Practice papers

Planning for a cookie-less future: How browser and mobile privacy changes will impact marketing, targeting and analytics

Received (in revised form): 27th May, 2021

Ian Thomas
Independent Consultant, UK

Ian Thomas is a 20-year veteran of the data and analytics industry. He co-founded one of the industry's first web analytics firms and has held senior data leadership roles at Microsoft and Publicis Groupe, dealing with some of the world's largest and most complex datasets, and building effective cross-functional teams to bring data to life. He is now an independent consultant and interim chief data officer, advising businesses on how to build world-class data platforms and teams.

E-mail: ian@ianthomasdata.com

Abstract Recent and impending changes to the way that browsers and mobile platforms handle third-party cookies and ad IDs will have a profound impact on the digital advertising ecosystem. This paper examines these changes in the context of the development of the ad-tech and digital media industry, and concludes that while these developments may benefit users by protecting them from intrusive third-party tracking and targeting, they risk further consolidating power with the three dominant companies in the sector, namely Google, Facebook and Amazon, and advertisers and marketers will have to work hard to ensure they do not become over-dependent on these suppliers. At the same time, the changes offer an opportunity to move back to a better equilibrium between advertising and the content that it appears alongside, driving value for both advertisers and consumers.

KEYWORDS: privacy, cookies, ad-tech, Google, Facebook, Apple

INTRODUCTION

The current model of digital advertising, which has been the primary model for most of the past 20 years, relies heavily on a complex distributed ecosystem of third-party services providing ad delivery, targeting, tracking and measurement. At the heart of this ecosystem is the cookie (and its mobile-app counterpart, the ad ID) — a persistent identifier that enables advertisers, publishers and ad-tech companies to track individuals as they use the internet. Despite the reporting and consent requirements introduced by recent laws such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act 2018, it is almost impossible for individuals to understand and control the use of third-party cookies to capture detailed information about their online activities.

A BRIEF HISTORY OF DIGITAL ADVERTISING AND USER DATA

In the early 2000s, many advertisers and publishers interacted directly or via media agencies. Large advertisers that could afford to hire the services of a media agency were able to buy advertising inventory from multiple publishers and manage ad delivery across these sources through the use of advertiser ad platforms such as DoubleClick and Atlas. Publishers, in turn, hired specialist ad sales and operations teams to service their clients' needs, and implemented publisher ad platforms (many provided by the same companies, like DoubleClick) to manage their ad supply across multiple sources of demand, and optimise monetisation.

In the late 2000s, Google's search advertising platform opened up digital advertising to small advertisers, and publishers looked for a way to leverage this. These smaller advertisers could not afford to implement their own advertiser ad platform or build direct relationships with publishers; nor could the publishers afford to service thousands of small advertisers directly. Ad networks (such as Atlas's DrivePM network) sprung up to fill this gap: by acting as an intermediary between publishers and advertisers, they were able to aggregate supply and slice it into segments in order to match advertisers to inventory, across multiple sites. Over the next few years, advertising networks morphed into demand-side platforms (DSPs), which offered real-time bidding on ad inventory based upon the individual that was seeing the ad — known as programmatic advertising.

While all this was happening, two other important developments were taking place. First, having acquired DoubleClick in 2007, Google started to build out a comprehensive ad platform that combined tools for advertisers and publishers with its growing network of third-party ad inventory. Google AdSense (launched in 2003) enabled publishers to provide ad inventory for Google to monetise by indexing the content of the publisher's site and using the content as synthetic 'keywords' to select targeted advertisements from Google's advertisers.

The second important development was the emergence of Facebook's advertising business. Facebook leveraged the very rich data that users shared about themselves to enable advertisers to buy highly user-targeted ads, reaching only the users they want to reach. Initially these advertisements would only run on Facebook itself (much as advertising through Google's AdWords started out solely on google.com) but in 2014 Facebook launched the Facebook Audience Network.[1] Much like AdSense, the Audience Network allows third-party publishers (particularly mobile app developers) to monetise their properties by making inventory available for advertisers who are buying through Facebook.

Collectively, these new models of ad buying and selling — DSPs, Google and Facebook — created a highly user-focused model of ad targeting, selection and measurement, relying heavily upon the passing of user data to third-party services, and, most importantly, on being able to set and retrieve a persistent user identifier.

Figure 1 shows some of the complex data and cookie flows involved in a typical programmatic ad call.

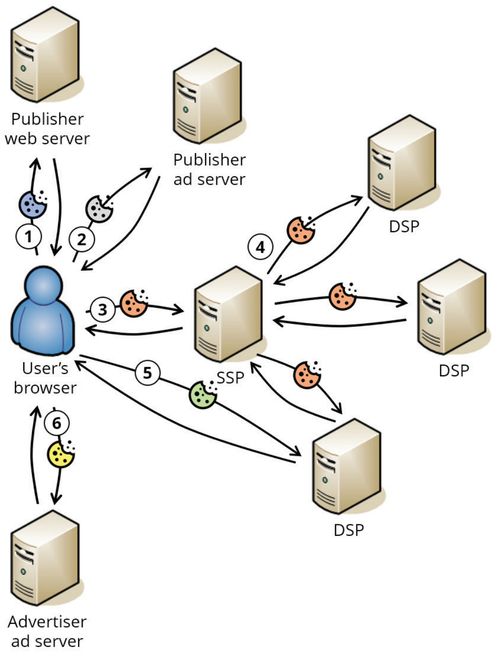
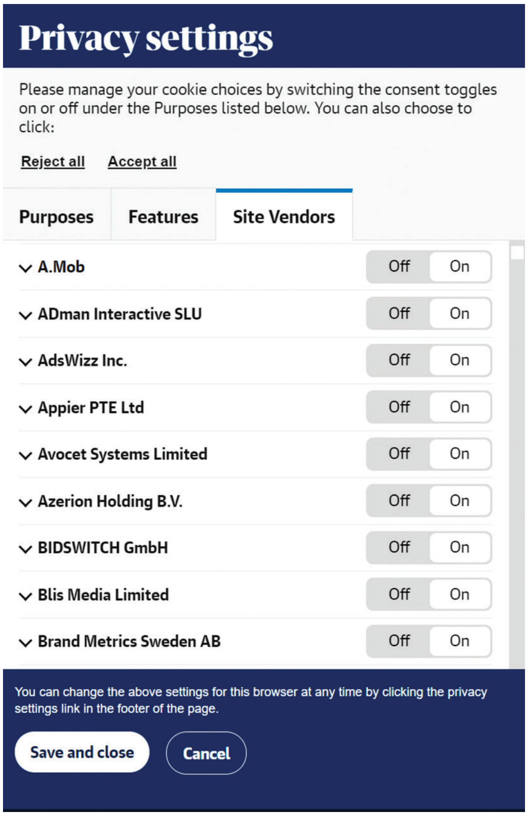


Figure 1: Flow of cookies in a typical programmatic advertisement delivery setup

The steps in this process are as follows:

1. The user's browser requests a page from a publisher's website, and is served HTML plus a first-party cookie.
2. The publisher website directs the browser to contact the publisher's ad server, which sets a cookie and directs the browser to contact the publisher's DSP.
3. The DSP sets (or reads) a third-party cookie and gathers some other information about the user (eg the browser they are using and their IP address).
4. The DSP conducts a live auction for the advertisement spot by contacting multiple sell-side platforms (SSPs), passing the user's cookie and other data to each, and passes details of the winning DSP back to the browser.
5. The browser contacts the winning DSP and gets details of the actual advertisement to be delivered. The DSP sets a third-party cookie to track the number of auctions it is winning for each user.
6. The browser contacts the ad server for the advertiser to get the advertisement itself and then displays it. The advertiser ad server sets a third-party cookie for measurement and frequency capping.

Until 2018, this third-party tracking and data processing largely happened behind the scenes, with sites not required to notify users or gather consent; but that changed in 2018 with the introduction of the GDPR. The GDPR requires organisations that process individuals' personal data to gain explicit consent to gather and process such data for digital marketing and measurement. In practice this has meant that sites have had to implement complex interfaces to capture consent for many different classes of cookies set by third-party services, as illustrated with the example given in Figure 2.



Privacy settings

Please manage your cookie choices by switching the consent toggles on or off under the Purposes listed below. You can also choose to click:

Reject all Accept all

A.Mob	Off	On
ADman Interactive SLU	Off	On
AdsWizz Inc.	Off	On
Appier PTE Ltd	Off	On
Avocet Systems Limited	Off	On
Azerion Holding B.V.	Off	On
BIDSWITCH GmbH	Off	On
Blis Media Limited	Off	On
Brand Metrics Sweden AB	Off	On

You can change the above settings for this browser at any time by clicking the privacy settings link in the footer of the page.

Figure 2: The consent management interface on theguardian.com

These interfaces are not really fit for purpose — they are so confusing for users that they are wholly ineffective when it comes to capturing informed consent. The problem is not the consent management tools themselves — it is the incredibly complex web of third-party cookies and data flows that support digital advertising and measurement.

In response to this, Apple and — to a lesser extent — Google have started to take a much harder stance on the underlying technology (ie third-party cookies and ad IDs) that support so much of this complex ecosystem. However, their approaches contain a number of important differences.

APPLE, SAFARI AND THIRD-PARTY COOKIES

Apple has been pushing privacy as a differentiator for its products and services for several years, both in its Safari browser and in iOS. In 2017 it introduced Intelligent Tracking Prevention (ITP) into WebKit (the underlying browser tech for Safari), which limits the ability for sites to send or request data from third-party sites, known as *cross-site tracking*.

The privacy issue that Apple sought to address with ITP is that a third-party service that serves advertising into multiple sites, and sets a user cookie when it does so, can amass a large amount of information about the interests and behaviours of those users. This kind of audience data (known as 'cookie pools') has been an asset that DSPs and data management platforms have assiduously developed and monetised over the years.

A simple way to block such data collection would be to block all cross-site calls (and third-party cookies with them); but this would cause problems for many legitimate uses of this technique (such as federated login processes). The Apple ITP feature therefore uses machine learning to detect which sites are being used for cross-site tracking.

Since introducing ITP, Apple has tightened the restrictions it imposes, while at the same time introducing new functionality such as the Storage Access API[2] to enable sites to continue to have some relationships with third-party sites and data. In 2020 Apple further tightened ITP to block all third-party cookies. Sites can still use the Storage Access API to request an explicit opt-in from a user, but given that the user will need to have some good reason to agree to the third-party storage, this has essentially spelled the end of third-party cookies on Safari.

APPLE ID FOR ADVERTISING RESTRICTIONS

Alongside the tightening of ITP and its restrictions on third-party cookies and cross-site tracking, Apple is restricting the usage of the 'ID for Advertising' (IDFA) that enables app developers, mobile advertising networks and mobile measurement providers to measure the usage of mobile apps.

Apple introduced the IDFA back in 2012 as a way to persistently identify the device that an app is installed on. Any iOS app can access the IDFA and pass it to a service on the internet (such as a mobile advertising network). Because the IDFA is the same across apps, it works a bit like a third-party cookie; if App A passes the device's IDFA to a third-party service, and then App B passes the same ID, then the third-party service knows that the user is using both apps.

The IDFA has been very useful for many of the same things that cookies have been used for in the browser: advertisement targeting, measurement and response attribution, and rotation and frequency capping. Facebook has been a very extensive user of IDFA as a mechanism for enabling advertisement targeting in third-party apps in its Audience Network (and across its own apps, particularly between Facebook and Instagram). If a user interacts with a lot of content about, for example, gardening in the Facebook app, a third-party app that uses Facebook's Audience Network can use the IDFA to deliver advertisements about gardening to the user.

Although the IDFA is anonymous and user-resettable, it contributes greatly to the perception that users have that their phones are listening in on their conversations, as an interaction in one app can drive advertisement targeting in another app, which the user does not associate with that interaction.

In June 2020, Apple announced that it would be making a number of changes to privacy on iOS, under the heading of App Tracking Transparency.[3] Central to these changes is a change to the behaviour of IDFA. With iOS 14.5, apps that wish to use the user's IDFA will need to gather explicit opt-in consent from the user. This change went live on 26th April, 2021 and is now rolling out across the world with the iOS 14.5 update.

GOOGLE CHROME'S PRIVACY SANDBOX

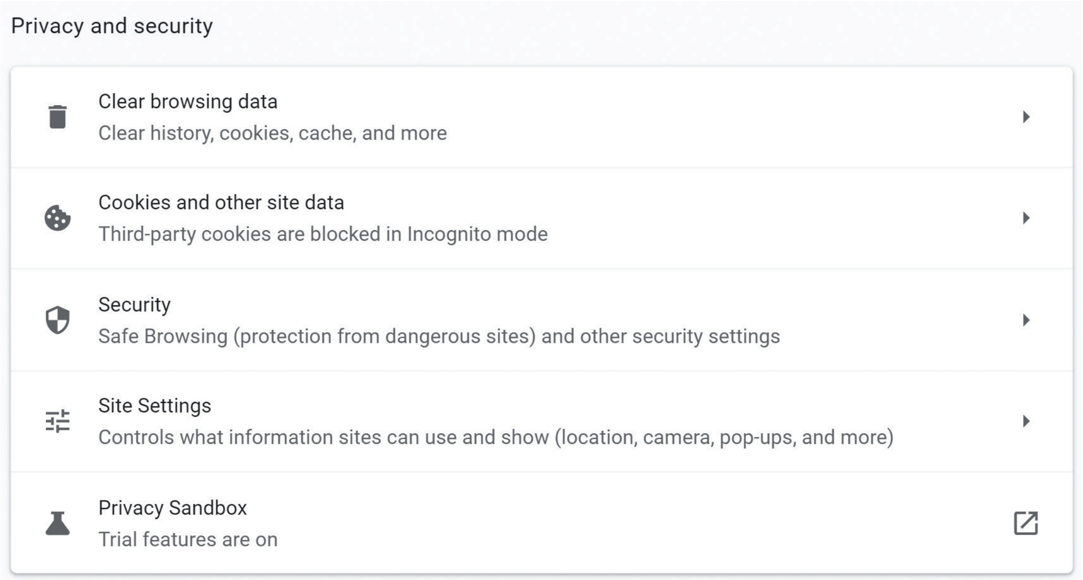
Google's relationship with tracking and user-level targeting has been very different from Apple's, because unlike Apple, it derives the majority of its revenues from advertising, much of which is user-targeted. As a result, it has been slower to introduce privacy features into its Chrome browser or Android mobile OS.

In January 2020, however, Google announced[4] that it would be phasing out third-party cookies in the Chrome browser within two years. In their place, Google is creating an open source initiative as part of the Chromium project, known as Privacy Sandbox.[5] Privacy Sandbox is a collection of technologies that Google is introducing to enable a move away from third-party cookies while not encouraging advertisers to just look for equally intrusive (and less transparent) alternatives, such as device fingerprinting. Privacy Sandbox is already live in the latest versions of Chrome (see Figure 3), although it has been largely disabled in Europe.

The Privacy Sandbox initiative represents one of several initiatives being pursued by members of the W3C's Improving Web Advertising Business Group,[6] which all share bird-themed names such as TURTLEDOVE (from Google), PARRROT (from Magnite), SPARROW (from Criteo) and PARAKEET (from Microsoft).

With the Privacy Sandbox, Google aims to provide capabilities that can replace the functions provided by third-party cookies. The most advanced and high-profile of these is a technology called Federated Learning of Cohorts[7] (FLoC), which aims to replicate the ability for advertisers to deliver interest/behaviour-based targeting groups without building cookie pools.

FLoC is a browser-based technology that places users in one or more interest-based groups (or 'cohorts') based upon the sites they visit, using a machine-learning algorithm. FLoC exposes several JavaScript functions that make it possible for a website to then discover whether the user is in a particular cohort and deliver targeted content. Because the profiling is happening within the user's browser, no user-level information is sent to the internet, so third-party sites cannot build cookie pools or



Privacy and security

Clear browsing data
Clear history, cookies, cache, and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site Settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

Privacy Sandbox
Trial features are on

Figure 3: The Google Privacy Sandbox option in Chrome

access the information directly. Through careful design of the segmentation algorithm FLoC aims to minimise the risk of the system being used to reverse-engineer user information.

To address the issue of advertisers and publishers being able to create their own interest segments, in particular to enable retargeting without cookies, Google has a second project, called TURTLEDOVE.[8] TURTLEDOVE provides a mechanism for advertisers to add users to 'Interest Groups' that are stored in the browser — for example, a shoe retailer might add someone who visits their site to an interest group called 'shoe shoppers'. At the same time, the advertiser specifies which third-party advertising networks can access this interest group information.

Later, the browser makes an asynchronous request to the advertising network(s) that were specified by the advertiser, in order to download a bundle of data (essentially, a bid plus some other serving data) that it will later use to run a browser-side auction when an opportunity to show an advertisement from that network arises (ie when the user visits a publisher site that uses that advertising network). When the user visits such a site, the browser compares the bids that it has previously downloaded and picks the highest bid.

A key idea of TURTLEDOVE is that it separates the context of the bid gathering from the actual opportunity to serve an ad. This means that advertisers cannot tailor their bids by publisher. It also makes it harder for advertisers to deliver targeted creatives within a particular interest segment. To address some of these issues, Google has extended TURTLEDOVE with a project called FLEDGE,[9] which it will be trialling later in 2021. One of FLEDGE's main additions is to allow the bidding process at ad delivery time to make a call to a trusted third-party server that can provide more contextual decision-making at the time the advertisement is requested.

Google's Privacy Sandbox, FLoC and FLEDGE all need to be properly in place and accepted by the web community and advertising industry before Google is likely to shut off third-party cookies in Chrome. Because of this, Google recently announced[10] that it was delaying this shut off until 2023.

Google hopes that other browsers that use the Chromium open source engine (such as Opera and Microsoft's Edge) will adopt the Privacy Sandbox features and implement their own versions of the algorithm. However, enthusiasm is low, with none of the major browser-makers signing on. Brave, Microsoft, Vivaldi and Mozilla have all come out against FLoC, and have disabled it in their browsers.[11]

Additionally, the reaction from regulators and other industry groups has ranged from sceptical to outright negative, with the Electronic Frontier Foundation greeting FLoC with an article entitled 'Google's FLoC is a terrible idea'.[12] Criticism of FLoC centres on two major areas of concern:

- *It does not actually represent an improvement to privacy:* FLoC replaces one set of poorly understood tracking technologies (cookies) with another (the FLoC algorithm and the data it stores in the browser). Furthermore, because the operation of FLoC involves the processing of personal data, European data regulators are considering whether explicit user consent will be needed in order to comply with GDPR/e-privacy legislation. In light of these concerns, Google has not yet enabled FLoC in Chrome in GDPR countries.[13]
- *FLoC will further concentrate advertising power with Google:* Google commanded a 31 per cent share of the digital advertising market in 2019,[14] while Chrome currently has about 65 per cent global market share in April 2021.[15] This means that Google will potentially control the interest segment definitions for almost two-thirds of the

> web's users, which raises the real risk that Google will exploit this information to grant an unfair advantage to its own advertising network.

Because of this latter issue, the UK's Competition and Markets Authority has opened an investigation into whether FLoC represents an unacceptable concentration of power with Google's advertising ecosystem.[16] The investigation will be conducted in partnership with the Information Commissioner's Office (the UK privacy regulator) to consider the privacy implications of Sandbox and FLoC also.

GOOGLE'S ANDROID ADVERTISING ID

Like Apple's iOS, Google's Android OS also sets an anonymous ID on mobile devices, called the Android Advertiser ID (AAID). Google has announced no plans to introduce any form of user consent for the use of the AAID. Privacy advocate Max Schrems has brought a complaint[17] before France's Data Protection Authority, CNIL, claiming that the behaviour of the AAID is a violation of GDPR. Schrems has had significant success in the past with bringing privacy complaints in the EU, most notably against Facebook, so his actions should be taken seriously; there is thus a significant chance that Google may be forced to implement a similar consent mechanism to Apple's, at least in Europe.

IMPACT TO THE DIGITAL ADVERTISING ECONOMY

As may be becoming clear to the reader, the situation around third-party cookies, cross-site tracking and mobile ad IDs is a very complex and rapidly developing one, and it is far from clear how it will develop. However, given Apple's actions and Google's stated intent, it is fair to assume that the writing is on the wall for cookies and ad IDs. This will have a profound impact on all parts of the advertising industry.

PUBLISHERS

Independent publishers are concerned that these changes will make it harder for them to monetise their content effectively, by making it harder to offer audience-targeted ad inventory. In these worries they have an ally in Google, which published a paper[18] in 2019 describing the result of a test it performed across 500 global publishers to estimate the impact of blocking third-party cookies on advertising revenues. The study showed that average revenue declined by 52 per cent. However, another study[19] by a trio of researchers from the Universities of Minnesota, California Irvine and Carnegie Mellon calculated only a 4 per cent drop in revenue.

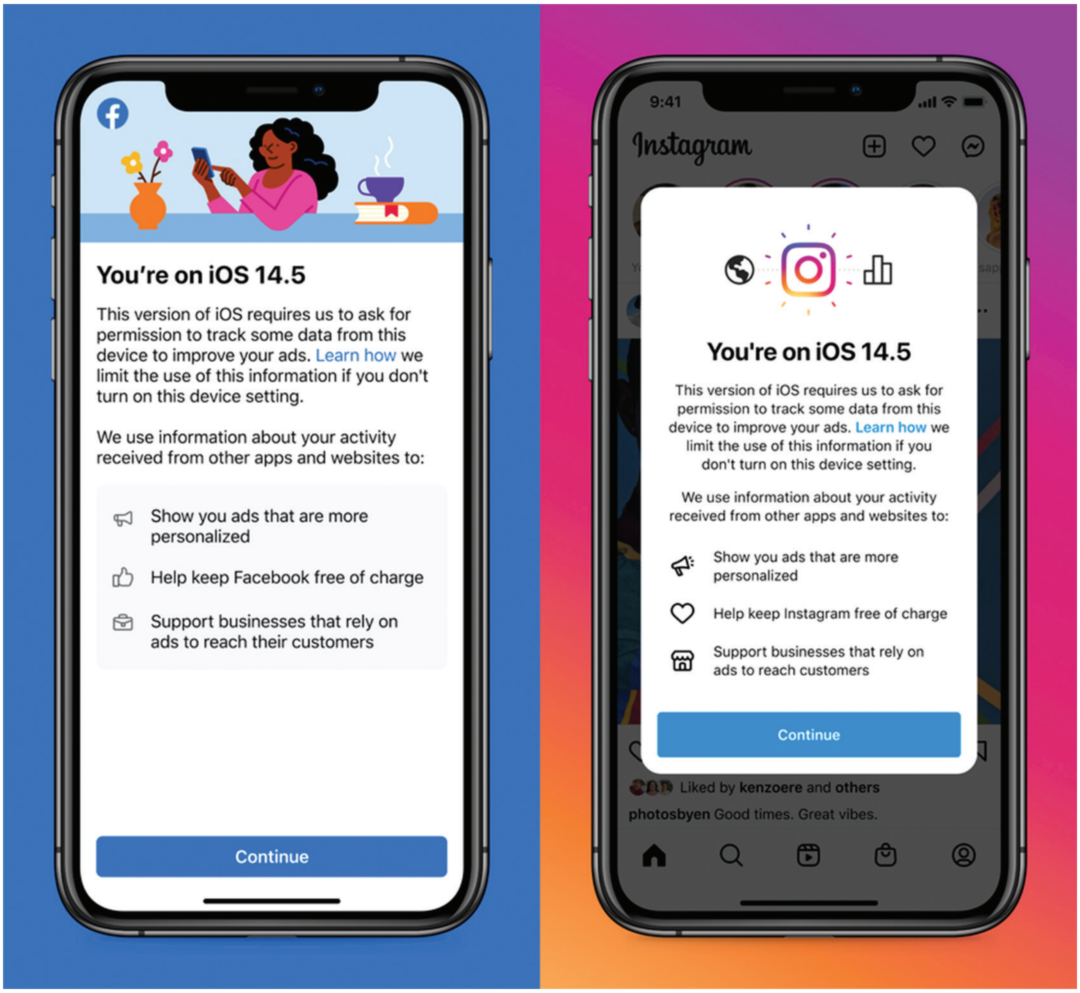
The real revenue impact is likely somewhere in the range between these two estimates, but it is important to remember that publishers will inevitably adjust their monetisation strategies to minimise the impact of losing user-targeted inventory, so it is very hard to predict the true impact on content publishing businesses.

The trials and tribulations of the print media industry in the last 20 years, seeing their advertising revenues tumble as they moved online, is a well-known story; but some of the ways that the industry has adapted, with its heavy focus on user-targeted advertisements that may be unconnected to the broader content of the site, have not served it well. The phenomenon of 'click-bait' headlines that exist purely to draw traffic to the site in the hope that it will monetise once there, likely via an advertisement that bears no relation to the site's content or brand, has cheapened much journalism. With a reduced ability to earn an 'easy' buck this way, publishers may need to focus more on generating real engagement with their content, which could be a good thing for the consumer.

The impact to the advertising businesses of Google and Facebook is harder to predict. In the run-up to Apple's new IDFA opt-in requirement, Facebook created a campaign to advocate for targeted advertising, arguing that it enables small businesses to promote themselves and enable their 'good ideas to be found';[20] and the Facebook and Instagram apps now present a pop-up screen to users on iOS 14.5 extolling the virtues of agreeing to accept cross-app tracking (see Figure 4).

In March 2021, however, Mark Zuckerberg appeared to change tack, stating that the IDFA/cookie changes could actually strengthen Facebook's business.[21] It is quite easy to see how Facebook could become more dominant, at the expense of advertisers and independent publishers, in a cookie-less world. Facebook does not need to use third-party cookies or ad IDs to offer highly targeted advertising on its own sites and apps, while sites that participate in the Facebook Audience Network would be significantly affected (as they need to serve a Facebook third-party cookie to users). This may well have the effect of driving more advertiser demand to Facebook itself at the expense of its third-party network.

Another company that will likely grow its influence in a post-cookie world is Amazon. Amazon's advertising business already accounts for an estimated 10 per cent of US digital ad spending,[22] and is steadily taking market share from Google, as many users



You're on iOS 14.5

This version of iOS requires us to ask for permission to track some data from this device to improve your ads. Learn how we limit the use of this information if you don't turn on this device setting.

We use information about your activity received from other apps and websites to:

- Show you ads that are more personalized
- Help keep Facebook free of charge
- Support businesses that rely on ads to reach their customers

You're on iOS 14.5

This version of iOS requires us to ask for permission to track some data from this device to improve your ads. Learn how we limit the use of this information if you don't turn on this device setting.

We use information about your activity received from other apps and websites to:

- Show you ads that are more personalized
- Help keep Instagram free of charge
- Support businesses that rely on ads to reach customers

Continue
Liked by kenzoere and others
photosbyen Good times. Great vibes.

Figure 4: Facebook and Instagram pop-ups on iOS 14.5

who are looking to buy something now go straight to Amazon to search for that item rather than bothering with a web search first. Amazon's other major advantage is that it can offer advertisers a complete end-to-end measurement and attribution capability as it controls the entire purchase funnel. Furthermore, Amazon can leverage its very large customer dataset to offer fine-grained user targeting for advertisers; and it can do all these things without having to rely on third-party cookies.

ADVERTISERS

Advertisers have for years been moving down a path of greater and greater reliance on user-level targeting. Many advertisers' media plans have already become somewhat hollowed out by the emergence of Google, Facebook and Amazon as behemoths in the digital ad space, often consisting of little more than a few branded run-of-site/sponsorship efforts for brand recognition, paired with audience-based buys on these networks and perhaps a programmatic platform like Criteo. A further consolidation of audience reach and engagement in the hands of these companies could further distort this picture, leaving advertisers even more at their mercy.

Moving away from purely audience-based buying will represent a substantial adjustment for advertisers and their media agencies, whose planning departments have polarised between non-addressable media (still much of television and radio) and addressable/digital media, and who will need to reconnect these two practices to bring the implied audience insights of non-addressable media back into digital.

Smaller advertisers (especially business-to-consumer advertisers), on the other hand, will likely become almost completely dependent on the 'big three', and thus dependent on their algorithms for pricing and displaying their advertisements. The presence of three major competitors for advertising dollars may at least provide some protection from price gouging, but it is hard to imagine any significant threat to this near-triopoly.

ADAPTING TO A COOKIE-LESS FUTURE

Despite the disruption and extra complexity, it will be highly worthwhile for advertisers to do more than just work within the walled gardens of Google, Amazon and Facebook in a post-cookie world. Here is a list of areas that advertisers and marketers should investigate, and some areas they should avoid:

- *Content/contextual targeting:* Contextual targeting (using the content of the page or video in which an advertisement appears as a means to decide which advertisement to show) is one of the oldest forms of ad targeting, and thanks to platforms like Google AdSense it has continued to be an important if less glamorous form of ad targeting. In a study[23] by GumGum in 2018, 26 per cent of UK respondents and 31 per cent of US respondents planned to increase their spend on contextual targeting, driven by the desire to achieve compliance with laws like GDPR and keep up with industry trends on using user data for targeting.

  Contextual targeting must be done carefully, to avoid potentially embarrassing combinations of serious/upsetting content (such as a news story about a train crash) with advertisements that could be deemed inappropriate in such a context (such as an advertisement for a train company). This requires more care than 'fire and forget' user-targeted advertising (which can nevertheless generate its own issues when it runs alongside inappropriate content[24]). Nevertheless, this could end up creating a benefit for advertisers and publishers — if there is more connection between the content that individuals are consuming and the advertisements that run alongside that content, those advertisements are likely to be more memorable. Another study[25] by GumGum and SPARK Neuro claimed that contextually-relevant advertisements showed a 2.2-fold increase in ad recall.

- *Driving upper-funnel conversions:* Another way for advertisers to address the demise of third-party cookies is to build their own audience data and use that for targeted customer relationship marketing. While this strategy is very much in evidence on the many websites that bombard users with invitations to sign up for marketing e-mails, there is room for more innovation, in order to provide a better trade-off of value to the user for the right to capture some information about them. Applying some of the principles of content marketing from business-to-business (the 'enter your details to get our white paper' model) may enable business-to-consumer marketers to create an exchange of value in return for some user data.
- *Gathering retargeting consent:* Apple's privacy framework, in particular its Storage Access API, provides advertisers with a mechanism for gathering a kind of 'retargeting consent' that would allow some third-party cookie usage (for a limited amount of time); while the FLEDGE proposal from Google could permit something similar (albeit via a different mechanism). This could lead to a situation where users are asked if they would like to be reminded about a site as they move around the internet. While the idea that users would actively opt into retargeting might sound far-fetched, those that do would likely have high intent to purchase, meaning that an approach like this could reap disproportionate benefits.
- *Device fingerprinting/alternatives to cookies:* It may be tempting to attempt to fall back on some other methods of identifying 'unique' users, such as device fingerprinting (a combination of device user agent, IP and other information) or using browser LocalStorage. Advertisers should avoid doing this — not least because Apple's and Google's privacy efforts are designed to block device fingerprinting, but also because it runs afoul of GDPR, as users cannot switch off or withhold their device fingerprint (at least not easily).

CONCLUSION

The imminent demise of third-party cookies will deliver privacy benefits for users, and may help to make digital and mobile advertising feel less creepy and intrusive, although it may also make it less relevant. At the same time, however, it will also likely strengthen the hands of Google, Facebook and Amazon as they continue to grow their walled-garden advertising ecosystems that are much less dependent on third-party cookies and data flows. As well as looking for other ways to buy relevant advertising inventory (such as via contextual targeting), advertisers should remain wary of becoming completely dependent on one of these providers, as this could leave them highly vulnerable to price shocks and other disruptions. Meanwhile, advertisers and marketers should continue to look for creative ways to build first-party data about their audience, to enable more personalised and targeted communications towards the top of the funnel.

References

1. Facebook (n.d.) 'Facebook Audience Network', available at: https://www.facebook.com/audiencenetwork (accessed 27th May, 2021).
2. Wilander, J. (2018) 'Introducing Storage Access API', available at: https://webkit.org/blog/8124/introducing-storage-access-api/ (accessed 27th May, 2021).
3. Apple (n.d.) 'App Tracking Transparency (Apple Developer Documentation)', available at: https://developer.apple.com/documentation/apptrackingtransparency (accessed 27th May, 2021).
4. Schuh, J. (2020) 'Building a more private web: A path towards making third party cookies obsolete', available at: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html (accessed 27th May, 2021).

5. Google (n.d.) 'The Privacy Sandbox: Technology for a more private web', available at: https://www.privacysandbox.com (accessed 27th May, 2021).
6. Worldwide Web Consortium (n.d.) 'Improving Web Advertising Business Group', available at: https://www.w3.org/community/web-adv/ (accessed 27th May, 2021).
7. GitHub (n.d.) 'Federated Learning of Cohorts (FLoC)', available at: https://github.com/WICG/floc (accessed 27th May, 2021).
8. GitHub (n.d.) 'TURTLEDOVE', available at: https://github.com/WICG/turtledove (accessed 27th May, 2021).
9. GitHub (n.d.) 'First Experiment (FLEDGE)', available at: https://github.com/WICG/turtledove/blob/main/FLEDGE.md (accessed 27th May, 2021).
10. Google, (2021) 'An updated timeline for Privacy Sandbox milestones', available at: https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/ (accessed 29th June, 2021).
11. Endicott, S. (2021) 'Microsoft, Vivaldi, Mozilla, and Brave turn down Google's FLoC', available at: https://www.windowscentral.com/microsoft-vivaldi-mozilla-and-other-browser-makers-turn-down-googles-floc (accessed 27th May, 2021).
12. Cyphers, B. (2021) 'Google's FLoC is a terrible idea', available at: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea (accessed 27th May, 2021).
13. Schiff, A. (2021) 'Google will not run FLoC origin tests in Europe due to GDPR concerns (at least for now)', available at: https://www.adexchanger.com/platforms/google-will-not-run-floc-origin-tests-in-europe-due-to-gdpr-concerns/ (accessed 27th May, 2021).
14. T4 (n.d.) 'Internet advertising market share', available at: https://www.t4.ai/industry/internet-advertising-market-share (accessed 27th May, 2021).
15. Statcounter (n.d.) 'Browser market share worldwide', available at: https://gs.statcounter.com/browser-market-share (accessed 27th May, 2021).
16. Competition & Markets Authority (2021) 'CMA to investigate Google's "Privacy Sandbox" browser changes', available at: https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (accessed 27th May, 2021).
17. Noyb (2021) 'Complaint Under Article 82 Loi No. 78-17 du 6 Janvier 1978', available at: https://noyb.eu/sites/default/files/2021-04/AAIDcomplaint_Redacted.pdf (accessed 27th May, 2021).
18. Ravichandran, D. and Korula, N. (2019) 'Effect of disabling third-party cookies on publisher revenue', available at: https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf (accessed 27th May, 2021).
19. Marotta, V., Abhishek, V. and Acquisti, A. (2019) 'Online tracking and publishers' revenues: an empirical analysis', in Proceedings of the 2019 Workshop on the Economics of Information Security, available at: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf (accessed 27th May, 2021).
20. Facebook (n.d.) 'Supporting small business with personalized ads', available at: https://about.facebook.com/supportsmallbusiness/personalized-ads (accessed 27th May, 2021).
21. Rodriguez, S. (2020) 'Zuckerberg: Facebook may be stronger after Apple privacy changes', available at: https://www.cnbc.com/2021/03/18/zuckerberg-facebook-may-be-in-stronger-position-after-apple-ios-14.html (accessed 27th May, 2021).
22. Perrin, N. (2020) 'Amazon Advertising 2020', available at: https://www.emarketer.com/content/amazon-advertising-2020 (accessed 27th May, 2021).
23. Drum Studios & GumGum (n.d.) 'Contextual advertising: the new frontier', available at: https://insights.gumgum.com/hubfs/Contextual-Advertising-the-new-frontier-final-guide.pdf (accessed 27th May, 2021).
24. Mostrous, A. (2017) 'YouTube hate preachers share screens with household names', *Times*, available at: https://www.thetimes.co.uk/article/youtube-hate-preachers-share-screens-with-household-names-kdmpmkkjk (accessed 27th May, 2021).
25. GumGum & SPARK Neuro (n.d.) 'Cognitextual: a neuroanalytic study of contextual ad effectiveness', available at: https://insights.gumgum.com/hubfs/Advertising/Advertising%20Newsletter/Volume%20IV/Cognitextual%20Study%20FULL%20GUIDE%20(1).pdf (accessed 27th May, 2021).