Google Halts Plan to Phase Out Third-Party Cookies: 3 Essential Next Steps for Businesses

Insights
8.15.24

Google no longer plans to remove third-party cookies from its web browser, according to a July 22 announcement. Instead, the tech giant will explore other options that allow users to make informed choices that apply across their web browsing, while also preserving an ad-supported internet. This has implications for businesses that engage in online marketing or find themselves at increased risk of facing a website privacy lawsuit — a trend that's on the rise in about 20 states. Here's what you need to know and three essential steps to consider taking now.

How Did We Get Here?

Google first announced its plan to phase out third-party cookies back in 2020, and it hoped to finalize the plan by 2022. At the time, Google set in motion a new enterprise, Privacy Sandbox, that would develop a set of open standards to fundamentally enhance web browsing privacy, while also supporting publishers. Its goal was to support privacy-preserving and open-standard mechanisms to ultimately render third-party cookies obsolete. This reconfiguration would have caused a dramatic shift in the ad-industry and the internet economy as a whole.

This, of course, did not happen in 2022 or beyond, as delays continued due to industry pushback, technical challenges, and evolving laws and regulations. The latest delay extended Google's timeline to 2025, but difficulties ultimately forced the company to end its push to remove third-party cookies from its browser.

What Happens Next?

While Google has announced that it no longer intends to remove third-party cookies from Chrome, it will continue to develop and test its Privacy Sandbox initiative and seek other privacy-preserving alternatives.

While these alternative privacy-preserving approaches may be viable in the future, businesses should continue to comply with applicable privacy law consent and notice requirements for the time being, including cookie notices, disclosures, and opt-in or opt-out options. It's also a good idea to review your website to identify what third-party cookies are in use. This is especially true given the dramatic rise in wiretapping suits filed against businesses that host third-party cookies.

3 Steps to Consider Taking Now

1. Review Your Website

Take a close look at your website to evaluate what pixels, web beacons, cookies, and other tracking tools are being used. Identify what data each tracking tool is disclosing and who is receiving it. Ascertain what third parties are doing with your data once they receive it. You should note that to do all this effectively and comprehensively would require using cookie scanning technology with the assistance of an expert to interpret the results and advise on an action plan. Fisher Phillips, or your privacy counsel, can help you accomplish this task.

2. Display Appropriate Disclosures

Before the consumer provides any information on your website — for example, through a search bar, a contact form, or chat feature — ensure your website includes disclosures that adequately describe the parties to the communication, who will receive the data, the further use (if any) of the data, and where your consumers can access information about your privacy and data use practices.

3. Consider Privacy Preserving Technologies

Many of the state comprehensive consumer privacy laws either recommend or require (in certain circumstances) the adoption of privacy preserving technologies on websites, like Global Privacy Controls (GPCs) or HTTP header field or JavaScript objects. Such technology would allow a user to set their browser to send an automatic signal to each website they visit telling the website that this user does not wish to have any data that can identify them collected or disclosed through cookies. If your website enables or accepts GPCs, the website would automatically accept the user's preset signal and comply with the user's choice without requiring the user to further select cookie choices upon navigating to the website. Depending on your organization's data practices, you may be required, and should at least consider, implementing automated ways to acknowledge consumer opt-out preference signals.

Conclusion

Fisher Phillips will continue to monitor Google's plans to implement privacy-preserving features while maintaining the use of third-party cookies. We will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System 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

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

David Shannon, CIPP/US

David Shannon, CIPP/US
Associate
415.926.7640
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

CCPA Resource Center