# Google defends tracking cookies—some experts aren’t buying it

## reader comments

261 with 151 posters participating

## Share this story

Google’s Chrome team is feeling pressure from competitors over ad tracking. Apple has long offered industry-leading protection against tracking cookies, while Mozilla recently announced that Firefox will begin blocking tracking cookies by default. Microsoft has been experimenting with tracking protection features in Edge, too.

But Google has a problem: it makes most of its money selling ads. Adopting the same aggressive cookie blocking techniques as its rivals could prevent Google’s customers from targeting ads—potentially hurting Google’s bottom line.

So in a blog post last week, Google outlined an alternative privacy vision—one that restricts some forms of user tracking without blocking the use of tracking cookies any time soon.

“Blocking cookies without another way to deliver relevant ads significantly reduces publishers’ primary means of funding, which jeopardizes the future of the vibrant Web,” Google’s Justin Schuh writes. (Those publishers, of course, include Ars publisher Conde Nast. We use cookies to serve targeted ads because they generate more revenue to support our journalism.)

Google also warns that completely blocking tracking cookies will cause ad networks to resort to browser fingerprinting as an alternative means of tracking users. Under this technique, a site harvests many small pieces of data about a user's browser—browser version, fonts installed, extensions active, screen size, and so forth—to generate a "fingerprint" that uniquely identifies a particular device.

So Google's proposal is to declare war on browser fingerprinting while only gradually restricting the use of cookies for ad targeting.

## A privacy sandbox?

To prevent fingerprinting, Google says it's working on a new approach called a "privacy budget." Under this approach, the browser would impose a hard cap on the amount of information any site could request from the browser that might reveal a user's identity. If a site exceeded the cap, the browser would either throw an error or it would return deliberately inaccurate or generic information.

But this is only a proposal, not a shipping feature. And it has some obvious challenges. Some API calls might return so much information that they could identify the user all on their own. If a site made one of these calls, the browser would need to warn the user and get explicit approval—which could be annoying for users. And there's a risk that a too-strict privacy budget could break some existing sites even if they're not engaging in user fingerprinting.

The privacy budget is one component of a larger framework Google calls a "privacy sandbox." The goal is to enable advertisers to serve more relevant ads without allowing them to track individual users:

> *We're exploring how to deliver ads to large groups of similar people without letting individually identifying data ever*

> *leave your browser — building on the* ***Differential Privacy*** *techniques we've been using in Chrome for nearly 5 years to collect anonymous telemetry information. New technologies like* ***Federated Learning*** *show that it's possible for your browser to avoid revealing that you are a member of a group that likes Beyoncé and sweater vests until it can be sure that group contains thousands of other people.*

## Some pro-privacy experts remain skeptical

Google's post was blasted by a pair of Princeton computer scientists who have long advocated for stricter browser privacy protections. They point out that Apple and Mozilla are also working to restrict browser fingerprinting. They argue that it's a non-sequitur to say that the risk of fingerprinting is a reason not to adopt robust restrictions on cookie-based tracking.

The researchers disputed Google's claim that nuking tracking cookies would undermine the economic foundation of the online advertising industry. They point out that after the EU adopted the General Data Protection Regulation, the New York Times discontinued its use of tracking cookies in Europe. The Grey Lady shifted to using contextual and geographic ad targeting—and its ad revenue hasn't suffered as a result.

They also argued that Google is now endorsing ideas that the company dismissed as impractical earlier this decade.

"Privacy preserving ad targeting has been an active research area for over a decade," the pair wrote. They argue that Google was dismissive of alternatives to cookie-based ad tracking during the Do Not Track debate earlier in the decade. "We are glad that Google is now taking this direction more seriously, but a few belated think pieces aren't much

progress.”

Browser privacy has emerged as an important differentiator for Google’s rivals in the browser market. Apple in particular has been running ads in recent months touting the privacy protections offered by the iPhone. These attacks put Google in a difficult position, because Google can’t match its rivals’ privacy protections without potentially hurting its own lucrative ad business.

https://arstechnica.com/?p=1558091