

Google pledges to avoid user-identified tracking when phasing out third-party cookies

3 Mar 2021 | 14:00 GMT | Insight

By Matthew Newman

Google pledged today that, when it quashes its web-browser tracking cookies next year, it has no plans to move to more invasive user-identifier tracking techniques, such as personally identifiable information-based graphs based on users' e-mail addresses.

Google pledged today that, when it quashes its web-browser tracking cookies next year, it has no plans to move to more invasive user-identifier tracking techniques, such as personally identifiable information-based graphs based on users' e-mail addresses.

“We will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products,” David Temkin, Google’s product management director for ads, privacy and trust, said in a blog post (see [here](#)).

The statement comes as Apple prepares to update its mobile operating system, iOS, to allow users to see and block third-party tracking.

Apple's move, expected in early spring, will prevent apps from using its advertising identifier, or IDFA, number without obtaining each user’s explicit consent for targeting. Facebook and other companies that rely on targeted advertising have

strongly criticized Apple's plans, arguing that the changes could slash website sales for small businesses by 60 percent because they will be less able to use targeted ads.

Google said there's no reason that people should accept being tracked across the web "to get the benefits of relevant advertising. Moreover, it said, advertisers don't need to track users "to get the performance of digital advertising."

— Chrome —

Google's announcement comes as the company faces twin lawsuits in California accusing it of breaking federal and state laws over data collection through its Chrome web browser.

In one of those cases, Google told Chrome users that "personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on Sync." In fact, the plaintiffs allege their personal information from browsing in Chrome's basic mode was fed into services such as Google Ad Manager and Google Analytics, which target display advertising (see [here](#)).

Last week, the second of those two Chrome cases took a surprising turn when a Google lawyer told US District Judge Lucy Koh that Google code embedded in the website of the Northern District of California is allowing the tech giant to track people who access the court site (see [here](#)). This week, Google acknowledged the embedded Google search box is personal data for ad-targeting (see [here](#)), after Koh said she was "deeply disturbed" about the privacy implications (see [here](#)).

— Europe —

In Europe, behavioral advertising has come under intense scrutiny in recent months from legislators, as well as privacy and competition regulators. The European Parliament called on the European Commission before it proposed far-reaching rules to regulate platforms “to further assess options for regulating targeted advertising, including a phaseout leading to a ban” (see [here](#)).

Last month, the European Data Protection Supervisor, which oversees EU institutions' data privacy, called on the bloc's legislators to push for "phasing out" and then "prohibiting" the use of targeted ads (see [here](#)).

Google's push to phase out third-party cookies coincides with Apple's plans to allow users to opt out of IDFA tracking are raising concerns that advertisers will explore new forms of user tracking to evade privacy rules, such as “device fingerprinting.”

Device fingerprinting is a technique used to identify users through certain attributes of a device — such as a phone’s operating system, the type of web browser, configurations like Internet connections, battery or language settings, and usage patterns. These attributes can be correlated with repeat visits to apps from the same smartphone and then used to identify and track someone online.

Google also vowed that it won’t use or build user-specific profiles based on an individual's activity across the web, like personal identifiable information-based graphs. With this technique, marketers create an identity graph with “unique identifiers” from where users’ data is collected: device IDs, e-mail addresses, phone numbers, cookie data and transactions.

“We don’t believe these solutions will meet rising consumer expectations for

privacy, nor will they stand up to rapidly evolving regulatory restrictions, and therefore aren't a sustainable long-term investment," Google said.

Some large publishers, such as The New York Times, have decided to phase out "third-party" cookies — text files that track online activity and are used for behavioral advertising.

Google said it plans to "take third-party cookies out of the advertising equation and instead hide individuals within large crowds of people with common interests."

The company said its "web products will be powered by privacy-preserving APIs which prevent individual tracking while still delivering results for advertisers and publishers."

In 2020, Google said that it would phase out third-party cookies by 2022. It is now developing a proposal known as FLoC, or Federated Learning of Cohorts, a "Privacy Sandbox" technology that will be based on interest-based advertising. The company wants to use tools letting advertisers run targeted ads without access to users' personal details.

But these plans have attracted the scrutiny of the UK's antitrust regulator, the Competition and Markets Authority, which is investigating complaints that Google's replacement of third-party cookies will have a "significant" impact on news publishers and digital advertisers.

Some companies also suspect that Google is using the pretext of consumer privacy concerns to consolidate its control over web traffic. The CMA is attuned to these concerns: It said it will assess whether advertising spending could become "even more concentrated on Google's ecosystem at the expense of its competitors" (see

[here](#)).

In Brussels, the commission is exploring whether Google bundles various Internet advertising technologies and squeezes publishers through changes to data services (see [here](#)).

Google also said that it will continue to support “first-party relationships on our ad platforms for partners.” First-party data is information that companies collect from their own sources, such as when customers enter information on a company's website or app.

“We'll deepen our support for solutions that build on these direct relationships between consumers and the brands and publishers they engage with,” Google said.

With reporting by Mike Swift.

Please e-mail editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.