Your Business's Mobile App Could Be Subject to California Attorney General Investigation

Insights
1.31.23

The California Attorney General just announced an investigative sweep of mobile apps that allegedly fail to meet the requirements of state data privacy law, meaning businesses that conduct business through apps need to immediately ensure they are compliant with the latest laws and regulations. And given that California data privacy law impacts businesses across the country, you might not be spared just because you don't have a physical location in the state. Timed to coincide with January 28's Data Privacy Day – the annual day aiming at raising awareness and promoting best practices surrounding digital privacy and data protection – you should use the warning as an important reminder to determine whether you are selling mobile data and have a mechanism for users to opt out of such sales. For businesses with a mobile app, what do you need to know about the California Consumer Privacy Act's (CCPA) requirements pertaining to the sale of personal information and consumers' related rights?

Is Our App Really Selling Personal Information?

The first thing you should determine is whether your business's app is selling personal information. Your first instinct might be to answer in the negative, but you should take a second look. After all, the CCPA is a law full of everyday terms that do not align with how we use the words in everyday conversation.

To understand what the California Attorney General is enforcing with these new investigations, start with how the CCPA defines two key terms:

- "Personal information" is broadly defined to include any data that identifies or is reasonably capable of being linked to a California resident or household. Specific examples include names, Internet Protocol address, and unique personal identifiers.
- "Selling" is the exchange of personal information for monetary or other valuable consideration.

With these definitions in mind – and assuming you are not literally providing your app data in exchange for money – let's discuss some common ways in which your app may be selling personal information but for other valuable consideration besides money.

Scenario 1: If you have third-party advertising on your app that makes available personal information of app users (such as username, device ID, IP address, or any other unique identifier that tells the app that someone is a specific user) to the third party that placed the ad, then you are selling personal information.

Scenario 2: Your app uses a third party to run data analytics on app user activity. Even if you do not personally see, possess, or have access to the analytics data, that does not mean the third party does not sell the data collected from or about your app users, or that the third party does not use this data for its own commercial purposes outside the scope of the services provided to your business. Even if you are paying the analytics provider for the analytics service (or even if you are not paying them for services), you may still be selling personal information to the analytics provider if that third party is not contractually restricted from using the data about your app users for its own purposes.

What Should We Do?

Selling personal information under the CCPA is not unlawful. But if you determine that you are doing just that through your mobile app, there are hoops that you need to jump through to comply with the law.

- First, you need a just-in-time notice that directs or refers the user to your privacy policy and a copy of your privacy policy readily accessible to users in the app.
- Second, your privacy policy (both in the app and on your website) must disclose that you are selling personal information.
- Third, you must implement methods for your users to effectively opt out of the sale of personal information.

If you do not want to deal with the fuss of opt-outs, you can avoid having some of the data disclosure being considered a sale by entering into a service provider agreement that prevents any third parties from using data they receive or process about your app users for purposes outside of providing you services (assuming the third party providing you services is amenable to such restriction).

But be aware, if your app is providing data to be used for cross-context behavioral advertising (e.g., targeted advertising), that is also considered "sharing" under the CCPA starting as of January 1 of this year – and you must still provide opt-outs for that. And, regardless of whether you stop selling (or sharing), you still need to note in your privacy policy that you sold or shared personal information within the last 12 months and provide a link to your privacy policy in your app if you are collecting any personal information.

What About the Authorized Agent Portion of the AG Sweep?

For businesses unfamiliar with the "authorized agent" requirement of the CCPA, you should know that a new cottage industry has sprung up that is engaged by consumers to act as their authorized

agent in submitting CCPA requests. The law gives consumers the right to make various CCPA requests through an authorized agent – that is, a third party designated by the consumer to make the request on their behalf. If you are unceremoniously rejecting any CCPA requests not made by the consumer themselves, you should stop.

You also should familiarize yourself with the CCPA requirements for authorized agents, including what you can and cannot ask for of the authorized agent – and make sure your privacy policy addresses how authorized agents can make a request on a consumer's behalf.

Is There Anything Else We Should Know?

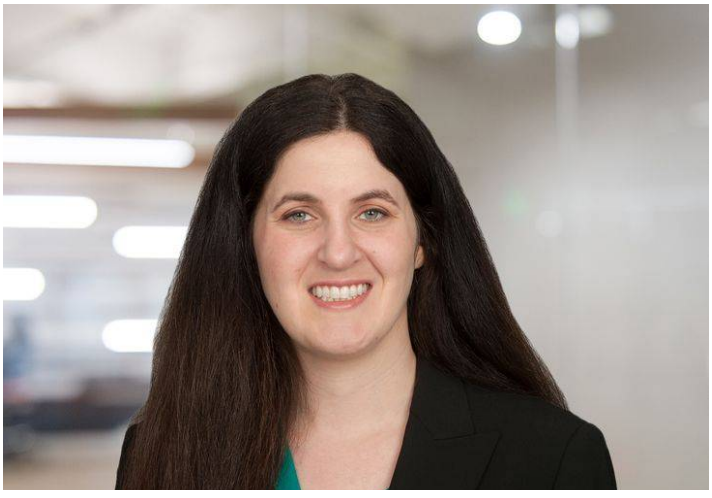
If you have not updated any of your policies or practices related to the CCPA since the law first went into effect, now is the time. The California Privacy Rights Act – which significantly amends the CCPA – just went into effect on January 1. While the California Attorney General's current enforcement actions appear to be focused on rights that existed prior to the recent amendment, at some point that will change – and you will want to be ready!

More generally, businesses everywhere should be mindful that CCPA enforcement is ongoing, even though the latest CCPA amendment that took effect January 1 will not be enforced by the new agency established by this amendment until July 1. If your business is subject to the CCPA and has not taken steps to comply, now is the time.

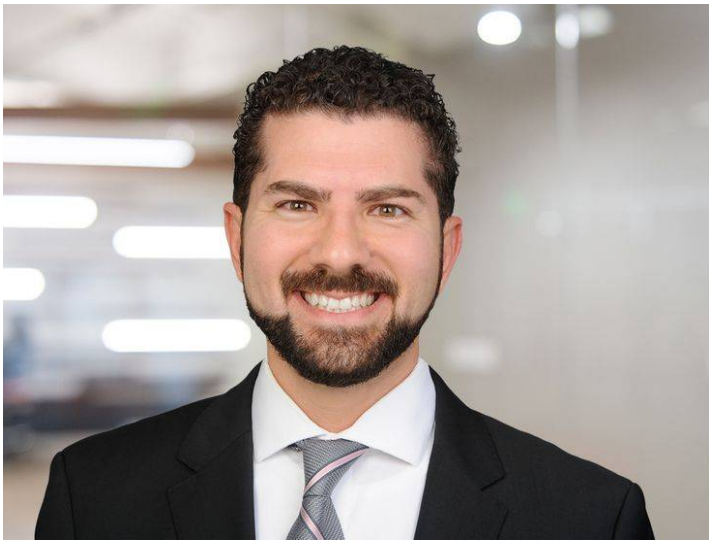
Conclusion

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 direct 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

Service Focus

Consumer Privacy Team

Privacy and Cyber

Trending

CCPA Resource Center