# The end of Third-Party cookies

Pressure from regulators and consumers has led many within the tech industry to declare third-party cookies will soon come to an end. In this section we will discuss the changes that major players are doing and how it will impact digital advertising market.

## Why third-party cookies are going away?

3rd Party Cookies power all the ways we track, target, and measure performance in digital advertising. However, they track users silently. As an industry, we didn't do a great job of educating users how and why we use cookies. And we didn't give people a way to opt-out.

As a consumer, you have little control over who is collecting this information or where it is going—you are able to clear cookies from your own browser, but you'll never be able to manage or delete servers holding third-party data that has already been gathered.

In response to the perceived lack of transparency and control for individuals, data breaches, and "creepiness" in advertising, privacy legislation from the EU and California now give users control over their data. Effectively, these policies give users the ability to block various tracking technologies or request the deletion of their data. Tech companies such as Apple and Mozilla have also responded by giving users control of how their data is used both within browsers and devices.

Implementing and increasing security features to protect the privacy of users is nothing new and has been going on for years now, and for the most part **website users will actually benefit from it**. One of the first companies to do so is Apple and Mozilla, while others are yet to follow.

## Full third-party cookie blocking by Safari

Apple first launched Safari Intelligent Tracking Prevention (ITP) within Safari on 2017, where it immediately set a new bar for web privacy standards on both desktop and mobile by blocking some, but not all, cookies by default.

With the beginning of spring of 2020 Apple launched a major update to its ITP, the privacy feature that allows the company's web browser to block cookies and prevent advertisers from snooping on your web habits. In simple sense - **Safari by default blocked all third-party cookies**. That means that no advertiser or website is able to follow you around the internet using the commonplace tracking technology.

To blocking third-party cookies across the board and by default, ITP now has safeguards against trackers using the very nature of tracking prevention as a way to keep tabs on users. The new feature set also ensures that websites and trackers can't use login IDs to digitally fingerprint users who might otherwise be using tracking prevention or other privacy tools.

# Firefox blocks third-party cookies

On 2019 Firefox announced that their Enhanced Tracking Protection will automatically be turned on by default for all users worldwide as part of the 'Standard' setting in the Firefox browser and will block known "third-party tracking cookies".

**Enhanced Tracking Protection** works behind-the-scenes to keep a company from forming a profile of you based on their tracking of your browsing behavior across websites — often without your knowledge or consent. Those profiles and the information they contain may then be sold and used for purposes you never knew or intended. Enhanced Tracking Protection helps to mitigate this threat and puts you back in control of your online experience.

Mozilla follows a different approach when blocking trackers and cookies than Apple does. Instead of blocking or limiting **all third-party** and **client side cookies** by default, Firefox uses the Disconnect list to determine whether a cookie should be blocked or not. This curated list contains thousands of known tracking companies and is updated on a regular basis. The reasoning behind this decision is **to keep the web experience as seamless and functional as possible**, since some cookies are crucial for web building.

# Chrome will block third-party cookies

It is not a surprise that with the changes that Apple and Mozilla launched Google would follow. The company revealed its "Privacy Sandbox" in August 2019, an initiative to personalize (or target) web ads while still preserving user privacy. In January 2020, Google announced that it hoped to block third-party cookies from its Chrome browser by 2022 — a move that other browsers, like Safari and Firefox, made years ago. Google has planned to replace third-party cookies with technology developed through Privacy Sandbox.

That's where Google's Federated Learning of Cohorts (FLoC) comes in, which Google says is a "privacy-first" and "interest-based" advertising technology. With FLoC, Chrome will keep track of a user's browsing habits across the web, and then place the user in various audiences, or "cohorts," based on those habits. Advertisers will then target their ads to cohorts, rather than an individual user. So if you're looking for a browser that doesn't collect your data for ads — as an individual or as part of an anonymous audience — you might want to try a different one. (By the way, you can turn off ad personalization, activity tracking, and delete the data Google has collected about you here.)

In many cases this development is a direct reaction to new security holes, workarounds, aggressive tracking and shady business techniques and will most likely continue in the future.

Finally, while Google says it is committed to developing and using ad tech that doesn’t rely on tracking and advertising to users, other companies are developing their own non-cookie tracking methods that do, and you could still be tracked by them when you use Chrome (or another browser). The core companies will be presented in another chapter.

---

Revision #5
Created 16 June 2021 05:27:38 by Gabriele
Updated 26 August 2022 12:21:37 by Gabriele