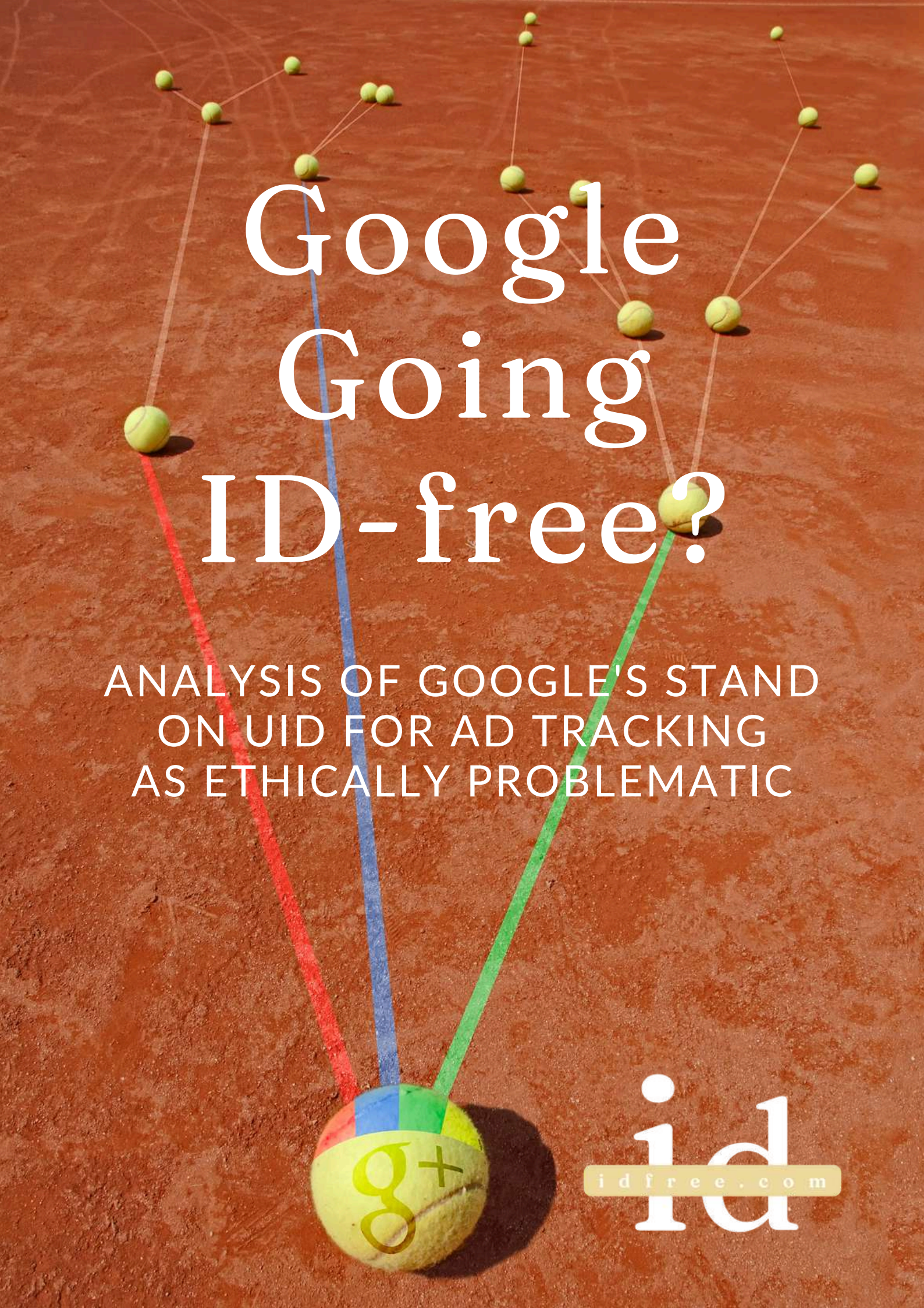
Google Going ID-free?

ANALYSIS OF GOOGLE'S STAND ON UID FOR AD TRACKING AS ETHICALLY PROBLEMATIC



idfree.com

GOOGLE GOING IDFREE?

First Google killed the third-party cookies, now they are killing UIDs and other hashed identifiers.

It is a good thing, but the industry needs other options than the one's Google and Apple provide. Preferably solutions and ideas that work across all the different advertising channels, and ideas that do not rely on collecting and storing user's private data or browser history.

"Today, we're making explicit that once third-party cookies are phased out, we will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products."

"Starting with iOS 14.5, iPadOS 14.5, and tvOS 14.5, you'll need to receive the user's permission through the AppTracking Transparency framework to track them or access their device's advertising identifier."

Back in September 2019, Mozilla Firefox blocked 3rd. party cookies by default. Apple's Safari did the same in March 2020.

In January 2020 Google announced that Google Chrome would block 3rd. party cookies by default from 2022.

This date was first postponed to 2023. And lately postponed again to 2024 in order to test more in Privacy Sandbox.

THE THREE BROWSERS ACCOUNT FOR APP. 85% OF ALL GLOBAL WEB TRAFFIC.

AN ID IS AN ID

The upcoming death of 3rd. party cookies have set off a technological race to develop alternatives to the cookie.

Known as unified IDs or UIDs - often ID frameworks built from hashed and encrypted email addresses or other personally identifiable information.

There is no shortage of initiatives like The Trade Desk's UID 2.0, The Advertising ID Consortium, IABs DigiTrust ID, ID5, LiveRamp, Tapad, Zeotap, InfoSum, and many others.

Shared by them all is the ambition to create a persistent ID to identify users as they move around the web.

THE WRONG PATCH

At idfree.com we have always been sceptical. To have a persistent and stable ID-based on the user's personally identifiable information replacing the third-party cookie is an odd choice from a privacy point of view.

AN ID IS AN ID.
HASHING OF PERSONAL DATA ACCOMPLISHES ONLY PSEUDONYMIZATION, NOT ANONYMIZATION.

We know that many of the companies mentioned are going a long way to ensure user consent and privacy.

But from our point of view, the core idea - IDs based on users' personally identifiable information - has always seemed like **the wrong path**.

On March 3rd 2021, Google dropped another bomb in the post-cookie debate!

Google's Director of Product Management, Ads Privacy and Trust David Temkin, put up a blogpost that stated:

"If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web. [....]

Today, we're making explicit that once third-party cookies are phased out, we will not build alternate identifiers to track individuals as they browse across the web, nor will we use them in our products.

We realize this means other providers may offer a level of user identity for ad tracking across the web that we will not - like PII graphs based on people's email addresses.

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."

THAT IS THE MAIN REASON WHY WE DEVELOPED IDFREE.COM

UIDS ARE ETHICALLY PROBLEMATIC

In straightforward wording, Google says that UIDs for ad tracking are ethically problematic *and could very soon become illegal*.

And that they will not be accepted in Google's products like Google Ads, DV360, and YouTube.

WOW!

REJECTING UIDS

Google is here following the same path as Apple, who recently accounted that:

"Starting with iOS 14.5, iPad OS 14.5, and tv OS 14.5, you'll need to receive the user's permission through the AppTracking-Transparency framework to track them or access their device's advertising identifier."

In the announcement, Apple states that hashed IDs, including emails and phone numbers collected elsewhere, can not be used as a replacement for app tracking on iOS 14.5.

That is true whether or not the hashed identifiers were collected with consent.

So the very idea of hashed IDs based on user's personally identifiable information has now firmly been rejected by both Apple and Google:

The two companies that control most web traffic and almost all app traffic.

THE TWO COMPANIES CONTROL MOST WEB TRAFFIC AND ALMOST ALL APP TRAFFIC.

WHAT NOW?

What on the surface looks like a good development
for user privacy can become a big issue for the advertising industry.

OWN TRACKING

Apple and Google are not naive and did not become multi-billion dollar businesses by playing nice.

Both Apple and Google are ready with their own solutions for tracking like Apple's AppTrackingTransparency framework and Google's privacy sandbox and the Federated Learning of Cohorts (FLoC).

Both the AppTrackingTransparency framework and especially the FLoc methodology are not flawless.

THEY CAN - AND SHOULD BE - DISCUSSED

As described by Google browsers with FLoC enabled will collect and store information about their user's browsing habits, then use that information to assign its user to a "*cohort*" or group on a weekly basis.

Preferably ideas that work across all the different digital advertising channels and ideas that do not rely on collecting and storing users' private data or browser history.

Users with similar browsing habits will be grouped into the same cohort. Google suggests an algorithm called SimHash to create the groups.

SimHash can be computed locally on each user's machine, so there's no need for a central server to collect behavioural data.

But even with SimHash the user's browser history and behavioural data still need to be collected and stored.

INDEPENDENCE

Relying only on solutions from Apple and Google is dangerous for independence, competition, and creativity in the advertising industry.

WE NEED MORE OPTIONS AND MORE IDEAS!

Preferably ideas that work across all the different digital advertising channels.

And ideas that do not rely on collecting and storing users' private data or browser history.