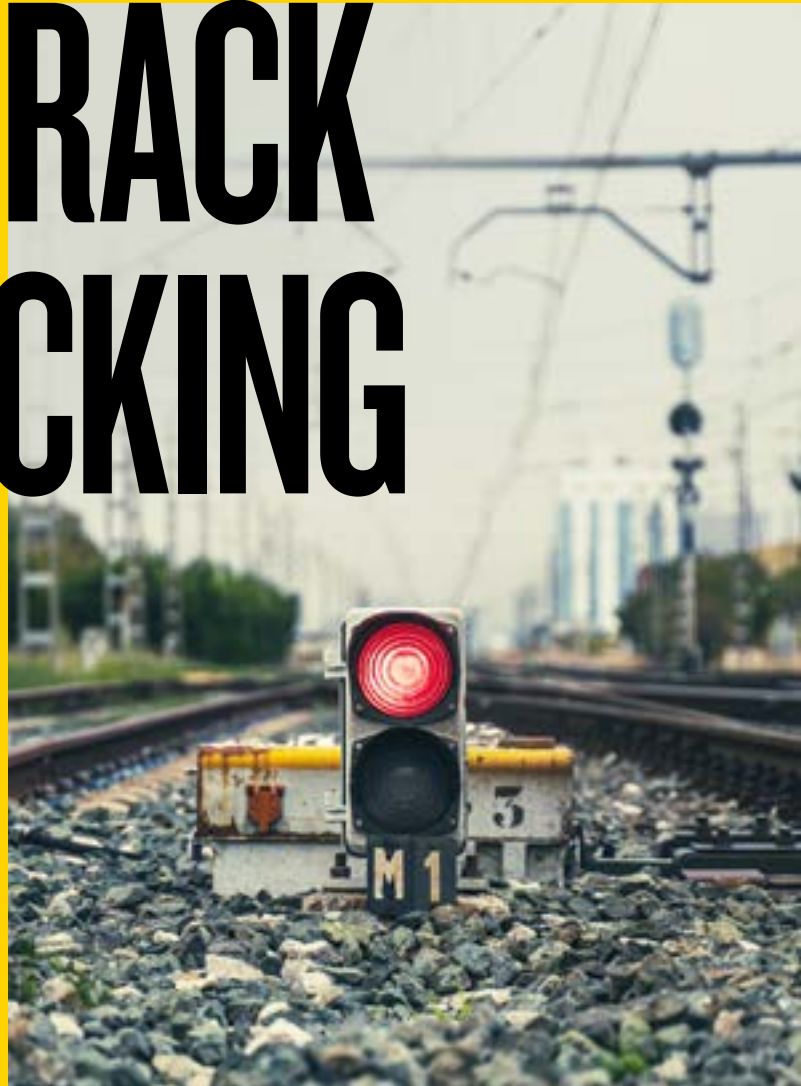


THE END OF THE TRACK FOR TRACKING

An explainer on 3rd party cookies, and a bit more



COLLABORATIVE

Insight . Ideas . Inspiration

March 2021

A wall covered in numerous security cameras, with two women standing at the bottom looking up at them.

INTRODUCTION

You may have seen coverage about the end of cookies, the cookie apocalypse, the end of days and so on in relation to some changes Google are making to how their web browser Chrome works and which bring it in line with what Apple's Safari and Firefox already do. This week [Ebiquity](#) has shared an excellent primer.

This document is an explainer - with more technical detail on the changes and potential impacts, and our point of view on what to do about them.



WHAT'S HAPPENED?

Since 2018 Apple has been degrading or removing the tracking functionality offered by 3rd party cookie technology from its Safari browser, under a programme called Intelligent Tracking Prevention (ITP). It didn't make the changes all at once. There's been something of a cat and mouse game as ad tech has found workarounds, Apple has closed the loophole allowing the workarounds, and ad tech has found a workaround for the workaround. But now, Apple's gone pretty hard core and Safari will soon not accept 3rd party cookies, at least not in any way that's useful to advertisers. Apple is also going to prevent all tracking across both web and mobile, including in-app, under a framework called App Tracking Transparency (ATT). Google has now confirmed that it is to follow suit by the end of this year with similar privacy-centric changes to its Chrome web browser. Together, Chrome and Safari make up the vast majority of browsers accessing the web, so this effectively means the end of 3rd

party cookies as a useful technology for advertisers.

Google's position on 3rd party cookies represents a relatively recent change of heart. It could be that Google has seen the light shining down from Apple's moral high ground, or perhaps is making changes now before it's forced to by legislation, or maybe it has designs on strengthening the masonry around its own walled garden; within which it can do all the tracking it likes, based on Google account log-ins. Google say they won't do this, but not all commentators are convinced.

What is clear, is that digital tracking and targeting across the web and across devices, is going to have to fundamentally change and the knock on impacts on the digital ad world will be huge.

Facebook - who stand to see their revenue shrink by US\$8BN over the next 12 months - is so cross with Apple that it has taken

out newspaper ads to publish its open letter chastising them for their anti-small-business-ness. Facebook says it's standing up for the small businesses they support through ad generated income. But Apple's changes are backed by Amnesty International, The Electronic Freedom Foundation (EFF) and pretty much every consumer rights organisation you can think of, who are collectively pressing Apple to get on with making the changes asap. Google's losses will likely be twice that of Facebook's, but perhaps not wishing to draw attention to what it does with Android and Play, it has remained silent on the Apple changes.

WHAT ARE THE KNOCK ON IMPACTS OF THESE CHANGES?

- All the 3rd party audience profiles we buy for behavioural targeting rely on 3rd party cookies. That's what powers the promise of 'precision at scale'. No 3rd party cookies, no 'precision at scale'. If you take away 'precision at scale', there's no incentive to use the open internet. As a result, we expect to see spends re-focused into a much smaller number of larger publishers who can offer substantial reach and at least some control over frequency – all the better able to do so if publishers club together and share their first party data to enhance interest based targeting, c.f. [The Ozone Project](#).
 - There's also likely to be an even greater concentration of budgets from corporate advertisers into the walled gardens of Google, Facebook and Amazon who each have their own rich data sources.
 - Website retargeting receives a knockout blow. Forget it – it won't be possible.
 - All this directly threatens small publishers and niche content producers by diverting ad budgets away from the open internet. No targeting = no ads = no income = no sites and a less rich and diverse internet for all of us.
 - The dream of accurate digital cross channel and cross device attribution is going to be comprehensively trashed.
 - And the ad tech industry, invested in servicing 3rd party cookie based programmatic targeting, is left out to hang – stock values took a big hit after Google's recent announcement; now's not a great time to invest in ad tech.
- It's probably an understatement to describe the work to find an alternative to 3rd party cookies as merely feverish.



3RD PARTY COOKIE ALTERNATIVES - WHAT'S COOKIN'?

Fingerprinting

One alternative to 3rd party cookies is to use something called 'device fingerprinting'. Our browsers are, counterintuitively, unique entities to the point they have their own fingerprint - you can learn more from the [EFF](#). Ad tech vendor FlashTalking (globally the main competition to Google's ad server, Google Campaign Manager) provides cookieless tracking (FTrack) based on fingerprinting. Apple and Google, however, have been very clear that their intention is to massively restrict device fingerprinting on the web (Google) and everywhere else too (Apple).

A universal ID

Another solution is a persistent ID identifier which we all use across devices and the web. Enter ID2.O, supported by the internet Advertising Bureau ([IAB](#)), developed by programmatic bidding software vendor, The Trade Desk ([TTD](#)) and a whole bunch of tech and publisher partners, and to be maintained and managed by an independent body [Prebid.org](#).

This is all very jolly, but how will it work? The proposal is that publishers will sign up to using ID2.O, then when someone comes to their site they'll be presented with an opportunity to universally sign up too. Once registered you will be automatically signed-in to all other participating publishers and will benefit from being served more relevant advertising tailored to their interests and web browsing preferences.

The problem with this is that people want more relevant advertising in the same way that they want neater holes in their heads. But if it's the only way to access content (effectively an ID paywall) it might get some traction.

However it's not only punters that may be reluctant to sign-up to ID2.O - this solution erodes publishers' unique understanding of their audiences, as these insights are now effectively shared across a range of unconnected publishers. Why pay high CPMs for high net worth individuals on The Times when you can target them cheaply through ID2.O on thetrainline.com? True, that effectively is the promise of 3rd party cookie audiences. But publishers have always resented it, and for some publishers this proposal will seem a lot like turkeys voting for Christmas. There's very much a business model challenge here on top of the technical and behavioural challenges.

Cohort based targeting and learning

But why do we even need to target individuals? In other areas of media we are perfectly comfortable observing what happens in the aggregate. Why not digital?



Google's solution, [FLEDGE](#) (First Locally Executed Decision over Groups) is based on [Turtledove](#) - the framework for making the decision on ad targeting privately in the browser, and uses [FLoCs](#) Federated Learning of Cohorts, to group together browsers and report collectively on interests and profile. FLoCs replaces PIGIN (Private Interest Groups, Including Noise). FLoCs works by sometimes sending back fake info (the noise in PIGIN) so you cannot deduce the facts about an individual from the group data. Thus protecting the privacy of all those in the cohort. [Explainer here](#). Attribution is reported back in aggregate for the cohort, not at the individual level. This sounds like a good solution but it puts yet more power into Google's hands and there are suspicions that Google could use FLoCs to competitive advantage. It's fair to say the [EFF is not a fan](#). In fact it's hard to find anyone who is. Criteo (a website visitor retargeting firm) has proposed [SPARROW](#) (Secure Private Advertising Remotely Run On Webserver) because of concerns over only Google being able to 'see' the auction. [PARRROT](#) (Publisher Auction Responsibility Retention Revision of TurtleDove) suggests Turtledove be amended to place the auction under publisher control. Google is "working with the industry" around these concerns. Anyone hoping that Google was going to invent cookies 2.0 for the whole industry to use, will be disappointed in the roadmap that [has now been made clear](#) - they have no intention of any such thing.

So, we are a long way away from landing on a solution to replace the functionality of 3rd party cookies. Brace for impact.

¹ Not a real word.

BUT WAIT, WERE COOKIES REALLY ALL THAT TASTY?



There's all sorts of parts of the internet that 3rd party cookies cannot reach.

- Facebook ads – you can put a click tracker on and see people when they click, but you can't impression track – ditto most social platforms.
- Google search – no impression tracking, although again, you can of course click track.
- Various sorts of OLV that just technically have no way of being associated with a cookie.
- Connected TV – doesn't work that way.
- Apps on mobile devices – they don't use cookies – they do use other technologies, but as mentioned, Apple is switching that tracking capability off too.
- And of course, TV, posters, print, cinema etc etc cannot track people with a cookie.

So any tracking picture we had, based on 3rd party cookies, had 'gaps' to say the very least. Consider as well that according to [FlashTalking](#) 30% of devices block or delete all cookies and 50% of cookies are deleted within 48 hours.

So how good are 3rd party cookie based audiences? Building those audiences relies on 'cookie matching' where you look at different sets of cookies and try to identify the shared cookies that represent a unique individual. Between two sets of cookies a good match rate is 60%; a low rate 20%. There's an obvious trade off between accuracy and scale. 3rd party data audiences tend to be opaquely created and not necessarily based on the freshest data. All in all, it's hardly the best conditions for laser sharp precision.

You may wonder how come so much faith (and cash) has come to be invested in 3rd party cookie based tracking solutions. Truthfully, it's because they've thus far been the best solution we have; certainly better than nothing at all – but the gaps and weaknesses have been somewhat overlooked in favour of a more compelling story about precision and control. That story has always had gaping holes in it.

So maybe it was time to find a different way to do things anyway.



SO WHERE DO WE GO FROM HERE?

We expect to see a greater concentration of spend into a smaller number of publishers. On the whole, this is a good thing. VCCP Media already actively advises our clients to adopt a 'fewer, bigger, better' strategy. This is because, even in retargeting, we believe context matters, because always in media 'brands are the company they keep'. Being on a well established site with quality content brings positive association to a brand that isn't possible to replicate elsewhere. This doesn't mean abandoning the benefits of programmatic. It means a greater focus on buying models like programmatic guaranteed (PG) and private marketplaces (PMPs) with publisher enriched 1st party data.

VCCP are proud to be a member of The [Conscious Advertising Network](#). Whilst there will be a concentration of budgets into larger publishers, publisher cohorts and walled gardens, we also strongly encourage advertisers to consider how their budgets can be spent to support smaller quality publishers with bang-on audiences, and

publishers whose content supports and encourages diversity and inclusion in our communities. It's in all of our interests to maintain a rich, diverse, ad funded web.

Targeting by context and audience profile, with quality publishers with good reach and brand association should therefore be the starting point for most advertisers, and comparative tests should be deployed by performance marketers to learn how the new way stacks up with the old.

For clients invested in the Google stack we'd advise testing FLoCs as soon as public testing is open (very soon).

Similarly, we'd advise testing app campaigns with Apple's [SKAdNetwork](#) - a cohorts based approach to measurement and analytics like FLoCs but for apps.

For multi-touch attribution (MTA), the game is up. So there is now a very limited window

to learn from MTA. There are 'cookieless' solutions - but these rely on fingerprinting and other data passover that both Apple and Google have committed to closing down. And we'd argue that for most advertisers, the cost of multi-touch attribution modelling far outweighs the benefits they ever see from it. Better to simply develop a robust test and learn programme and invest in more sophisticated predictive modelling based on the patterns in media and business outcomes you observe. We would argue that this is a more powerful analytics approach anyway. You need a different approach to the maths is all - perhaps that's for another explainer on what's happening in analytics.



IN SUMMARY

The way we track and target both web users and app users is going to have to change as the two giants of the industry, Google and Apple, have committed to removing the 3rd party cookie technology that has, as yet, powered this functionality. Apple is also changing the way we track and target across apps.

There are a bunch of alternatives to 3rd party cookies proposed, but none that all can agree on.

But there were always problems with cookie tracking, and app tracking.

So yes, this is the end of tracking as we know it. But in our view, that's probably not such a bad thing.

ICYDK - here's what 3rd party cookies are, and what do they do

Cookies are small text files stored by your browser. They make it easier for you to use the web by storing information locally (i.e. in your browser) like the fact you're logged-in and on page 3 of a 5 page application form. Very handy dandy!

A cookie, placed by your bank when you sign-in to mybankwithmymoneyinit.com is a 1st party cookie. It's placed by the site you are visiting. You're on mybankwithmymoneyinit.com - it says so in the address bar of your browser - and the cookie is served by the webserver at mybankwithmymoneyinit.com, they match. So far, so straightforward.

But sometimes web pages are made up of components served by more than one web server. Say you're on mailonline.com reading the sidebar of shame. All those Facebook share buttons are not actually 'on' mailonline.com - they're just pulled into the mailonline's pages from Facebook's web server. And as Facebook serves its share button, it can also serve a cookie. That would be a 3rd party cookie. You are the 1st party, the mailonline is the 2nd party, and Facebook is the 3rd party. When Facebook drops its cookie, it can then read the information in that cookie, and recognise you, whenever it 'sees' you on the web - e.g. when you go to any other site with the Facebook share buttons. It doesn't have to be a share button, or even anything visible to humans. All sorts of ad tech serves pixels (and other code) into the web pages we browse and as we do, drops 3rd party cookies into our browsers. After the technical changes are rolled out to Safari and Chrome, they will no longer accept these cookies - at least not in a way usable by ad tech for tracking.

ABOUT COLLABORATIVE

Collaborative is VCCP's insight platform, showcasing the collaborative thinking of its strategists from across the VCCP Partnership which include specialists in media, communications and experience design.

Report author: Steve Taylor.

If you have any questions or for more information please contact collaborative@vccp.com

COLLABORATIVE

Insight . Ideas . Inspiration