California Agency Provides Insights into CCPA Enforcement Priorities: 3 Tips for Staying Off the Enforcement Radar

Insights
8.01.24

A recent board meeting of state officials revealed that the California agency responsible for overseeing the state's landmark consumer privacy law received over 2,000 complaints for alleged violations in the past year alone – and provided a glimpse into what its enforcement priorities will be in the year ahead. The July 16 meeting for the California Privacy Protection Agency recounted the 2,176 complaints received over potential California Consumer Privacy Act (CCPA) violations and reviewed how such complaints shape the Agency's enforcement priorities. Here is what businesses need to know to avoid getting caught in the enforcement crosshairs – and three steps you can take to put yourself in the best position.

Enforcement Priorities

At the latest board meeting, Michael S. Macko, the Agency's Deputy Director of Enforcement, provided an inside look into what the Agency's enforcement priorities have been and will be moving forward. To date, it has been focused on CCPA-required privacy notices and policies; the right to delete and whether businesses are adequately responding to and complying with deletion requests; and the implementation of a process for responding to consumer requests.

Moving forward, the Agency will focus enforcement on:

- Improperly requiring consumers to **verify their identity to opt-out of the selling or sharing of consumer data** or to limit the use of sensitive personal data. (Businesses are not permitted to verify an identity on such requests. If you have a good faith, reasonable, and documented belief that such a request is fraudulent, you may deny the request. But the onus is on the business to explain why it believes the requestor is not who they say they are rather than on the requestor to prove their identity.)
- Failing to provide **notice to consumers** about the sale or sharing of personal data. Remember that in the context of the CCPA, "sale" means disclosure of data to a third party that is not a service provider or contractor (meaning not a vendor restricted contractually from using or disclosing the data outside the scope of services provided) in exchange for monetary or other valuable consideration. And "sharing" means disclosure of data for purposes of cross-context behavioral advertising (i.e., targeted ads).

- Violating the CCPA in a manner that targets or affects **vulnerable groups** (such as minors under 16).
- Issues addressed in **Enforcement Advisories**. (The Agency issued its first Enforcement Advisory earlier this year focusing on data minimization.)

Dark Patterns Emerge as Newest Priority

One additional enforcement priority mentioned was the use of dark patterns to prevent consumers from asserting their rights under the CCPA. Dark patterns are user interfaces that subvert or impair a user's ability to make a choice or decision regarding the use of their personal information.

The CCPA defines a dark pattern by what it is not – that is, if your consumer request process and consent mechanisms do not embody the following principles, you may have a dark pattern. Here are principles businesses should keep in mind to avoid dark patterns:

- Use language that is easy to understand – avoid legalese or hyper-technical language.
- Symmetry in choice. If you provide a "yes" or "accept" option, you need to provide a "no" or "reject" option. It cannot be harder or more time-consuming to exercise a choice that is more privacy-protective.
- Avoid language or interactive elements that are confusing.
- Avoid choice architecture that impairs a consumer's ability to make a choice. Requiring a consumer to click through multiple screens or bundling options may be considered interference.
- Easy to execute. Avoid circular or broken links or links that do not clearly lead to what a consumer is seeking to do.

Next Steps: 3 Steps to Consider

1. Review Your Consumer Response Practices. Several of the enforcement priorities – in one way or another – get at the consumer response system. The CCPA has specific requirements and deadlines that govern the consumer response process, and the requirements on how to respond differ from request-to-request. (There are over 20 pages of regulations relating to consumer requests!) It is important that your business familiarize yourself with the process and be able to comply. If you do not have a manual that outlines your process in detail, consider having your privacy counsel (like Fisher Phillips) prepare one for you.

2. Ensure Your Notices and Privacy Policies are Complete and Accurate. Notices and privacy policies should accurately describe your business practices, including the categories of personal information you collect, who you disclose it to, and how you use it. Moreover, the CCPA requires privacy policies to be updated at least once annually. If your privacy policy is more than one year old, you must update it.

3. Review Your Website for Dark Patterns. Take a close look at your website with an eye towards the five principles of what does not make a dark pattern discussed above. More than that, take your website for a test drive. Has someone checked all the links and contact points in the privacy policy and related to consumer rights work? Have you asked someone unfamiliar with the website to try to exercise consumer rights and confirmed they are able to do so?

Conclusion

Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information directly to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team. You can also visit our firm's CCPA Resource Center at any time.

Related People

Darcey M. Groden, CIPP/US
Associate
858.597.9627
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Alexandra Volpicelli
Associate
415.926.7650
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills