other requests under the CCPA, and how the organization might train these staff members. It will be

important to maintain consistency when carrying out these obligations.

7. Review vendor contracts for those vendors with access to Workforce Member personal information (such as IT providers, HRIS software and service providers, payroll processors, travel agencies, and professional service providers). Provisions should address appropriate security safeguards, data breach reporting obligations, use and disclosure limitations, data retention and disposal, and the ability to assist the business in responding to a Workforce Member rights request. Employers should be negotiating, reviewing, or renegotiate existing vendor contracts to ensure the vendor's ability to comply with access rights relating to information collected and retained. This practice dovetails with the requirements of Cal. Civ. Code 1798.81.5(c) to contractually require that a third party with whom the business shares personal information maintains reasonable security procedures to safeguard the business's personal information.

8. Review organizational and technical access controls. As discussed above, the CCPA permits a consumer to bring a private cause of action against a business for the unauthorized access and exfiltration, theft, or disclosure of personal information as a result of the business's failure to implement and maintain reasonable security procedures and practices. California's breach notification law excepts from the definition of a breach an unauthorized but good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, as long as the information is not used or subject to further unauthorized disclosure. However, in permitting a private cause of action for a data breach, the CCPA does not provide for this exception. As a result, an employer may be liable for the unauthorized access of Workforce Member personal information by its employees and agents even if the incident is not a reportable breach under Cal. Civ. Code section 1798.82. To guard against this, businesses should ensure their organization has appropriate policies and procedures in place, including role-based access, password management, system auditing, and training.

9. Review the business's written information security program (WISP) or internal administrative and technical policies and procedures to reflect and demonstrate compliance with the CCPA requirements of security safeguards appropriate to the nature of the information to protect the personal information.

## Conclusion

Many of the steps listed above may be adapted to satisfy other data privacy protection frameworks, assist in developing a robust internal data protection program, or position the business for future regulatory obligations. All 50 U.S. states have now enacted data breach notification laws. Many have enacted laws addressing data safeguarding, disposal, or vendor management, and many, like the state of Washington, may begin advancing legislation similar to the CCPA. Several federal data protection laws are under consideration and countries around the world continue enacting national data privacy laws to protect individuals. This legislative activity, combined with the growing public awareness of data privacy rights and concerns, makes the development of a meaningful data protection program an essential component of business operations.



National Law Review, Volumess IX, Number 29