Businesses Nationwide Face New Privacy Obligations Thanks To California Vote

Insights
11.04.20

Californians just passed a ballot measure that will soon expand the nation's most stringent data privacy law – and it will have an impact on employers across the country. By voting in favor of Proposition 24 – the California Privacy Rights Act of 2020 (CPRA) – employers and businesses will face an expansion of the state's landmark privacy law, the California Consumer Privacy Act of 2018 (CCPA). Most provisions of the CPRA go into effect on January 1, 2023, although some provisions have a 12-month lookback, as explained below. What do employers and businesses need to know about this dramatic new legal obligation – especially those beyond the California border who may not recognize their obligations?

The New Law In A Nutshell
Despite being California legislation, these privacy laws affect employers and businesses nationwide. Any employer or business — regardless of where they are located — who has an employee in California, accepts applications from California residents for positions anywhere in the nation, has customers in California who are natural persons, or otherwise does business in California (even if only over the internet) may be subject to the CCPA and CPRA.

Currently, the CCPA applies to any such business that meets any one of the following criteria:

1. Has gross annual revenue in excess of $25 million from anywhere in the world, not just in California;
2. Annually receives, buys, sells or shares for commercial purposes the personal information of 50,000 or more California residents, households or devices; or
3. Derive 50% or more of its annual revenue from selling personal information.

But even if none of these criteria apply, the CCPA can still apply to subsidiaries and franchisees if they meet a broad "control" test and share a common name or trademark with the covered business that "controls" them.

While the CCPA took effect on January 1, 2020, many key provisions as they applied to employees and job applicants were deferred until January 1, 2021.

The CPRA makes numerous substantive changes to the CCPA, including:

- **Changes to which businesses are required to comply with the CCPA;**
- **Additional protections for a new subcategory of personal information called "sensitive personal information";**
- **Additional limitations on the collection and use of personal information;**
- **New requirements on a business's relationships with third-parties;**
- **The right of consumers to request correction of inaccurate personal information; and**
- **The creation of a new enforcement agency called the California Privacy Protection Agency.**

For further discussion on these changes, read our summary here.

For the most part, the new law does not become effective until January 1, 2023. However, employers and businesses that meet the criteria for coverage under the CCPA are still required to comply with the CCPA until then. The CPRA does extend the exemptions of the majority of CCPA rights applying to job applicants, employees, and independent contractors and in the business-to-business context until January 1, 2023. With the exception of the right to access, the CPRA will only apply to personal information collected by businesses on or after January 1, 2022.

The CCPA And CPRA Pave The Way For Further Litigation

While the CPRA creates a new agency to enforce the CCPA and CPRA starting on January 1, 2023, employers and businesses should be wary of CCPA-related litigation and enforcement actions that have already begun, as well as additional litigation that will inevitably result from the CCPA and CPRA. Under the express language of the CCPA, with the exception of some carve-outs for data breaches, nothing in the CCPA was to be interpreted to provide a basis for a private right of action under any other law.

However, the CCPA proceeded to create ambiguity by stating that such a pronouncement "shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution." This ambiguity still exists under the CPRA. Employers should therefore expect plaintiffs' attorneys to argue that the CCPA and CPRA can provide a basis for both wrongful termination claims by employees and claims under California's Unfair Competition Law.

The CPRA explicitly makes it unlawful to retaliate against an employee, job applicant, or independent contractor for exercising their rights under the CCPA and CPRA. The good news for employers is that this provision does not go into effect until January 1, 2023, at the same time that the majority of CCPA and CPRA rights become effective for employees, job applicants, and independent contractors.

However, we can expect that employees will argue that exercising their CCPA rights is a protected activity for purposes of alleging a wrongful termination cause of action. Employers and businesses who are actually sued, regardless of the type of cause of action, will also likely see plaintiffs'

attorneys using and abusing the right to access to circumvent traditional discovery methods to obtain information regarding their clients.

Additionally, employers and other businesses will likely see an increase of cases brought under California's Unfair Competition Law (UCL), citing not just to the anti-discrimination and anti-retaliation provisions of the CCPA and CPRA, but to any violation of the CCPA and CPRA. The UCL provides a private right of action for any unlawful business act or practice. A party bringing a UCL claim can seek an injunction against further unlawful activity, disgorgement of profits, and attorneys' fees.

Several lawsuits have already been filed in California under the UCL that are based on alleged violations of the CCPA. This appears to be the current approach of plaintiffs' attorneys for circumventing the CCPA's limitation on private rights of action for CCPA violations other than a data breach. While private litigants cannot seek the same penalties under the CCPA as the Attorney General can in an enforcement action, they have taken the position that the UCL gives them the right to pursue monetary restitution, injunctive relief, and attorneys' fees to remedy violations of the CCPA.

Uncertainties Abound As To What The CPRA-Created Right To Correct Inaccurate Information Will Mean For Employers

Under the CCPA, consumers who are California residents have the right to request access and deletion of their personal information, in addition to opting out of the sale of their personal information. These rights have not gone into effect for employees, job applicants, and independent contractors who are natural persons, and they are delayed until January 1, 2023 under the CPRA. The CPRA, however, creates an additional right that consumers and employees will be able to exercise starting on January 1, 2023 — the right to correct inaccurate information.

The CPRA says little about how this right to correct will work in practice. The CPRA states that the nature of the personal information and the purposes for which the information is collected will be taken into account but the CPRA fails to explain how they will be taken into account. Likewise, the CPRA states that a business "shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer," but the CPRA fails to explain what constitutes reasonable efforts.

The right to correct inaccurate information is of particular concern for employers. Among questions employers will have is what information are employees allowed to request to correct? Can employees argue that the CPRA gives them the right to correct their personnel records — including discipline records or performance reviews — when they disagree with their employer's version of events? Can an employee request a correction of findings into investigations of employee misconduct? If the employer's investigation found that an employee engaged in theft, timecard fraud, or sexual harassment, will this employee have a CPRA right to request that the employer correct the record to their liking and then claim retaliation for exercising their CPRA right? The CPRA does not provide answers to any of these questions.

Ultimately, employers and businesses will need to wait until regulations interpreting this right to correct are drafted for answers to these questions. The CPRA has specifically deferred to the California Attorney General or the California Privacy Protection Agency to create regulations to address, among other issues, "requests for the correction of accurate information," "how concerns regarding the accuracy of the information may be resolved," and "the steps a business may take to prevent fraud."

CCPA Exemptions Applicable to Employers and Business-to-Business Transactions Extended, But Only Briefly

By no later than January 1, 2023, businesses subject to the CPRA must implement mechanisms to provide their employees, job applicants, independent contractors, and individuals currently covered by the business-to-business exemption the rights to access, delete, or opt out of the sale of their personal information. The business-to-business exemption states the certain rights under the CCPA do not apply to individuals who are acting in the capacity of employees, owners, or representatives of any entity (whether for-profit, non-profit, or government) when communicating with or providing their personal information to a business covered by the CCPA.

Currently, there is no guidance on how businesses are expected to apply the CCPA and CPRA to these exempted groups. For example, the "right to delete" may be meaningless in the employment context, as employers will almost always have a legitimate reason that satisfies one of the exceptions to the right to delete. Employers are legally required to keep many employment-related records, so why create a system for employees to submit deletion requests that will routinely be declined? This is especially problematic in light of the anti-retaliation provisions, as disgruntled employees could attempt to insulate themselves from employer discipline or termination by engaging in protected activity and exercising their CCPA and CPRA rights.

That said, the California Privacy Protection Agency may promulgate regulations providing guidance on how these rights will apply in the employment context. Employers should keep an eye on the activities of the California Privacy Protection Agency and plan to start creating policies and procedures to apply the CCPA and CPRA to these exempted groups once such regulations are issued.

Data Minimization

An important new requirement for businesses subject to the CPRA is data minimization. This has never specifically been required by pre-existing California law, including the CCPA. The CPRA states that a business should only collect and use a consumer's personal information to the extent "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." This of course leaves room for debate on a case-by-case basis on whether a business actually needs to collect certain information or is collecting more than what it needs. The CPRA also prohibits a covered business from retaining personal information "for longer than is reasonably necessary" for the purpose for which it was collected. Exactly how long a piece of information should be kept will depend on several factors, and there is no one-size fits all answer.

The addition of this new requirement in the law means that businesses without a comprehensive data retention policy should consider adopting one. The best practice is to begin with mapping all your data and taking an inventory of what data you collect, what you use it for, and where you store it. This should also involve auditing whether you really need to collect all this data. Some of the data may be subject to minimum or maximum retention periods under applicable state or federal law. But for most of the data an average business might have, there will not be an applicable law or regulation prescribing exactly how long the data must be kept. Generally, an appropriate retention period would be a function of (a) any legal retention requirement, (b) the statute of limitations for any potential claim to which the data may be relevant, and (c) any other ongoing business objective for which the data may be needed.

Next Steps For Employers And Businesses

Although the CPRA does not go into effect until January 1, 2023, employers and businesses need to act now to bring themselves into compliance. Parts of the CPRA have a look-back period to January 1, 2022, and it can take six to 12 months for businesses to achieve full compliance — hence the need to start on your compliance journey today.

In addition, the CCPA has been in effect since January 1, 2020, and businesses subject to the CCPA are still obliged to comply with its provisions now. In other words, you do not get a reprieve from the CCPA until 2023. Under the CCPA, businesses which fail to take reasonable security measures to protect personal information of consumers may be liable for damages of $100 to $750 per consumer per incident or actual damages, whichever is greater. And businesses that fail to comply with other provisions of the CCPA may face enforcement actions by the Attorney General and penalties of up to $7,500 per violation.

Businesses will need to start thinking about how they will comply with the provisions of the CPRA effective January 1, 2023. Even businesses who are currently compliant with the CCPA will need to take further steps to bring them into compliance with the CPRA, including:

- Evaluating whether the CPRA will apply to them under amended criteria determining applicability;
- Updating notices to consumers, including employees, job applicants, and independent contractors;
- Updating a business's website and privacy policy to comply with new requirements under the CPRA;
- Creating mechanisms for employees, applicants, and independent contractors to exercise their full range of CCPA and CPRA rights; and
- Creating mechanisms to delete or destroy personal information for which they no longer have a business reason to retain.

Given the far-reach of the CCPA and CPRA, regional businesses need to consider to what extent they want to interact with the California market and thereby subject themselves to California privacy laws. Businesses with fairly minor ties to California that would still be subject to the CCPA and CPRA may want to evaluate whether they can and should take steps to cut their ties with California in order to avoid the long-arm of state privacy rights.

Compliance by the January 1, 2023 deadline will be imperative for business because of the creation of the California Privacy Protection Agency, which along with the California Attorney General may investigate and ultimately prosecute violations of the CCPA and CPRA. Businesses could face administrative or civil fines of up to $2,500 for each violation, or $7,500 if a violation is deemed intentional or involves minors. Businesses should be aware that, in the absence of any regulations stating otherwise, a violation could be deemed to be "per consumer."

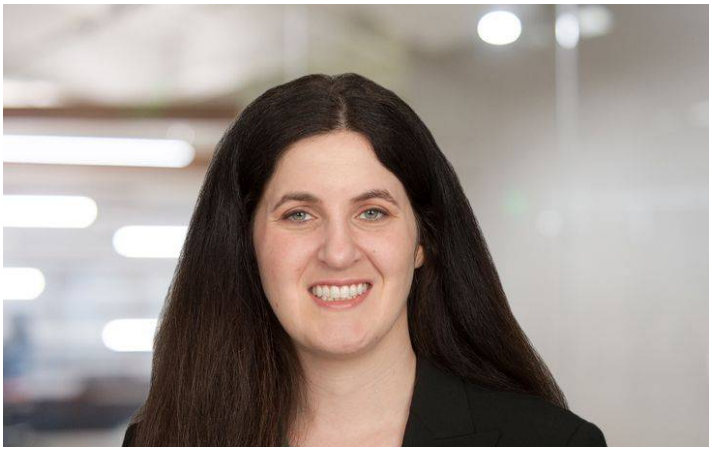
Bringing a business into a compliance with the CCPA and CPRA is a lengthy process even for the most diligent of businesses. Employers and businesses should start early to make sure that they are ready to be fully compliant by January 1, 2023.

Conclusion
Fisher Phillips will continue to monitor this situation and provide updates as appropriate. Make sure you are subscribed to Fisher Phillips' Alert System to get the most up-to-date information. For further information, contact on attorney in the Fisher Phillips CCPA Task Force, any attorney in any of our California offices, or any member of our Privacy and Cyber Practice Group.

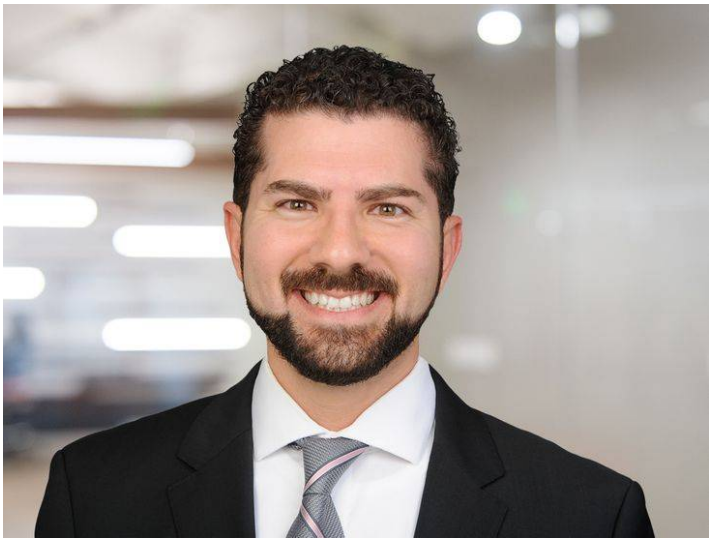
To Learn More, Register For November 16 Webinar
To learn more about the impact of Prop 24 on your business, join members of the Fisher Phillips CCPA Task Force for a webinar on November 16, 2020, 11am-12pm PST. Register by clicking **HERE**.

This Legal Alert provides an overview of a specific new state law. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People



Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Trending

CCPA Resource Center

Related Offices

Los Angeles

Irvine

Sacramento

San Diego

San Francisco

Woodland Hills