California Initiative To Amend State Privacy Law Qualifies For November Ballot

Insights
6.25.20

California's landmark privacy law could soon be amended with updated compliance burdens for employers – and it will be up to voters statewide to determine whether these changes take effect. An amendment to the California Consumer Privacy Act (CCPA), titled as the California Privacy Rights Act (CPRA), has just qualified to appear on the November 3, 2020 statewide ballot. If voters approve the measure, the CPRA would require covered businesses to implement policies and procedures to provide consumers—including employees—with certain privacy rights. What do California employers need to know about this development to prepare for a possible revision to their compliance obligations?

Background On State Privacy Law
The CCPA went into effect on January 1, 2020. Among the privacy rights codified by the statute, covered businesses are now required to provide disclosures to consumers and implement reasonable security measures to safeguard personal information. However, additional CCPA obligations for employees, job applicants, and independent contractors are on hold until January 1, 2021.

For further discussion on the CCPA's obligations, read our firm summary here.

What Changes Would CPRA Bring?
The good news for employers is that, if the CPRA is passed by the electorate in November, employers will have until January 1, 2023 to prepare to provide employees with the full range of CCPA rights (although disclosures would need to be updated before then). In fact, businesses would have until January 1, 2023 to bring themselves into compliance with all of the CPRA's amendments.

However, if approved by voters, the CPRA would make numerous substantive changes to the CCPA, some of which will increase the burden on businesses seeking to comply with the CCPA. These changes would include:

- 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 for consumers to request correction of inaccurate personal information; and
- The creation of a new enforcement agency called the California Privacy Protection Agency.

The CPRA would also limit how the legislature can amend the CCPA in the future, requiring that all future legislation be "consistent with and further the purpose of the CPRA." In other words, state lawmakers may be reluctant to attempt to address practical implementation problems or ambiguities in the CPRA for fear it may lead to litigation regarding whether the legislature has the right to do so.

What Should Employers Do?

While businesses may not need to worry about new obligations under the CPRA until January 1, 2023, businesses that are not already compliant with the CCPA should act now. One provision of the CPRA that is not stayed until 2023 would be the creation of the California Privacy Protection Agency. While the California Privacy Protection Agency could not investigate complaints and bring administrative actions until January 1, 2023, it would assume rulemaking responsibility for the CCPA, promote the CCPA, and provide guidance to consumers about their rights under the CCPA. For this reason, businesses may see both changes to CCPA requirements and a greater consumer awareness before 2023 if the CPRA passes.

Moreover, the CPRA ballot initiative does not change that businesses needed to be compliant with the CCPA as of January 1 of this year. While the California Attorney General has not started enforcing the CCPA yet, he will start doing so in a matter of days – on July 1, 2020. Businesses that are non-compliant could face penalties up to $2,500 for each violation or $7,500 for each intentional violation. And as of now, it is not clear whether a violation means per business or per consumer whose CCPA rights were violated. Businesses face further liability if there is a security breach because of a failure to take reasonable security measures.

For these reasons, businesses subject to the CCPA should have implemented or be implementing the following action items:

- Provide disclosures required by the CCPA to consumers, including employees;
- Draft a CCPA-compliant privacy policy;
- Implement measures for consumers to exercise their CCPA rights; and
- Implement reasonable security measures required by the CCPA.

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 your Fisher Phillips attorney, any attorney in any of our California offices, or any member of our Privacy and Cyber Practice Group.

This Legal Alert provides an overview of a specific developing situation. 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

Service Focus

Consumer Privacy Team

Privacy and Cyber

Trending

CCPA Resource Center

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills