Google’s Fingerprinting Returns In 8 Weeks And It Will Track Your Devices

Digital fingerprinting is suddenly back and it will be everywhere—here's what you need to know.

By Zak Doffman

Jan 08, 2025 12:21 PM · 7 min. read · View original

Warning—digital fingerprinting is back

getty

Republished on December 21 with Google’s proposals to change search for iPhone and Android users as a response

to the U.S. government's push for it to sell off Chrome.

With Google's last tracking u-turn fresh in the mind, here comes another one. Not only have cookies won a stay of execution, it now looks like digital fingerprinting is back as well. But as one regulator has pointed out, Google itself has said that this type of tracking "subverts user choice and is wrong." And yet here we are—wrong or not. "We think this change is irresponsible," the regulator warns.

For its part, Google cites advances in so-called privacy-enhancing technologies (PETs) as raising the bar for user privacy, enabling it to loosen the shackles on advertisers and the hidden trackers that underpin the internet and make the whole ecosystem work. This, it says, will unlock "new ways for brands to manage and activate their data safely and securely," while "also giving people the privacy protections they expect." The risk is that this simply rolls the dark side of tracking cookies forward into a new era, and in a way that is impossible for users to unpick to understand their risks.

ForbesFBI Warns Gmail, Outlook, Apple Mail Users—Check 3 Things To Stop AttacksBy Zak Doffman

The specifics are complex—these are the algorithms that ingest all the data signals you give off when browsing the internet on any device, some based on who you are—device, IP and credential identifiers, but also the sites you visit and apps you use as a map to be followed and analyzed. The change has been prompted, Google explains, in part by "the broader range of surfaces on which ads are served." This includes smart TVs and gaming consoles, as well as all your usual browser and app activity.

While Chrome has taken plenty of flack for tracking, this takes it to a new, very different level. "In the past decade," Google says, "the way people engage with the internet changed dramatically. So we're constantly evaluating our policies to ensure they reflect the latest evolutions in technology and meet our partners' needs and users' expectations." And so from February 16, Google will be "less prescriptive with partners in how they target and measure ads" across "the

broader range of surfaces on which ads are served (such as Connected TVs and gaming consoles)."

"Fingerprinting involves the collection of pieces of information about a device's software or hardware, which, when combined, can uniquely identify a particular device and user," explains Stephen Almond, representing the UK's Information Commissioner's Office. "The ICO's view is that fingerprinting is not a fair means of tracking users online because it is likely to reduce people's choice and control over how their information is collected. The change to Google's policy means that fingerprinting could now replace the functions of third-party cookies."

The ICO says that "when you choose an option on a consent banner or 'clear all site data' in your browser, you are generally controlling the use of cookies and other traditional forms of local storage. Fingerprinting, however, relies on signals that you cannot easily wipe. So, even if you 'clear all site data', the organisation using fingerprinting techniques could immediately identify you again. This is not transparent and cannot easily be controlled. Fingerprinting is harder for browsers to block and therefore, even privacy-conscious users will find this difficult to stop."


Upcoming February update to the platforms program policies

Changes to user tracking confirmed

Google

Both the regulator and Google have confirmed they'll continue to engage on this change, which the ICO says is a "u-turn in its position and the departure it represents from our expectation of a privacy-friendly internet." The regulator has also issued a stark warning for

businesses that might be readying themselves for the gloves to come off in February when the changes kick in. "Businesses do not have free rein to use fingerprinting as they please. Like all advertising technology, it must be lawfully and transparently deployed—and if it is not, the ICO will act."

Google gives an example of the need for such fingerprinting in its announcement—smart TVs and streaming services. "Internet users are embracing Connected TV (CTV) experiences, making it one of the fastest growing advertising channels. Businesses who advertise on CTV need the ability to connect with relevant audiences and understand the effectiveness of their campaigns. As people and households increasingly shift to streaming platforms, the ecosystem should invest in and develop solutions that are effective and measurable in an incredibly fragmented environment." I have approached Google for any comments on the regulatory warnings following its announced change.

Put simply—cross-platform, cross-device ad tracking. A move which does take the focus away from Chrome as being the epicenter of Google's tracking empire—the timing of which is interesting.

It's hard to imagine a more complex backdrop, with the ongoing DOJ action that is expected to see changes mandated, including the potential for Chrome to be divested. Then there is the uncertainty as to what will replace tracking cookies. "Businesses should not consider fingerprinting a simple solution to the loss of third-party cookies and other cross-site tracking signals," the ICO says, insisting users have "meaningful control over how their information is used to show them personalized adverts."

At its simplest, while tracking cookies are a nasty underpin to the internet, they can be seen and controlled, whether by those website popups or electing to use some form of private browsing that blocks such cookies altogether. Digital fingerprinting is not as obvious and so is harder to spot and to block, it's also more open to

clever manipulation as the tracking industry tests boundaries.

Google says it can "apply privacy-preserving protections that help businesses reach their customers across these new platforms without the need to re-identify them. And because we're looking to encourage responsible data use as the new standard across the web, we'll also partner with the broader ads industry and help make PETs more accessible."

ForbesMicrosoft Warns Millions Of Windows Users—Change Your Browser To Stop AttacksBy Zak Doffman

Google has been fighting this ad tracking battle for years now. It first announced its Privacy Sandbox in 2019, a search for a better way to track users across the internet and serve their data to advertisers. Its stated intent has been privacy-preserving tracking, which have included a range of masking technologies, grouping users into semi-anonymized cohorts, and a newer suggestion of an opt-in.

But Google now has a newer battle on its hand, and it could force change faster than the pedestrian pace of these tracking changes which have now hit a painful stalemate. Both battles have implications for Chrome, even if it's not divested in the most extreme outcome. As reported by *The New York Times*, Google is now seeking to get in front of this. "Google said on Friday what it thought should change to address a ruling that it had illegally maintained a monopoly over online search: not much."

Google's goal appears to be to reverse slowly back over the line it is ruled to have crossed, that it has "illegally maintained a monopoly in online search by paying companies like Apple and Samsung to be the search engine that automatically appears when users open a web browser or a smartphone. In response, the government last month asked the judge to force Google to sell Chrome." Search is advertising's twin pillar—between them they hold up the empire. And Google dominates search with key deals with Apple and across Android which have made "google" synonymous with "search."

Lee-Anne Mulholland—Google's VP for Regulatory Affairs—suggests in a blogpost that "if DOJ felt that Google investing in Chrome, or our development of AI, or the way we crawl the web, or develop our algorithms, were at all anticompetitive, it could have filed those cases. It did not." She warned that "DOJ's proposal would harm American consumers and undermine America's global technology leadership at a critical juncture — such as by requiring us to share people's private search queries with foreign and domestic rivals, and restricting our ability to innovate and improve our products."

Google's proposed remedies include changing agreements with "browser companies like Apple and Mozilla," such that they would "have the freedom to do deals with whatever search engine they think is best for their users… Our proposal allows browsers to continue to offer Google Search to their users and earn revenue from that partnership. But it also provides them with additional flexibility: It would allow for multiple default agreements across different platforms (e.g., a different default search

engine for iPhones and iPads) and browsing modes, plus the ability to change their default search provider at least every 12 months," which was the period of time referenced by the court.

ForbesNew iPhone, Android Warning—Do Not Install These AppsBy Zak Doffman

And Google has also suggested something similar on Android, giving "device makers have additional flexibility in preloading multiple search engines, and preloading any Google app independently of preloading Search or Chrome. Again, this will give our partners additional flexibility and our rivals like Microsoft more chances to bid for placement." The interesting twist here is Microsoft spamming its own Windows users with constant ads and security warnings, pushing Edge and Bing.

The timing is all very interesting. Digital fingerprinting is back on the table and is going beyond traditional browsers, just as the tracking and search ecosystems are being shaken up. There are more moving parts now than there have been for many years—the long period of stability is coming to an end, driven by

AI as much as anything else. It’s very unclear where this will end up.

For users, though, the choices should be clear and transparent at all times. You should know when and how you are being tracked, and you should have an easy-button to say thanks, but no thanks.