

## **New California Legislation Enhances Employees' Privacy Rights**

With the California Consumer Privacy Act of 2018 (CCPA) set to take effect on January 1, 2020, California Governor Gavin Newsom signed amendments in October 2019 providing businesses some temporary shelter from the CCPA provisions with respect to information of their employees, job applicants and independent contractors. Even with the amendments, effective January 1, 2020, covered businesses (1) must provide disclosures to employees about the categories of personal information collected and the purpose for which the categories of personal information will be used, and (2) would be subject to such individuals becoming entitled to statutory damages for data breaches of a California employee's personal information. One year later, on January 1, 2021, all rights under the CCPA become effective for covered businesses, including the right of employees to request access to their information and the right to request that their information be deleted.

The CCPA defines a "business" as a legal for-profit entity that collects "personal information" of California residents, does business in California and that meets any of the following three thresholds:

- Gross annual revenue exceeds \$25 million
- Buys, receives, sells or shares personal information of 50,000 or more consumers, households or devices
- Derives 50% or more of its annual revenue from selling personal information Civ. Code § 1798.140(c)(1)

Significantly, a business does not have to be physically located in California for the CCPA to apply. A "consumer" is broadly defined as any "natural person who is a California resident." Civ. Code § 1798.140(g). "Personal information" is broadly defined and includes "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer." Civ. Code § 1798.140(o)(1). The CCPA identifies 11 categories of information, including common identifiers such as name, address, email and Social Security numbers, but also other categories such as professional or employment information, internet activity such as browsing history, and even inferences drawn from any of the categories of information. The CCPA provides consumers with several rights—including the right to know, the right to access, the right to opt out of sale and the right to delete.

The new amendment signed into law, [AB 25](#), provides a limited, temporary one-year relief for employers with respect to employee, job applicant and contractor information. AB 25 exempts personal information that is collected by a business about a consumer who is acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of or contractor of that business to the extent that the consumer's personal information is collected and used by the business solely within the context of the consumer's role or former role as one of the foregoing. Likewise, emergency contact information would be exempt in such context as well. However, AB 25 does not exempt a business from all CCPA obligations. Starting January 1, 2020, a covered business still needs to provide notice, at or before the time of collection, of the categories of personal information the business collects from consumers (including its employees and similar individuals) and the purposes for which the categories of personal information will be used by the business. Employees also retain their right to bring a private action for a data breach. The AB 25 exemption for businesses expires on January 1, 2021.

The California attorney general has released its proposed regulations, which set forth specific requirements for compliance with the CCPA, including the "notice at collection" that an employer still needs to provide. The regulations would require the business to include in its notice the following:

- A list of the categories of personal information collected on its workforce, with each category description written in a manner that provides consumers a meaningful understanding of the information being collected
- A list of the business or commercial purpose(s) for each category of personal information
- An opt-out website link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" if the business sells personal information
- A link to the business's privacy policy, or in the case of offline notices, the web address of the business's privacy policy

The disclosure should also be easy to read and understand, should avoid legal jargon, should draw the consumer's attention, should be translatable into other languages, should be accessible to consumers with disabilities and should be accessible to workers before any personal information is collected.

In addition, employees and all consumers retain the right to statutory damages in the amount of \$100 to \$750 per data incident if their personal information is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business' violation of its duty to implement and maintain reasonable security procedures and appropriate practices.

### **Full Protections of CCPA Extend to Applicants, Employees and Contractors on January 1, 2021**

Unless AB 25 protections are extended, it will expire and all rights and obligations under the CCPA will extend to all employees and similar individuals. Some rights include the following:

- The right to request that a business disclose what personal information the company has collected
- The right to know what personal information is being sold or disclosed and to whom
- The right to request and receive a copy of all of the above information in a readily useable format
- The right to request that the company delete their personal information (the right to be forgotten)
- The right to opt-out of the sale of their personal information
- The right to be free from discrimination for exercising any rights

### **Takeaways for Employers**

All businesses, including those not physically located in California, should verify whether theirs is a covered "business" and whether they must comply with the CCPA. Covered businesses should ensure they comply with the notice at collection requirement and make sure they have reasonable security measures in place to protect the employees' and consumers' personal information. Covered businesses should also identify and inventory all data that may be considered personal information under the CCPA, and all third parties with whom the company shares personal information, including benefits providers, insurance companies, payroll companies and staffing vendors. Covered businesses should also ensure that all third parties enter into service provider agreements and such agreements should reflect the third party's commitment to comply with the CCPA and to protect all sensitive employee data. Finally, covered businesses should update employee privacy policies to include CCPA rights.

More information on the CCPA and how it will affect both businesses and consumers [can be found here](#).

## Authors



### **Javier F. Garcia**

Partner

[JGarcia@perkinscoie.com](mailto:JGarcia@perkinscoie.com) [310.788.3293](tel:310.788.3293)



### **Emily A. Bushaw**

Partner

[EBushaw@perkinscoie.com](mailto:EBushaw@perkinscoie.com) [206.359.3069](tel:206.359.3069)

## Explore more in

[Labor & Employment](#)

## Related insights

Update

**[Employers and Immigration Under Trump: What You Need To Know](#)**

Update

**[‘Tis the Season... for Cybercriminals: A Holiday Reminder for Retailers](#)**