This iOS 26 Feature Can Give You More Privacy in Safari

Summary

iOS 26 introduced Advanced Tracking and Fingerprinting Protection in Safari, which obscures browser and device data to prevent digital fingerprinting. This feature, enabled by default for all browsing, helps protect user privacy from targeted advertising, price discrimination, and potential surveillance. While it enhances privacy, it may impact website functionality, so users can adjust the setting to Private Browsing or disable it entirely if needed.

Everyone can benefit from a little more online privacy.

Zachary McAuliffe Nov. 2, 2025 3:00 a.m. PT

Apple/Cole Kan/CNET

Apple released iOS 26 in September, and the update introduced a handful of new features to your iPhone such as call screening and new ringtones. The update also included some improved privacy measures against digital fingerprinting. Everyone can benefit from these advanced privacy measures on their device.

Because we do most things on digital devices these days, we may leave our digital fingerprints everywhere. CNET senior writer Attila Tomaschek told me that digital fingerprints consist of pieces of information about your device and browser, like your IP address, device type and even your screen resolution. He said fingerprints can be used for fraud detection as well as to improve website performance, but they can also be dangerous, which makes this iOS privacy feature so useful.

"Advertisers can build detailed profiles of users for targeted advertising, and companies may use fingerprinting for price

discrimination based on a user's location and other perceived demographics," he said. "Worse yet, an authoritarian government could leverage fingerprinting to surveil its populace, and digital fingerprints can help cybercriminals commit fraud and identity theft."

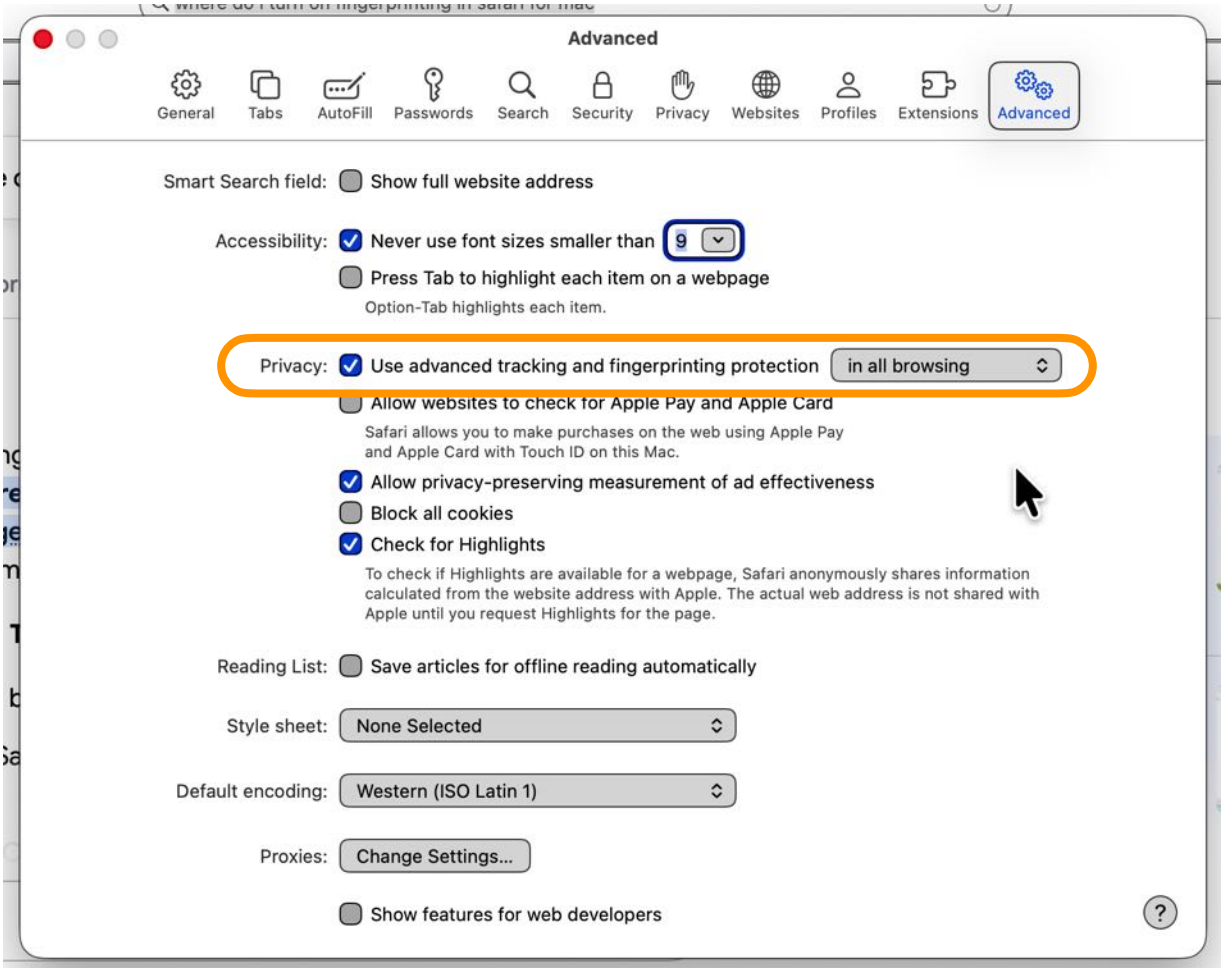
Companies can also sell these profiles to data brokers, who can take offline information from public records and other sources and attach it to your digital fingerprint. According to the cybersecurity company Avast, brokers could then sell this information to advertisers to target you more effectively.

Apple wrote online that these protections are enabled by default on all browsing. But here's where to find the setting to make sure you're getting the most privacy while using Safari or if you want to adjust the feature.

Note that your digital fingerprint is different from, and not related to, your biometric fingerprint.

Don't miss any of our unbiased tech content and lab-based reviews. Add CNET as a preferred Google source.

Where to find Advanced Tracking and Fingerprinting Protections



Editor's Note: The CNET article as published was not correct for macOS 26.3 indicating where to find instructions to modify the subject setting.The graphic shown above is correct and can be found at Safari **Settings**, **Advanced**, **Privacy**.

The Advanced Tracking and Fingerprinting menu will have ~~**two**~~ options **Private Browsing** and **All Browsing**. For the most protection, make sure All Browsing is selected -- it's signified by a check mark.

”Advanced Fingerprinting Protection, which was previously limited to Private Browsing, now protects all browsing in Safari," Apple wrote online. "It obscures browser and device data that can be used to create a digital fingerprint of users."

It's important to note that this setting applies only to Safari, so if you use another browser app, you might not get the same level of protection.

While blocking fingerprinting could help protect your data, there are some downsides to doing so. Tomaschek said fingerprinting can help websites remember your personal settings, so blocking this functionality could lead to a less convenient online experience. If blocking fingerprinting on all browsing is causing you too much of an inconvenience, follow the above steps and tap either **Off** to fully disable the feature or **Private Browsing** so it's only enabled when privately browsing.

Why are these protections important now?

Digital privacy and keeping your information secure are always important, but Google changed one of its policies concerning digital fingerprinting in December 2024.

Google wrote at the time that it was updating its policy around digital fingerprinting for two reasons. First, advances in privacy-enhancing technologies "give people the privacy protections they expect." The company said these advances present "new ways for brands to manage and activate their data safely and securely."

The second reason Google wrote it was updating its policy is because of the "rise of new ad-supported devices and platforms," like streaming services.

"With this update, we can help businesses, large and small, meet the opportunities of the evolving digital landscape, while meeting user expectations for privacy," Google wrote.

But not everyone was convinced this was a good idea. The UK's Information Commissioner's Office wrote at the time that digital fingerprinting will likely reduce people's choices and control over their data. The office called Google's change "irresponsible," as well as -- quoting Google's own 2019 position on fingerprinting -- "wrong."

Google did not immediately respond to a request for comment.

Other ways to combat digital fingerprinting

Tomaschek told me that while a VPN can mask your IP address and use ad and tracker blockers, it's not a comprehensive solution to combating digital fingerprinting. He suggests using a combination of different tactics. That could mean using a privacy-focused browser like the Mullvad Browser or a privacy-focused extension like Privacy Badger from the Electronic Frontier Foundation, in conjunction with a VPN.

While they can't prevent a company from collecting your digital fingerprint, a data removal service could help remove data that is already out in the wild. So you could use one of those services to remove your data before using a combination of other tools to try to protect your digital fingerprint.

For more on iOS 26, here's my review of the OS, how to reduce the Liquid Glass effects in the update and how to enable call and text screening on your iPhone. You can also check out our iOS 26 cheat sheet.