APR 21
Mack DeGeurin

WordPress's proposed FloC ban could disrupt Google's plan to replace third-party cookies

Article

WordPress is considering a proposal that would block Google's third-party cookie alternative by default on all sites powered by its content management system, over privacy concerns.

The proposal—which is not yet finalized—would add several lines of code to WordPress-powered sites to detect Google's alternative tracking technology, called Federated Learning of Cohorts (FLoC), and label it a "security threat." WordPress is also considering creating a toggle switch to allow its end users to opt in to FLoC on their sites, if they so desire.

If WordPress moves forward with its proposal, it would join a coalition of internet companies publicly opposing FLoC citing privacy concerns.

- **Brave:** Earlier this month, Brave announced its browsers wouldn't support FLoC and claimed FLoC was bad for user privacy.
- **DuckDuckGo:** Around the same time, DuckDuckGo released a Chrome browser extension blocking FLoC tracking.
- **Firefox:** A Mozilla spokesperson recently told Digiday that the company had "no current plans" to implement FLoC in Firefox, adding: "We don't buy into the assumption that the industry needs billions of data points about people."
- **Edge:** Finally, Microsoft this week reportedly disabled FLoC on its Edge browser.

FLoC uses machine learning within browsers to sort internet users into groups—called cohorts—of thousands of people based on their perceived interests, which advertisers can then use instead of cookies to serve targeted ads. While FLoC supporters like analyst Eric Seufert have called it a "sensible approach to privacy-preserving ads targeting," critics like the Electronic Frontier Foundation (EFF) claim it presents new privacy issues and expands Google's data-gathering power beyond the capability afforded by cookies. . Bennett Cyphers, an EFF technologist, observes that FLoC shares summaries of user's recent browsing activity with marketers, raising questions specifically over cross-context exposure and Google's use of fingerprinting practices which, Cyphers argues, combine to create a system that could ultimately exacerbate discrimination and predatory targeting.

If WordPress chooses to label FLoC as a security threat, it could cut Google off from a sizable chunk of monetizable behavioral data. Defiant web browsers can impede FLoC's reach, but only to a marginal extent: GoogleChrome made up a whopping 68% of worldwide desktop web browser traffic share in Q4 2020, per StatCounter. On the other hand, WordPress' sphere of influence transcends browsers—by its own estimation, WordPress-powered sites reportedly account for at least 41% of all websites. WordPress finds itself with the power to act as an arbiter of advertising and data privacy, deciding the nature and degree

of the targeted ads that appear on sites it hosts. If WordPress takes such a stance, it could open the door for other providers of internet infrastructure to follow suit.

Desktop Web Browser Traffic Share Worldwide, Q1 2020-Q4 2020

% of total

	Q1 2020	Q2 2020	Q3 2020	Q4 2020
Chrome	68.7%	68.3%	69.7%	68.3%
Safari	8.7%	9.3%	8.5%	9.6%
Firefox	9.6%	8.9%	8.4%	8.0%
Edge	0.3%	1.5%	4.9%	6.6%
Opera	2.4%	2.4%	2.4%	2.5%
Internet Explorer	3.7%	3.1%	2.6%	2.4%
Edge Legacy	4.6%	4.3%	1.4%	0.7%
360 Safe Browser	0.2%	0.7%	0.7%	0.6%
Yandex browser	0.5%	0.5%	0.4%	0.4%
Mozilla	0.2%	0.2%	0.2%	0.2%
Other	1.2%	1.0%	0.9%	0.8%

Note: numbers may not add up to 100% due to rounding
Source: StatCounter, "Global Stats"; Insider Intelligence calculations, Jan 22, 2021

262853 eMarketer | InsiderIntelligence.com