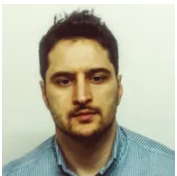


EX1052

Apple blocks third-party cookies in Safari

Safari becomes second browser after the Tor Browser to block third-party cookies by default for all users.



Written by **Catalin Cimpanu**, Contributor

March 24, 2020 at 3:30 p.m. PT

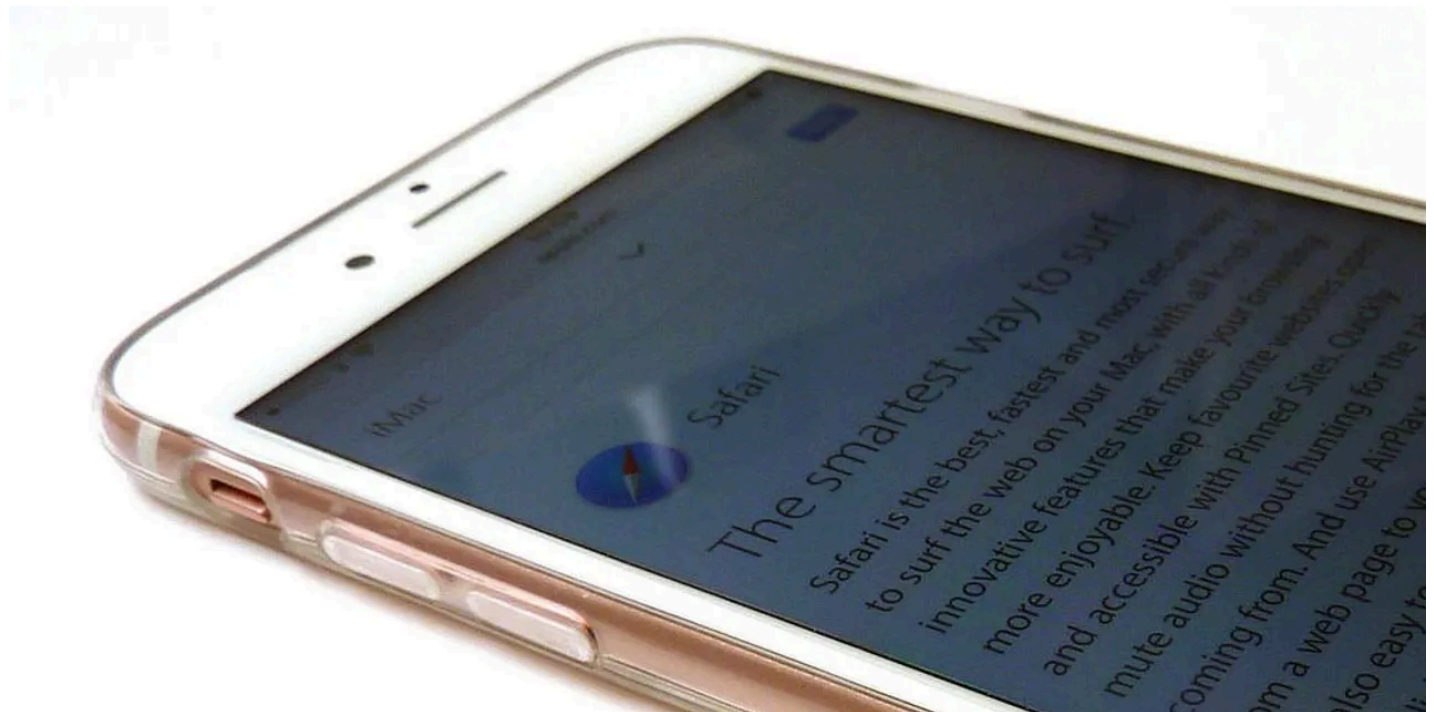


Image: Nobbby

Starting today, with the release of Safari 13.1 and through updates to the Intelligent Tracking Prevention (ITP) privacy feature, Apple now blocks all third-party cookies in Safari by default.

The company's move means that online advertisers and analytics firms cannot use browser cookie files anymore to track users as they visit different sites across the internet.

But Apple says the move isn't actually a big deal, since they were already blocking most third-party cookies used for tracking anyway.

"It might seem like a bigger change than it is," said John Wilander, an Apple software engineer. "But we've added so many restrictions to ITP since its initial release in 2017 that we are now at a place where most third-party cookies are already blocked in Safari."

Second browser to block third-party cookies for all users

Apple's Safari has now become the second browser -- after the Tor Browser -- to block all third-party cookies by default for all its users.

However, while Apple was quicker to block third-party cookies in Safari, Google is actually the one who pushed browser makers towards making this move in the first place, in a May 2019 blog post.

At the time, Google announced plans to block third-party cookies by default in Chrome and in the Chromium open-source project, on which multiple other browsers are built.

Google released Chrome v80 at the start of February with support for third-party cookie blocking (under the name of SameSite cookies), but the feature won't fully roll out to all Chrome's users until 2022.

Microsoft's Edge, which runs a version of Google's Chromium open-source browser has also begun gradually blocking third-party cookies as well, but the feature is not enabled by default for all its users either.

Apple's decision today doesn't mean that Safari now blocks all user tracking, but only tracking methods that rely on planting a cookie file in Safari and (re-)checking that cookie time and time again to identify the user as he moves from site to site.

Other user tracking solutions, such as user/browser fingerprinting, will most likely continue to work.

A small step forward for web privacy

Nonetheless, this is a major step in the right direction. With Google, Safari, Microsoft, and all the other Chromium-based browsers on board, now, the vast majority of current web browsers block third-party cookies or are on their way towards full blocks.

"This update takes several important steps to fight cross-site tracking and make it more safe to browse the web," Wilander explained in a Twitter thread today.

"First of all, it paves the way. We will report on our experiences of full third-party cookie blocking to the privacy groups in W3C to help other browsers take the leap.

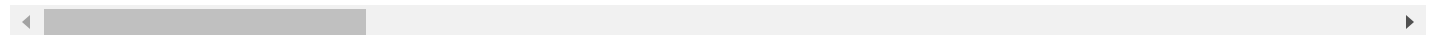
"Second, full third-party cookie blocking removes statefulness in cookie blocking.

"Third, full third-party cookie blocking fully disables login fingerprinting, a problem on the web described already 12 years ago. Without protection, trackers can figure out which websites you're logged in to and use it as a fingerprint," Wilander added.

"Fourth, full third-party cookie blocking solves cross-site request forgeries. This is one of the web's original security vulnerabilities and discussed in communities like OWASP for well over a decade. Those vulnerabilities are now gone in Safari."

More on the move and what it means to developers and website owners is available in [the WebKit team's blog post](#).

All the Chromium-based browsers

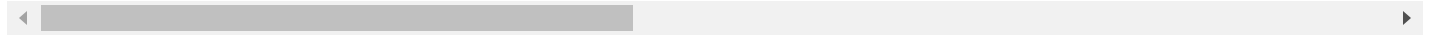


/ security

The best VPN services of 2024: Expert tested

How to turn on Private DNS Mode on Android (and why you should)

The best you can



 **Editorial standards**

show comments ↓

we equip you to harness the power of disruptive innovation, at work and at home.

topics

[galleries](#)

[videos](#)

[do not sell or share my personal information](#)

[about ZDNET](#)

[meet the team](#)

[sitemap](#)

[reprint policy](#)

[join | log in](#)

[newsletters](#)

[site assistance](#)

[licensing](#)

[accessibility](#)

© 2024 ZDNET, A Ziff Davis company. All rights reserved. **[Privacy Policy](#)** || **[Cookie Settings](#)** |
[Advertise](#) | **[Terms of Use](#)**