Insights, News & Events

CALIFORNIA REGULATORS TAKE LEAP FORWARD IN CREATING ROBUST PRIVACY PROTECTION RULES

Insights
Jun 1, 2022

The next step in drafting the long-delayed privacy regulations for the California businesses subject to the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA) took place late last week – and businesses need to start preparing because the California Privacy Protection Agency has made clear it wants the regulations to give the law real teeth. Some of the key items addressed in the proposed regulations released on May 27 include guidance on the new rights created by the CPRA, a limitation on how businesses should use website interfaces and content to persuade consumers not to exercise CCPA/CPRA rights, and information on addressing opt-out signals for websites.

What is not in the proposed regulations are any limitations on CCPA/CPRA rights for employees, job applicants, or independent contractors, and no extension of the current partial exemption for those individuals. Therefore, businesses must prepare to fully comply with all CCPA and CPRA obligations for employees, job applicants, and independent contractors come January 1, 2023. What do you need to know about this latest step and how can you prepare for this fast-approaching date?

California Privacy Protection Agency Would Have Sweeping Investigatory Powers

If the proposed regulations are adopted as drafted, the Agency will have a large base from which it can decide to open an investigation. Not only will the Agency be able to open an investigation based on information from sworn

Related People

Darcey M. Groden, CIPP/US

Partner

858.597.9627

Service Focus

Consumer Privacy Team

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

affidavits under penalty from the general public, it will have the power to initiate an investigation based on referrals from other government agencies, private organizations, and even nonsworn or anonymous complaints.

Further, the Agency will have the authority to audit business for CCPA/CPRA compliance. Currently, the proposed regulations provide three scenarios under which an audit may be conducted:

- to investigate possible violations of the CCPA/CPRA,
- if a business's processing of personal information presents significant risk of consumer privacy or security, or
- if the business has a history of noncompliance with the CCPA/CPRA or any other privacy protection law.

This provides a couple of takeaways for businesses. First, it is not clear what constitutes "significant risk of consumer privacy or security," but it seems likely that personal information which is considered "sensitive personal information" may fall into that bucket. Sensitive personal information includes things such as social security numbers, driver's license numbers, precise geolocation, certain financial information, racial or ethnic origin, and union membership. For this reason, businesses should scrutinize what sensitive personal information they have, whether they need it (employers do for at least some sensitive personal information collected about employees), and make sure their privacy policies and practices ensure adequate security for it.

Second, businesses should take care not just to ensure their CCPA/CPRA compliance, but to determine whether there are any other privacy protection laws in California or elsewhere they are subject to – and whether they are in compliance with them as well. Currently, four states in addition to California have comprehensive data protection laws that are scheduled to go into effect in the near future. This is on top of other more narrowly targeted consumer protection laws on the federal level, in California, and in other states – noncompliance with them could make a business a target for an audit in California.

Other Big Changes in the Proposed Regulations

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

The draft proposed regulations are a whopping 66 pages long. While some of the information in them restates prior regulations, reorganizes prior regulations, or strikes out language from prior regulations, there is too much to comprehensively address here. Nevertheless, here are some highlights that businesses will need to address:

1. Your business will need to revisit the language and functionality of notice banners, submitting CCPA/CPRA requests, and obtaining consumer consent. The proposed regulations provide a lengthy description of what constitutes "dark patterns" – user interfaces designed to manipulate or subvert consumer choice. Having options on a website that are "Yes" and "Ask me later" (rather than "Yes" and "No"), defaulting into a choice that is considered less protective of privacy, and manipulative language (such as making a consumer click through reasons why opting out of the sale of personal information is a bad choice) are all dark patterns under the proposed regulations. The buzzwords to avoid dark patterns are "balance" and "symmetry in choice" – options that are considered less protective of privacy rights cannot be promoted over more protective options.

2. You will need to incorporate updated requirements into your notices and privacy policies. In addition to some technical changes to these documents required by the new regulations, you will need to incorporate new rights such as the right to limit the use of sensitive personal information and the right to correct inaccurate information. Additionally, you will need to familiarize yourself with the requirements for how to act on the rights to limit the use of sensitive personal information and how to correct inaccurate personal information.

3. The regulations establish rules for opt-out preference signals for online consumers to opt-out of the selling or sharing of their personal information. You will need to become familiar with the requirements, including how to notify consumers their opt-out signal was honored and how to reconcile situations where the opt-out signal conflicts with other preferences the consumer has shared with a business. You should plan to start early on working with your IT vendors to ensure that you have this buttoned up ahead of 2023.

How the Sausage Is Made

For those interested in the procedural background about how these proposed regulations came to be and what comes next, this section is for you. The CPRA mandated that final regulations be adopted by July 1, 2022. While it seems likely the Board will vote to provide a notice of proposed rulemaking at the Agency's upcoming June 8 Board Meeting, it is not feasible that final regulations will be adopted by the July 1 date. More realistically, the earliest date for having final regulations is August.

Here is a very basic timeline of what we should see coming:

- The Board will need to vote to publish a notice of proposed rulemaking to the public.
- There is then at least a 45-day public comment period, although the Board can choose to have the public comment period be longer. There will additionally be a public hearing for comments to be made.
- Based on the comments, changes could be made to the proposed regulations. If the changes are major, there needs to be a new 45-day public comment period. If the changes are substantial and sufficiently related to the prior draft of the regulations, there is a minimum 15-day comment period. If there are no changes or the changes are nonsubstantial and sufficiently related to the original regulations, then there is no comment period. (This last one is incredibly unlikely.)
- If multiple sets of changes are made, each set is subject to the 45-day, 15-day, or no-public-comment period as set forth above. (The original regulations promulgated by the California Attorney General had one 45-day public comment period and two 15-day public comment periods because there were two sets of modifications.)
- Once the regulations are final, Agency staff will prepare the final package, including the Final Statement of Reasons and responses to all public comments. The Board will then approve the filing of the final package with the Office of Administrative Law (OAL). When approved by OAL, the regulations will be filed with the Secretary of State with a published effective date thereafter.

What all this means is that businesses should expect to have to wait at least 60 days — possibly longer — after the Board

votes to publish a notice of proposed rulemaking and gets the ball rolling.

It is also important to emphasize here that there may be further regulations coming later this year. The Board contemplated a second set of regulations to follow to address businesses' obligations to perform annual cybersecurity audits, businesses' obligations to submit regular risk assessments to the Agency, and automated decision making. This second set of regulations could potentially be published for review before the process to finalize this current set of proposed regulations has finished.

Next Steps

These regulations are far from final, and we likely will see some tweaking in response to the public comment period. However, businesses should not expect a wholesale rewrite or that they will be thrown out altogether. While businesses should wait until the regulations are finalized to update their notices and privacy policies, these regulations nevertheless provide some guideposts on what businesses should be doing now to prepare.

1. CCPA and CPRA compliance will require cooperation across the various departments or divisions that handle or collect personal information for a business. These will include, but may not be limited to, Human Resources, IT (or whoever handles a business's website), and any consumer-facing departments. If your business has not yet identified key stakeholders, you need to do so and loop in representatives from these stakeholder departments to assist with CCPA/CPRA compliance.

2. Your business should update and assess its data inventory. Data inventories are not limited to information coming through any one department, and they should involve a broad look across the entire business (thus, why it is important to have stakeholders from various departments). In updating your data inventory, you should take special care in ensuring that your data inventory is complete, identifies which data is sensitive personal information under the CPRA, includes inferences about consumers, and includes all uses for personal information. This data inventory will be a backbone towards drafting updated notices and complying with consumer requests to exercise CCPA and CPRA rights.

3. Your business should implement data minimization standards, including creating a data retention policy. The new CPRA requirements mandate that notices to consumers explain how long businesses will keep personal information, which in turn means you need to evaluate how long to keep personal information and then put that down into a data retention schedule. However, it is not enough to have a policy in writing on how long to keep information — you need to work through the process of how you will actually purge stale data on a large scale (as compared to deleting personal information in response to individual consumer requests).

The latter two steps are foundational to CCPA and CPRA compliance, even if every aspect of a step is not explicitly mentioned in the statute. Businesses that undertake these steps will better understand the lifecycle of the personal information going through their business, will be poised to leverage that information for CPRA compliance, and will find complying with the remaining portions of the regulations less daunting given their better understanding of the personal information within their possession.

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, the author of this Insight, any 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.