California's Groundbreaking Privacy Law Amended: What Do Employers Need To Know?

Insights
10.12.19

Governor Gavin Newsom just signed into law two amendments to the California Consumer Privacy Act (CCPA) that will have a direct impact on employers doing business in the state. The new amendments, signed on October 11, 2019 and taking effect on January 1, 2020, require covered businesses meeting a certain revenue threshold or other criteria to implement policies and procedures that provide consumers – which includes employees – certain privacy rights not previously available under existing law.

The first relevant amendment, AB 25, postpones by one year, until January 1, 2021, all the CCPA's requirements pertaining to employee data except for two: (1) reasonable security measures to safeguard the data, and (2) disclosure of the categories of personal information collected about employees and job applicants and the business purposes for which the information is used. The second relevant amendment, AB 1355, excludes from coverage of the CCPA, until January 1, 2021, specified "business-to-business" communications or transactions.

Even though enforcement by the California attorney general does not begin until July 1, 2020, the CCPA compliance deadline is just a few months away. Therefore, employers doing business in California should immediately consider whether the CCPA applies to them and if it does, determine what steps they should take to be ready.

First, Some Background: Does the CCPA Apply to You?

Before discussing AB 25 and AB 1355, the first question you should ask is whether the CCPA even applies to you. The only covered businesses that will be subject to the CCPA are those for-profit businesses that (a) do business in California, (b) collect the personal information of consumers including employees, and (c) satisfy any of the following three criteria:

- have annual gross revenues over $25 million; OR
- annually receive, sell, or share personal information 50,000 or more California residents or households or 50,000 devices; OR
- derive 50% or more of their annual revenue from selling personal information of consumers.

If you are a nonprofit, the CCPA does not apply to you unless your nonprofit is "controlled" by and shares common branding with a covered business (for example, a nonprofit foundation formed by a large business that bears the same brand and is therefore known to be affiliated with that business). The same is true of subsidiary businesses that do not fit the above criteria; if the parent business is covered by the CCPA, all subsidiaries that are "controlled" by and share common branding with that parent will also be subject to the CCPA. Here, "control" means ownership of or having the power to vote more than 50% of the shares or to elect the majority of the directors, or the power to exercise a controlling influence over the management of the entity.

If you are not a California business, you might be wondering what it means to "do business in California." The CCPA does not provide any explanation, and the attorney general's proposed regulations that were issued on October 10, 2019 do not address this issue either. In the absence of any legislative or regulatory guidance, this is best viewed in terms of what is sufficient to establish personal jurisdiction to haul a non-California business into state court in California. For purposes of CCPA coverage of employee data, if a non-California business that fits the revenue threshold or one of the other criteria has one employee in the state, that business must comply with the CCPA with respect to that employee's personal information. If a non-California business is actively and directly recruiting candidates for employment in California, the business would likely be subject to the CCPA with respect to personal information it collects from California candidates.

Employers doing business in California that do not meet the $25 million revenue threshold may still be covered by the CCPA if they have received from any source or shared the personal information of 50,000 or more California-based employees, job applicants, or other residents in the last 12 months. This includes not just your employees and job applicants, but also information about the family members and dependents of your employees that you may be collecting as part of insurance enrollment paperwork or even in an emergency contact form.

Another way of potentially satisfying the 50,000 threshold is if you collected and tracked through your website information about 50,000 or more devices that were used to access the website. For example, a small business that has a website with 137 unique visits per day and collects data about the devices or consumers who are accessing the site is likely going to meet the threshold.

Are Any Industries Exempt?

There are some exceptions, but they are more nuanced than a full exemption from the CCPA. For example, a HIPAA-covered entity is exempt from the CCPA with respect to patient information that is maintained in accordance with HIPAA regulations, but it is NOT exempt with respect to the data of its California-based employees and job applicants. Similarly, a consumer credit reporting agency or background check company is exempt from the CCPA with respect to information in consumer reports that it compiles and provides to its clients, but it is NOT exempt with respect to the data of its own California-based employees and job applicants.

What Employee Information is Covered by the CCPA?

What Employee Information is Covered by the CCPA?

The CCPA as enacted makes no distinction between employees and consumers. "Personal information" is defined so broadly that it potentially covers all information you collect, maintain, or share about job applicants, employees, and their family members or dependents that could identify the individual or be used in conjunction with other information to identity the individual.

This would include, for example, the name of an employee in conjunction with the state or federal protected category they are in (such as age, race, gender, sexual orientation, religion, disability, etc.). It also potentially would include network or internet activity logs on company computers assigned to employees that show user activity such as search and browser history. The definition of "personal information" also lists the broad category of "professional or employment-related information" without any definition or parameters of what that entails.

Covered employee information potentially could include, for example, personnel files, payroll records (pay stubs, timesheets, direct deposit information, tax withholding information, etc.), health insurance records, workers' compensation files, and training records. If you provide your employees any company computers or devices and collect information about their internet usage on those devices or geolocation information (to track where they go with the company-issued devices), this information could also be subject to the CCPA.

How Does AB 1355 Amend the CCPA?

AB 1355, which passed the legislature unanimously, makes a number of changes to the CCPA. First, it clarifies that personal information does not include information that has been "deidentified." Information is deidentified when all identifiers that would like the information to the individual have been removed, such as through redaction of information that could be used to identify the individual.

In addition, AB 1355 clarifies that personal information does not include "aggregate consumer information," which is defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device." In the employment context, aggregate information may be reports or spreadsheets with information about groups of employees where the names or other employee identifiers have been removed (for example, EEO-1 reports, demographic reports, or pay equity reports that address aggregate information for groups of employees without identifying them).

Finally, AB 1355 specifies that, until January 1, 2021, certain CCPA obligations do not apply to personal information reflecting specified "business-to-business" communications or transactions. Specifically, the bill excludes a communication or transaction between a business and a consumer (including another business) where the communication occurs solely within the context of the business conducting due diligence or providing or receiving a product or service from that business.

What Does the CCPA Require a Covered Employer to Do?

Employers have their work cut out for them, but the governor's signing of AB 25 gives you a one-year reprieve from having to comply with most of the CCPA's requirements. Covered businesses now have until January 1, 2021 to meet all the CCPA's requirements except for two.

First, covered businesses must still ensure they have implemented reasonable security measures, both physical and electronic, to safeguard the personal information of employees and job applicants. In the event of a data breach resulting from failure to implement reasonable security measures, an affected employee can file an individual lawsuit or a class action and potentially recover between $100 and $750 per consumer per data breach incident or their actual damages, whichever is greater. Accordingly, all covered businesses should reassess their electronic and physical security measures to ensure they are all up to date. It is a best practice to undergo an *external* security audit by an independent security consulting firm, not by your internal or outsourced IT vendor.

Prior to a security audit, however, and in order for such audit to be comprehensive enough, you should engage in "data mapping," which involves mapping out in a living document that is continually updated (1) all of the items of personal information the business collects, retains or shares; (2) where the information is physically and electronically stored; (3) who at the company has access to the information; (4) with whom the information is shared outside the company; and (5) the business purposes for which the information is used or shared. A data map will help facilitate a guide the security auditor to ensure that reasonable security measures are in place at all access points and for all items of information maintained by the business.

Second, the deadline will remain January 1, 2020 for the requirement of disclosing to employees and job applicants the categories of personal information you collect about them and the purposes for which the information will be used. This disclosure must be made before or at the time you receive personal information of any employee or job applicant.

The disclosure need not list every piece of information you collect about the employee, but rather only the categories of information. For clarity, you should consider listing examples of information within each category (for example, "Employee Pre-Hire Documents, such as job applications, resumes, background check forms and results, drug test forms and results, job interview notes, and candidate evaluation records.").

The CCPA provides several examples of business purposes for which information may be maintained and that covered employers can list in the disclosure. Starting January 1, 2020, covered employers will be prohibited from using any employee personal information for any purpose that is not listed in the disclosure provided to employees. Therefore, the disclosure should be as comprehensive as possible in terms of identifying all business purposes for which the information is used. Examples of business purposes that are common in the employment context include the following:

- to comply with state and federal law requiring employers to maintain certain records;

- to effectively process payroll;
- to administer and maintain group health insurance benefits, 401K and/or retirement plans; and
- to manage employee performance of their job duties.

While the CCPA simply requires the disclosure notice to identify the categories of personal information and business purposes (which many practitioners have interpreted to mean two separate lists of all the categories followed by all the business purposes for which all the information may be used), the attorney general's proposed regulations if adopted would require the notice to list for each category of personal information all the business purposes that the particular category of information will be used for. The proposed regulations are not expected to become final rules until the spring of 2020.

For current employees, the disclosure can be made to them as a group in the employee handbook or through a memo to all employees. Technically, there is no requirement that employees sign an acknowledgment of receipt of the disclosure, but practically having their signature will be the only sure way to prove that they received it. We often encounter employees who later deny receipt of policy documents in order to leverage an advantage in litigation, and it's easy to avoid this situation by obtaining a simple signature.

As for job applicants, since the CCPA requires that the disclosure be made at or before the transaction in which the personal information is collected, the best approach is to include the disclosure with the job application.

Without Further Action, What Will a Covered Employer Have to Do by January 1, 2021?

AB 25 does not exempt employers from any of the CCPA's requirements, but rather employers will have an additional year to comply with all but the two requirements discussed above. Unless the exemption is further extended by the legislature next year, the CCPA will require covered employers to do the following, among other steps, by January 1, 2021:

- Expand the disclosure provided to employees and job applicants in 2020. In addition to describing the categories of information the employer collects and the business purposes for which it uses the information, the disclosure must provide them with notice of their rights under the CCPA (including the right of access, deletion, and receiving a copy of the information), state whether the information is being shared with any third parties, and identify the categories of third parties with whom the employer will share the information. The CCPA prohibits using the information for any purpose that is not listed in the disclosure and from sharing the information with any third party that is not named as well. The disclosure can be amended.

- Implement at least two methods by which employees and job applicants can submit verifiable "consumer requests."

- Track and respond within 45 days to verified consumer requests from employees and job applicants. This can be extended an additional 45 days.

Again, unless the legislature extends the exemption further, there are three types of consumer requests that your employees and job applicants will be entitled to submit under the CCPA starting on January 1, 2021: (a) request for disclosure of what personal information you have about the individual or what information you have shared; (b) request for deletion of the information; and (c) request for access to or a copy of some or all of the information, which must be provided free of charge.

The third type of request is the most sweeping change that could potentially impose significant burdens on employers. Such requests include a request for a copy of all the employee's personal information the employer has obtained, compiled, or shared in the last 12 months. Since the definition of "personal information" is so broad, the CCPA (without amendment) may allow employees and their attorneys to request and obtain from you free of charge a lot more than what the law otherwise permits – a significant amount more than just an employee's personnel file and payroll records. To say that this permits potentially abusive and burdensome pre-litigation discovery would be an understatement.

The exemption created under AB 25 was limited to one year at the request of organized labor and privacy advocates, who indicated that they want to engage in a discussion in 2020 regarding concerns over "workplace privacy" and "workplace surveillance." If agreement is reached next year on these broad issues, there is hope within the business community that the exemption to the CCPA for employment data could be extended further. So employers will have to stay tuned next year to see if further relief is provided or whether the other requirements of the CCPA will apply to employers beginning in 2021.

Next Steps for Employers

As the CCPA's compliance deadline is fast approaching, you would be wise to stay ahead of the curve on privacy practices, whether or not you are presently subject to the CCPA. But if you are subject to the CCPA, then you have three tasks to complete by December 31, 2019 that practically require getting started as soon as possible: (1) "data map" all your employee data; (2) undergo a security audit to ensure that you have implemented reasonable physical and electronic security measures to protect private information; and (3) draft the disclosure to employees and job applicants as described above.

It is best to work with privacy counsel on these steps, especially so you could assert the attorney-client privilege over relevant communications. For example, security audits may reveal things you don't want plaintiffs' attorneys to discover; you don't want to give them the results of the audit on a silver platter to serve as their "Exhibit A." If the audit is performed at the direction and involvement of counsel, all communications and work product created during the audit would likely not be discoverable.

discoverable.

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

Benjamin M. Ebbink
Partner
916.210.0400
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Privacy and Cyber