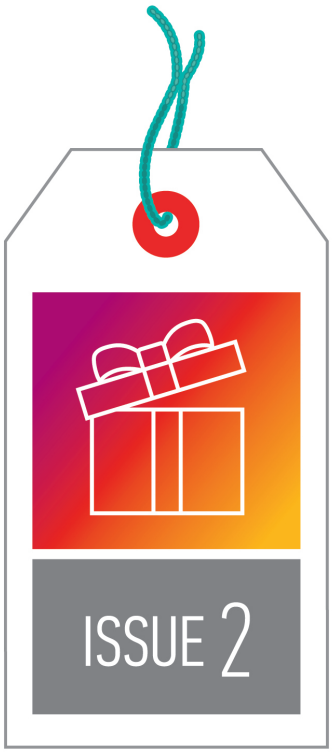
Updates
October 20, 2022

Coal in the Stocking for Retail Employers: The California Privacy



As the California Privacy Rights Act (CPRA) replaces its predecessor, the California Consumer Privacy Act (CCPA), on January 1, 2023, retailers face a significant amount of compliance preparation—and right at peak season. The CCPA temporarily exempted employment-related and business-to-business information until the effective date of the CPRA. It was widely expected that the same exemption would be carried forward to the CPRA. However, the California legislative session closed on August 31, 2022, without codifying the employee or business-to-business exemption.

Retailers doing business in the state of California who meet one or more of the following criteria need to quickly address how the new law will affect their employees, applicants, and independent contractors:

- As of January 1 of the calendar year, the company exceeded $25 million in annual gross revenues in the preceding calendar year.
- The company buys, sells, or shares the personal information (PI) of more than 100,000 California households or consumers.
- The company derives 50% or more of its revenues from sharing or selling PI.

The CPRA requires covered employers to limit the collection, use, retention, and sharing of an employee's PI within certain parameters. The law requires employers to provide new notices or obtain an employee's explicit consent before collecting, using, retaining, or sharing PI outside of certain exceptions. It also grants employees significant new rights, including the following:

- **Deletion.** Request deletion of PI collected from the individual.

- **Correction.** Ask for a correction of inaccurate PI.
- **Right to know.** Right to know how the employer collects and handles the individual's PI and how to receive copies of specific pieces of PI (e.g., access their own data).

In many ways, the right to deletion is a bit of window dressing—most requests may be denied due to an employer's obligation to retain data to comply with federal or state laws or where deletion would prevent the business from exercising or defending legal claims. However, responding to the Right-to-Know requests and providing access to PI will be a significant lift for employers.

The CPRA imposes significant new obligations on covered employers, including requirements related to data retention, data minimization, and purpose limitation. Employers must also pass deletion requests to service providers, contractors, and third parties to which they have sold or shared information. The law mandates additional provisions that businesses must include in their contracts with service providers, contractors, and other third parties. Regulations issued under the law are likely to increase auditing requirements, such as performing cybersecurity audits on an annual basis and providing the California Privacy Protection Agency (CPPA) with regular risk assessments.

Steps To Take

There is a chance that the law will be modified or a grace period extended before the July 1, 2023, enforcement deadline. However, employers are advised to take action while there is still sufficient time to prepare. Although most affected retailers have initiated significant planning with respect to consumer data, the following are the top 10 steps that should be undertaken for employment information.

1. **Data map.** It is impossible to respond to data subject access and deletion requests if an employer is not sure what categories of PI and sensitive information they collect from applicants, employees, or independent contractors; how they use that information; and where the information is stored. Many retailers initially started—and abandoned—data mapping employee information when CCPA began, so existing data maps, if any, are likely to be outdated. In a retail environment, it is fairly typical for employee data to be stored throughout the enterprise, with pockets of data in off-site storage, store or distribution-specific human resources (HR) centers, headquarters, and various human resources information systems (HRIS). It will take time and effort to interview key stakeholders to ensure all data is appropriately accounted for. For many retailers, their employees are also often consumers. In most cases, it is recommended to differentiate employee versus consumer data.
2. **Determine if data is within scope.** Once the employer has mapped all the data, it needs to categorize that data as either "professional employment-related information," which is within the scope of CPRA, or "company" data not considered employee PI. In some cases, this decision may also require an update to company policies regarding the acceptable use of email, mobile devices, handbooks, and other data-containing entities. This is also a good time to reevaluate the company's document retention policies.
3. **Determine if PI is being sold or shared.** Evaluate whether there is any "sale" or "sharing" of PI to third-party vendors, such as benefits consultants. In the employment context, there are rarely true "sales," as in the exchange of data for money. Still, employers must carefully analyze whether the information is otherwise rented, released, disclosed, disseminated, made available, or otherwise transferred to a third party for money or valuable consideration. The CPRA defines "sharing" as the transfer or making available of PI "by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration." While "sharing" is unlikely to arise in an employment context, if information is exchanged for valuable consideration, such as administrative fee discounts or free pilot benefit programs, employers may need to evaluate whether employees must be provided with a right to opt out of the transfer of their information to the vendor.

4. **Evaluate sensitive PI use.** Determine what "sensitive" PI is collected, evaluate how it is used, and determine if appropriate notice and ability to limit disclosure are needed. Sensitive PI includes information such as an individual's government identification (driver's license, passport numbers, state ID, and Social Security numbers); precise geolocation; ethnic or racial origins; biometric data and genetics; union membership; religious or philosophical beliefs; private communications content (text, mail, or email) where the company is not the intended recipient of such communications; and information about one's sexual orientation, sex life, or health. From an employment perspective, diversity, equity, and inclusion data and certain geolocation data can be potentially problematic. A careful review is necessary to determine if the employer is inferring characteristics about the employee based on the information. If so, special rules apply.
5. **Determine whether rights will be limited to California residents.** Limiting data subject rights for California residents may raise employee relations issues as team members may express concerns about the collection and usage of their PI on a perceived inequitable basis. This may be especially problematic for retailers that are facing a historic surge of union-organizing campaigns.
6. **Update privacy notices.** This is a reminder to be mindful of terminology here, as applicants and independent contractors are covered by the scope of the CPRA, but they are not employees. Co-employment claims may arise if businesses refer to all groups as "employees." Consider whether to have separate privacy notices for applicants and independent contractors.
7. **Update notice at collection.** Privacy notices are designed to be prospective in nature, describing why the business collects PI and what it may do with it in the future. A notice at collection is a little different and should be provided when the data is actually being requested from the employee to present sufficient information about the categories of PI to be collected at that very moment, the purposes for which it is collected or used, and whether the PI will be sold or shared so that the individual can decide whether to disclose the information.
8. **Determine who will handle DSARs.** Consider whether to partner with an external vendor to verify the identity of requesting individuals, track requests, and respond to data subject access requests (DSARs). Internal responding departments may be inundated with requests if new data subject rights are not limited to California residents. Coordination with in-house human resources and legal teams will be needed, as the response deadlines for CPRA are typically within 45 days of a request, with a one-time 45-day extension where "reasonably necessary." However, the California Labor Code typically requires the production of personnel files within 30 days and payroll records within 21 days. Ineffective coordination may lead to late production of documents, the imposition of fines and penalties, and may open the door to potential class-action risk.
9. **Update vendor contracts as necessary.** Vendors who directly house PI about employees, such as payroll and benefits administrators, may need to respond directly to DSARs. Vendor contracts must be thoroughly reviewed and potentially amended to address this responsibility.
10. **Be flexible.** Although regulations are forthcoming, employers simply cannot wait until issuance and expect to meet compliance deadlines. Flexibility is key, and employers will need to be nimble and potentially change course or modify compliance strategies.

Authors

April A. Goff

Partner
AGoff@perkinscoie.com 214.259.4954

Explore more in

Labor & Employment Privacy & Security Retail & Consumer Products

Related insights

Update

FERC Meeting Agenda Summaries for October 2024

Update

New White House Requirements for Government Procurement of AI Technologies: Key Considerations for Contractors