February 2021

A GUIDE TO THE POST THIRD-PARTY COOKIE ERA

iabeurope.eu

iab europe

Contents

Contents

Introduction

In May 2020, IAB Europe released a 'Guide to the Post Third-Party Cookie Era', to prepare brands, agencies, publishers and tech intermediaries for the much-anticipated post-third-party cookie advertising ecosystem. The guide, which had been developed by experts from IAB Europe's Programmatic Trading Committee (PTC), provided a level-setting background into the current use of digital advertising cookies, the contributing factors to their depletion and an overview of the alternative solutions that are currently available.

As solutions have evolved, the PTC has now updated the Guide to provide the latest information and guidance on market alternatives to third-party cookies. One year on from the announcement that third-party cookies would be depleted, this edition of the Guide will provide the most up to date answers to the following questions:

- How will the depletion of third-party cookies impact stakeholders and the wider industry including Proprietary Platforms?
- How will the absence of third-party cookies affect the execution of digital advertising campaigns?
- What solutions currently exist to replace the usage of third-party cookies?
- What industry solutions are currently being developed and by whom?
- How can I get involved in contributing to the different solutions?

Industry Insights

To understand how involved stakeholders were with the different initiatives and how prepared they are for the new era, IAB Europe ran an industry poll in Q4 2020. Respondents were asked what new opportunities and challenges stakeholders foresee, and how prepared they are for these changes. They were also asked about the impact they think it will have on targeting, measurement, verification and overall investment. Over 100 industry professionals completed the poll and top line findings showed:

Priority in finding an alternative to the third-party cookie - nearly half of all respondents (and we had over 100 responses) said that it was critically important to find a solution. Only 13% cited it wasn't very important.

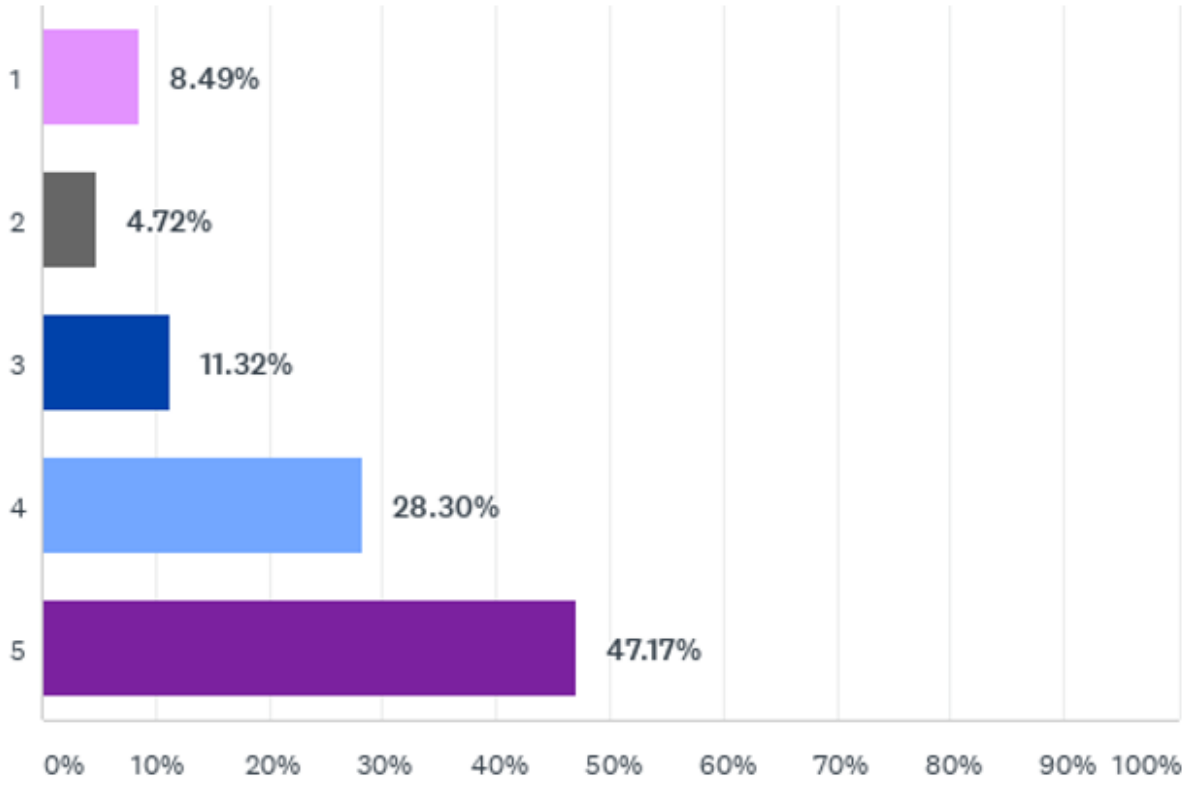


Figure1: *How much of a priority is finding an alternative to the third-party cookie? (1 not being important at all, 5 critically important).*

Preparedness in finding a new solution - But conversely, whilst it is a high priority, the majority are not prepared.

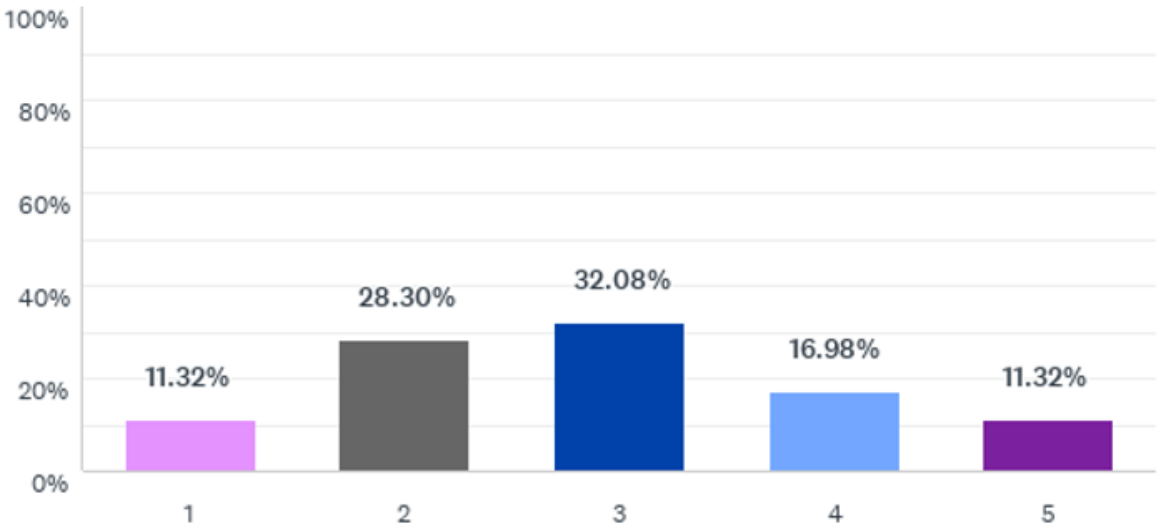


Figure 2: *How prepared is your company for the post-third party cookie era? (1 being not prepared at all 5 being very prepared).*

This is the purpose of the guide. To show the industry what is being developed and encourage participation in testing, collaboration and learning.

So to help stakeholders navigate and prepare for the post-third-party cookie advertising era, in this updated edition of the guide, additional key questions will also be covered:

- What alternative solutions may be suitable for my business?
- How can my company get involved in contributing to the industry wide solutions?
- How can we identify ID solutions to test and work effectively with?

This guide will continue to be regularly updated to reflect the changes and developments within the industry.

Section 1. Background Information

In August, Chrome announced a new initiative (known as Privacy Sandbox) to develop a set of open standards to fundamentally enhance privacy on the web. In January 2020 they then announced their plans to phase out support for third-party cookies in Chrome within the next two years. The blocking of third-party cookies in Chrome will bring the single biggest change to the digital advertising ecosystem since the introduction of real-time bidding in 2009. Currently, approximately 30% of available impressions are rendered on browsers (mostly Safari and Firefox) with no third-party cookies. As Chrome accounts for approximately 60% of the remaining browser usage, their announcement to phase out support for third-party cookies will essentially end cross-publisher based advertising.

While some industry commentators and thought leaders have gone to great lengths to paint a bleak picture of a cookie-free future, we need to be clear that this does not apply to all cookies. **First-party cookies** are stored by the domain (website) that a user visits directly. **Third-party cookies** are created by domains other than the one a user visits directly, hence the name **third-party**. Whilst they are used for cross-site tracking, retargeting and ad-serving they are also used to improve ad serving capabilities with frequency capping, creative sequencing and optimisation.

Giving the match rate issues involved, commentators have also said that the depletion of third-party cookies is a natural evolution of digital media, and one that has long been on the cards. Eliminating third-party cookies undoubtedly impacts multiple stages of the digital advertising supply chain, but suggesting it is going to be a death knell to the industry or destroy third-party audiences altogether, is misleading. It is, therefore, important to understand the changes it will make to how a campaign is served and delivered, to ensure solutions or alternative ways of reaching an audience can be achieved. Firstly, web (desktop and mobile enabled websites) and in-app are often separated. Cookies are a web-only technology, while in-app mobile ad identifiers (e.g. IDFA, AAID) or MAIDs, which are provided by the operating system, are currently used for identification.

From an advertising perspective, this will result in the following fundamental changes:

- Frequency capping dependent on cross-publisher identifiers, so without such identifiers this feature will no longer be available in its current form.
- Syndicating marketers first-party data to a publisher, transforms it into third-party data which without cross-publisher identifiers, retargeting or other forms of cross-publisher audience targeting will no longer be possible.
- First-party publisher data will also not be able to be used by publishers for audience extension without cross-publisher identifiers.
- Audience-based dynamic creative optimisation (DCO) will be greatly hindered without cross-publisher identifiers.
- DMPs (Data Management Platforms) cannot create identifier linkages in the same way they do today.
- View-through or multi-touch attribution will no longer be possible.

Most campaigns today will have at least one of these features applied, which means nearly all campaigns will have to find new approaches. With all of this in mind, it is essential to differentiate between two things:

- storage and access
- (campaign) data

Storage and Access

The browser knows two different storage types: cookies and web storage (also referred to as Document Object Model or DOM storage). Web storage comes as session storage and local storage (LSO), both allowing you to persist data on the browser client system similar to cookies. In simple terms, web storage is a further development of cookies, allowing much more capacity for storage and better developer APIs but also has differences to cookies. While cookies can be read by client and server, web storage is a client only technology, i.e. cookies are always sent with the HTTP(s) request of a page, while local storage needs to be explicitly read/written by JavaScript.

A cookie consists of a name (=key), a value (some data, e.g. ID for Advertising or other) and attributes (e.g. domain, path, expiry date, size, HTTP only, secure and samesite). The attributes mainly define data access allowance and lifetime. If a cookie is a first or third-party one, depends on the context it is read and written from. The context from where it is accessed defines if access is allowed or permitted. The cookie itself is a form of storage which can hold data, but it is not an identifier itself.

Publisher Example

Imagine you run mail.com, all cookies read and written in the same domain are first party, while all (not client-facing advertising) scripts embedded in the website from other domains (e.g., ssp.eu or adserver.eu) would be considered third-party and therefore so would cookies that are read from or written to them.

Advertiser Example

Even if an advertiser writes a cookie on their own www.advertiser.eu domain as a first-party for latter use in retargeting, this information cannot be accessed later on during ad delivery on the publisher website e.g. mail.com in order to deliver a personalised product ad with frequency capping and regency control, since from mail.com's perspective it is a third-party cookie.

Alternative, server side storage solutions, independent of web or in-app, are being developed in the context of advertising with the broad deprecation of third-party cookies in browsers and the rise of login based identifiers. More information on the alternative solutions being developed is detailed in section 5.

Campaign Data

In case an identifier to associate cross-publisher sessions exists, user-centric data can be highly beneficial to each campaign KPI. Campaign data, such as audience information, frequency capping and even performance related to contextual targeting, is not necessarily stored in the same place as the identifier itself, but typically on the server-side (e.g. in a DMP).

A standard case of data points related to an addressable user (i.e. a user related to via a persistent identifier) for nearly any campaign is "frequency capping". Advertisers or agencies use frequency capping to restrict the amount of times a user sees a campaign or creative within a specific timeframe. It doesn't matter if this frequency capping is set on a campaign, creative or inventory level, the target is to control the media spend per user.

The absence of frequency capping can significantly decrease the user experience for end users and maybe increase resistance to advertising. The removal of third-party cookies dramatically influences the ability of the buy side to control that aspect of a campaign.

Performance Marketing has been heavily built on (retargeting/intend) data points which associate product level, product category or shopping basket data to an addressable user.

Digital Brand Marketing campaigns use sociodemographic (e.g. age, gender, income, household size, family status), geo (IP, zip code, lat/lon), technical (Device, OS, browser, ISP, connection, screen size), affinity or interest data associated with an addressable user.

Stakeholder Evolution

Every stakeholder involved in the digital advertising ecosystem will somehow be affected by the depletion of third-party cookies. All stakeholders can expect reduced opportunities to collect and activate data at a user / device level given most publishers' reliance on cross-publisher identifiers.

Agencies will mostly take care of the conceptual workload, both for creating technology plans for advertisers and ensuring planning and buying continue in an audience activation manner. It is important for **marketers** to better understand their own customers and their first-party data will be key to this.

Publishers will need to reorganise their audience data collection and extension strategies. Communication between publishers, agencies and advertisers will be much more important.

DSPs and SSPs will need to ensure their technology can continue to deliver optimised digital advertising. DSPs are creating or joining ID marketplaces to overcome this challenge (more information in section 5).

SSPs are starting to construct new relationships with the buy side. In addition to supply path optimisation, they are providing extended ID sharing opportunities regarding measurement and engagement.

Section 2. The Three Contributing Factors to the Depletion of the Third-Party Cookie

There are three key areas to look at in terms of the developments in digital advertising over the last two years, which are resulting in diminished access to third-party cookies:

1. The Legal Environment Related to Data Collection and Use
2. Browser Gatekeeping
3. Ad Blocking

2.1 The Legal Environment Related to Data Collection and Use

The fundamental right to data privacy is recognised in many jurisdictions around the world. It empowers individuals with the right to know how their personal data is used and shared, including for purposes related to digital advertising. While the resulting additional transparency and control serve to improve user trust in the entities that handle their data, the compliance burden and effective exercise of rights by individuals, can constrain the collection of data, and thus the ability of publishers - whose revenue typically depends on the delivery of data-driven advertising - to adequately collaborate with third-party partners, in order to finance content services and journalism.

There is no singular overarching law regulating online privacy worldwide. Instead, a patchwork of regional, federal, state and local laws with varying degrees of stringency apply. That being said, under the leadership of the European Union (EU), whose member States have been pioneers in the development of strong privacy and data protection rules, a convergence can be observed, with the introduction of increasingly robust regulations in several jurisdictions, modelled on the EU's General Data Protection Regulation (GDPR).

While the legal landscape evolves continuously, the following section provides a snapshot overview of just some of the existing and upcoming regulatory instruments that impact the use of cookies, consumer choice, and tracking their digital activity.

EU's ePrivacy Directive and General Data Protection Regulation (GDPR)

The EU's ePrivacy Directive is the main EU instrument constraining the storage and access operations on user's devices. In accordance with the Directive, obtaining consent from the user is a precondition to any storage or access operation (e.g., of a cookie) on their device, irrespective of whether that operation concerns identifiable data. Such consent must be prior, freely given, specific, informed and unambiguous. In 2017, a proposal for a new ePrivacy Regulation to replace the Directive was published, to ensure further harmonisation of the rules. The latter is currently in the final stages of negotiations between European institutions.

In turn, the GDPR requires a legal basis for processing any personal data collected. It also guarantees a number of rights to users, directly connected to their personal data such as right of access, right to rectification, right to erasure, right to data portability and right to object. Online identifiers such as cookies and device identifiers are examples of personal data under the GDPR. Companies who engage with residents of the EU are required to comply with its provisions.

As a result of the combined requirements of the ePrivacy Directive and GDPR, obtaining user consent for the collection of personal data through cookies for the purpose of online advertising and analytics has, in many EU Member States, been implemented through "consent banners" – a banner placed at the top or bottom of a webpage containing disclosures with a consent request. Such banners have expanded over time to include additional information, beyond storage and access operations, which provides transparency into processing activities carried out in support of people's access to and navigation across publishers.

Transparency and consent requirements have brought about the adoption of tools such as IAB Europe's Transparency and Consent Framework (TCF), which is a cross-industry compliance standard created to facilitate compliance with certain provisions of the GDPR and ePrivacy Directive. It standardises how publishers, advertisers and ad tech vendors disclose the purposes for which they wish to use data and obtain permissions from the user.

California's Consumer Privacy Act (CCPA) and Privacy Rights Act (CPRA)

The CCPA was introduced as a State Law in California and enacted on 1 January 2020. Although the CCPA does not, like the GDPR, require users to opt-in to the collection and use of their personal information, it requires the implementation of specific privacy notices and opt-out tools. Specifically, the CCPA provides users with ownership over any privacy information and requires businesses processing California users' identifiable personal information to enable users to *inter alia*:

- Know what identifiable personal information is collected;
- Know whether and to whom their personal information is disclosed;
- Opt-out of its sale;
- Access any personal information collected; and
- Request deletion of personal information collected.

The CPRA, adopted in November 2020, revises and expands the CCPA, enhancing the rights granted to consumers, introducing additional requirements for businesses, and creating new enforcement mechanisms. The CPRA is scheduled to enter into force in January 2023.

California is the first state in the United States to pass such a comprehensive privacy law of this nature. However, there are a number of other state bills currently in various stages of review and legislation.

Canada's Consumer Privacy Protection Act (CPPA)

The CPPA was introduced in November 2020 with a view to increasing protections for users personal information by giving them more control over how businesses collect and process such data. The CPPA is the first major overhaul of Canada's PIPEDA (Personal Information Protection and Electronic Documents Act), which came into force in 2000. Under the CPPA, businesses are required to:

- Provide plain-language information for consumers so they can fully understand and meaningfully consent to use of their personal data;
- Provide users with the ability to transfer their personal data between businesses;
- Provide users with the ability to withdraw their consent and have their data deleted;
- Provide transparency into systems relying on artificial intelligence and making use of automated decision-making; and
- Provide the ability for users to have personally identifiable information removed.

Brazil's General Data Protection Law (LGPD)

The LGPD entered into force in September 2020 and is Brazil's first comprehensive privacy and data protection law to date. The LGPD is based on the EU's GDPR and is very similar in terms of its territorial (i.e., it applies to any organisation that processes personal data of users in Brazil) and material scope.

Under the law, organisations must establish a legal basis to process personal data and users are granted with rights very similar to those under GDPR, including rights to access, rectification, data portability, etc. The LGPD also contains rules with regard to governance and accountability and requires organisations to appoint data protection officers, maintain records of processing activities and implement detailed privacy notices.

So what do all these laws mean for user choice and tracking today?

1. Users have more rights than ever to control how their personal data/information is used in the digital advertising ecosystem and they're becoming increasingly aware of these rights.
2. Across the globe, the privacy and data protection legal framework is developing rapidly and companies need to do their utmost to comply with the law while using data for advertising related purposes, as well as meet user expectations.
3. Companies need to consider significant improvements, both in terms of technology and policy, to be able to track and target audiences across the web.
4. The need to comply with transparency, consent and personal data processing obligations does not end with the deprecation of third-party cookies.

2.2 Browser Gatekeeping

Increased awareness about privacy and the tracking of individuals on the Internet has resulted in new laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) to protect an individual's privacy as described above. In addition to simply complying with these laws, many companies are altering the ways in which other parties can access and use individual's personal data/information.

Market shares of browsers in Europe leave little room for interpretation. Chrome (60%) is by far the dominant player, be it on desktop or mobile devices, followed by Firefox (13.5%) and Safari (9.7%). Firefox has an exceptionally high share in Germany (25%), compared to all other EU countries.

Changes implemented by these browsers that alter the way in which other parties, such as publishers, advertisers, and ad tech companies can collect and use personal information/data therefore have a huge impact on the market.

The following overview should summarise what we could call the end of the third-party cookie era.

Safari (Apple)

Amongst all browsers, Safari has the longest history with these types of initiatives. Apple's goal for their WebKit web-browser engine is to "do its best to prevent all covert tracking, and all cross-site tracking". The company has been incorporating "Intelligent Tracking Prevention" (ITP) functionality incrementally into their browser for the last 2+ years. As market actors change their tactics to get around ITP's latest changes, Apple reduces their ability more and more to perform cross-site tracking.

With ITP 1.0 rolled out in June 2017 they blocked most third-party tracking cookies using in-browser machine learning.

As a result, if the user has not interacted with a tracking website in the last 30 days, third-party cookies are automatically deleted and all new third-party cookies from the site are blocked. If they have visited the tracking website resulting in the creation of a first-party cookie, this cookie can only be used in a third-party context for 24 hours. After 24 hours, the cookie can only be used in a first-party context. After 30 days without a return visit to the tracking website, the cookie is deleted.

The ITP functionality was updated as follows:

- March 2018: Addition of protection against HTTP Strict Transport Security (HSTS) abuse, by preventing a backdoor tactic used to create a persistent cross-site ID, used by illicit trackers.
- June 2018: Eliminating the 24-hour window during which first-party cookies can be used in a third-party context.
- February 2019: Blocking all third-party tracking cookies and limiting the lifecycle of first-party cookies to 7 days.
- April 2019: Reducing the maximum expiration for client-side first-party cookies to 24 hours when navigation to the site is through a "tracking website".
- September 2019: Made client-side first-party cookies expire after 24 hours, so that all "script writable" website data (primarily LocalStorage) will expire after 7 days.

These updates resulting in ITP 2.3 removed targeted advertising within Safari, and resulted not only in revenue declines for Publishers, but also removing those devices from many advertising campaigns. While these changes impact open web properties, it is important to note they do not impact the monetisation of apps in Apple's app store.

Mozilla Firefox - Enhanced Tracking Protection (ETP)

Firefox has made a strong play to position themselves as providing strong privacy protections. Mozilla's Anti-Tracking Policy enumerates their goals related to the uses they intend to block, only some of which are currently able to do. Like Apple, their goal is also to eliminate the ability to perform what they term covert or cross-site tracking.

Mozilla's version of the cookie limitation is called "Enhanced Tracking Prevention" (ETP). Mozilla initially announced a default activation of ETP, which was made available in beta versions to block third-party cookies based on the disconnect.me URL list, with v63 in October 2018. The default activation was not live until v65 in January 2019, even when ETP itself was already made available in deactivated mode.

Mozilla describes the feature as the following: Simplified content blocking settings give users standard, strict, and custom options to control online trackers. A redesigned content blocking section in the site information panel (viewed by expanding the small "i" icon in the address bar) shows what Firefox detects and blocks on each website you visit.

In June 2019, Mozilla followed up with v67.0.1 by activating the ETP feature on default for all "new" installations, thus increasing the third-party cookie block rate within Firefox to about 20% for the upcoming months.

Finally, at the beginning of September 2019, Mozilla activated the ETP feature within its v69 release by default for all "existing" installations. This resulted in third-party cookie blocking for up to 80% of the users within several weeks.

This solution relies on blacklists of websites known to perform tracking during private browsing or when in strict mode during all browsing. ETP blocks not only cookies for tracking sites, but blocks the actual calls to these sites. Users can easily switch to strict mode, which uses the second list, and enables call blocking for all browsing, rather than only for private browsing. However, strict mode breaks many websites (for example, sites using Adobe Launch or Dynamic Tag Management products to load functionality visible to the user). In the custom mode, users can elect to use the less restrictive list, but have it always enabled or they can choose to block third-party tracking cookies, but allow the calls. It is important to note that the overwhelming majority of Mozilla's funding derives from search advertising that does not rely on cookies.

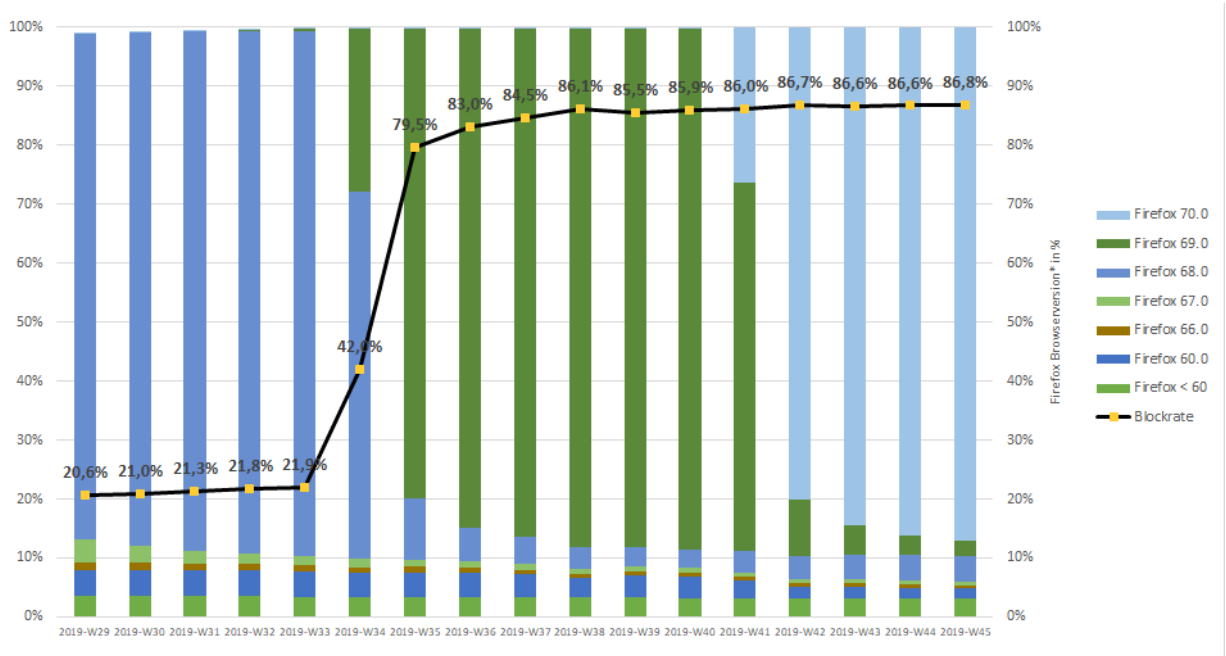


Figure 3: *Third-party cookie blocking rate measured for Mozilla Firefox in 2019*

Edge (Microsoft)

In a June 2019 blog post Microsoft announced the introduction of "Microsoft Tracking Prevention" (MTP). It appears very similar in functionality to Firefox's Enhanced Tracking Prevention, and may share open source code from disconnect.me. MTP offers three protection levels; basic, balanced (recommended) and strict. Balanced is the default. Unlike Firefox, MTP doesn't have a custom mode, and doesn't behave differently between InPrivate mode and not. Like ETP, it blocks third-party cookies from known tracking sites, and in strict mode blocks calls to those sites.

MTP was released to the public in Version 80 of Microsoft's Edge browser, launched on 15th January 2020. According to Microsoft, the three tracking prevention modes (especially the Strict mode) will help protect against the type of personalisation that leads to fingerprinting. Edge does not block ads natively, but you can download ad-blocking extensions. As the browser is now based on Chromium, many Chrome extensions (as well as extensions from the Microsoft Store) will work with this latest version of Edge, a distinct advantage.

Chrome (Google)

Google's Chrome announced in July 2019 an incoming change in the cookie labelling to improve some aspects of privacy and security. Following those announcements on 4th February 2020, Chrome started rolling out a new security feature that will require third-party cookies being labelled with "SameSite=None" and "Secure", making it mandatory to ensure those cookies are read via HTTPs.

In January, 2020 the company announced the plan to phase out support of third-party cookies in Chrome within two years. They would be replaced by a privacy preserving alternative that would make third-party cookies obsolete. The initiative of the "Privacy Sandbox" in their words will: "Create a thriving web ecosystem that is respectful of users and private by default.". The Privacy Sandbox represents an alternative pathway that Google, discussed with other industry stakeholders, is providing for the digital advertising industry to take, relying on anonymised non-addressable signals (that are not cookies) and five Application programming Interfaces (APIs). Advertisers will be able to use each API to receive aggregated data about issues like conversion and attribution (which entity is credited, say, for a purchase). The latest Chrome Blog announcements include trust tokens and a click conversion measurement API.

In March 2021, Chrome announced they will launch an origin trial for the Federated Learning of Cohorts API (FLoC), a way to reach people with relevant content and ads by clustering large groups of people with similar browsing patterns. Google Ads shared an update from their tests of the FLoC algorithm, which shows that the proposed API could be used to serve relevant interest-based ads. Chrome's new FLEDGE proposal (First "Locally-Executed Decision over Groups" Experiment) expands on TURTLEDOVE, a proposal that addresses how companies can build audiences, and reach prior visitors to their websites through remarketing. FLEDGE includes a way for on-device bidding algorithms to use additional information from a new trusted server designed for this purpose. The Aggregate Measurement API, which helps measure how many times unique users viewed an ad across multiple sites, will be opened up via public origin trials in H1 2021.

2.3 Ad Blocking

Ad blocking in a browser is a capability which removes online advertisements displaying on a website or web page. The most common ad blocking tools are browser extensions. Over the years, browsers started to incorporate core features of ad blocking extensions into their browser versions. One example is Mozilla's Firefox "Enhanced Tracking Protection" (ETP) which was default enabled beginning of September 2019 with the rollout of Firefox version 69.

In recent years, ad blocking is increasingly incorporated into the app ecosystem as well, but still lacks traction compared to browsers.

Today we see ad blocking and tracking script blocking as the two core features of these tools. They typically rely on external URL blacklists such as disconnect.me (used by Firefox ETP) or easylist.to (used by Adblock Plus browser extension) which are more or less publicly managed. But there are also AI driven approaches used to filter advertising and tracking.

The tools either prevent adtag delivery or they block the loading of any script domains known to be used for tracking and profiling. The two methods are blurred by now, since nearly any tracking or ad blocking tool provides both features.

The average ad blocking rate varies by market and the most common reasons to use ad block and tracking script tools are:

- Privacy concerns (personal data leakage)
- Security reasons (e.g. malware)
- Faster loading of websites
- Less distraction in content
- Save bandwidth (especially on mobile devices)
- Save battery

Aside from the “direct” ad blockers, be it a browser or browser extension feature, a less known factor are the indirect ad blockers rolled out by virus scanner applications. They offer either traffic filtering or install extensions without an easy option for users to deactivate or influence this behaviour.

Section 3. The Impact on Stakeholder Usage of Proprietary Platforms

The digital advertising industry has previously observed that seismic shifts in data privacy solutions and regulation sometimes bestow, inadvertently, greater dominance onto the proprietary platforms. A proprietary platform is any buying point that sits outside of the normal open RTB ecosystem and allows for the use of media, data or buying opportunities outside of that ecosystem. Historically many large publishers would sell the more premium subsets of their inventory (e.g., homepage masthead) directly / privately. Programmatic started as a way to help publishers sell scalable and make incremental revenue from the remainder of their inventory (that they found more difficult to sell directly). Proprietary platforms are now starting to appear from major publishers (or groups of publishers), data companies, demand platforms and even agencies. In an ecosystem without third-party cookies, proprietary platforms may be able to offer targeting based on a substantial amount of directly-identifiable, first-party data. However, in return for accessing the wealth of data, proprietary platforms may impose restrictions in control and transparency to buyers.

3.1 Proprietary Platforms and Advertisers

Investment in the open internet is increasingly important, to support scale and competitive pricing for advertisers, optimised demand for publishers, and increased content choices for consumers. It's therefore important that advertisers do not become reliant on just Proprietary Platforms to reach consumers. This may impact both reach and control & transparency:

Reach: Viewer attention is increasingly fragmenting, as consumers access content across screens and platforms both in the Proprietary Platforms and on the open internet. All the while, viewing content on an ever-expanding variety of platforms while 60% of advertising spend consistently goes into the platforms. If advertisers are investing most of their budget in these platforms, they risk missing opportunities to connect with their audience at scale.

Control and transparency: Proprietary Platforms prevent the sharing of log-level-data, restricting buyers' ability to validate data outside of that provided by the platforms themselves. The absence of log-level-data makes it difficult to validate results provided by the proprietary platforms. In addition, it hampers the ability for buyers to compare and attribute results from multiple platforms, reducing the value of this type of analysis and stifling competition.

3.2 Proprietary Platforms and Publishers

The loss of third-party cookies will put increasing pressure on publishers as yield and floor prices will drop, due to fewer buyers understanding the value of their bidding on specific advertising slots, which in turn impacts overall revenue.

It is also important to note that when we use the term publishers, we are referring to any site that makes its own content. This differs from platforms that are reliant on its consumer to make the content for them i.e. YouTube, Twitter, Instagram, Facebook, who also don't rely on third-party cookies, as they have their own logged-in user solution in place, so will be barely affected by the changes.

Estimates show that 70% of buyers rely on third-party cookies in 2020, therefore not only will advertisers be unable to segment users, but campaigns won't be able to run due to a reduction in data from the buy-side. Lack of frequency capping on the buyside will also impact campaigns resulting in closer relationships with publishers that are able to scale campaigns and utilise their first-party data. Previously buyers would have run campaigns across hundreds of publishers and overlaid their own audience targeting.

Many publishers still have a reliance on audience extension, whereby publishers use their first-party data across a network of premium publishers, when third-party cookie deprecation comes into play publishers will no longer be able to access this and revenue would be seriously hampered.

It is essential that publishers can find a balance to ensure that they create a great user experience for readers, offer a data solution for advertisers, and minimise their reliance on proprietary platforms to ensure sustainability.

3.3 **Proprietary Platforms** and Consumers

Without the choice of an open internet, consumers will have to increasingly pay to consume premium content or access it within proprietary platforms. Imagine a world where you can check the news only within a proprietary platform – it's not ideal. Indeed, access to free quality content from a range of sources is what makes the open internet so valuable. Consumers want choice and the ability to access trusted news sites that are available for all. They want the option to be able to access ad-funded "free" content or pay for content - a hybrid approach to content consumption.

In summary, rather than trying to replicate or find a "work around" for third-party cookies, it's critical for advertisers and publishers to gain maximum value from first-party data derived from direct to consumer touch points, as well as to diversify their activity beyond the proprietary platform. In doing so, they will realise the power they already wield to successfully reach, engage and measure interactions with their prospects and customers, wherever they are consuming content, and monetise their inventory on the open internet in this next evolution of advertising.

Section 4. The Impact on Measurement and Ad Verification

As an industry, technologies and advertising capabilities are constantly changing, and have been since online advertising formats were first created in 1994. Whilst the depletion of cookies is the latest significant change in the industry, ad verification and measurement can certainly adapt to a cookie-depleted world and has already started to.

4.1 Ad Verification

Most ad verification does not need to rely on cookies to detect fraud, deliver brand safety or measure viewability. Verification solutions will therefore be able to continue as before. Our recommendation would be to check with your trusted verification providers and ask them to confirm if their solution is reliant on third-party cookies. This will enable you to understand if their product suite is future proofed.

4.2 Measurement

The key change for measurement practices is that we can no longer rely on third-party cookies to identify exposure to advertising online. It is important to note however that third-party cookies will not entirely disappear in the next 12 months, so in some cases a mix of cookie data and other sources may be possible.

In this new world, several measurement approaches will be available to understand the impact of digital advertising investment, including:

1. Partnerships can be formed with publishers, networks and measurement companies to match passive exposure and respondent data. These integrations may allow for true cross-publisher, and cross-device measurement going forward.

2. Specific media consumption questions can still be used to model probability of exposure where passive exposure tracking is not possible. In some cases, and for some markets, this may be the most appropriate methodology to isolate campaign impact. Probabilistic exposure approaches will increasingly be blended with passive exposure approaches. Also, validations versus passive approaches will be used to further refine and improve the accuracy of probabilistic predictions.

3. Controlled exposure (online or in-person) lab approaches are increasingly being used to compare the effectiveness of content across multiple different media contexts. This approach is also being used to measure content, which has always been tricky to measure with cookies (e.g. influencer content or sponsorships).

4. Advanced analytics is currently being used, and can continue to be used, to model campaign impact based on various datasets (such as survey, sales, and media spend/delivery data), to understand total return on investment. Likewise, there is an untapped opportunity in measuring attention signals, one of the most effective ways to understand audience engagement and the true impact of campaigns.

5. Advertisers may use more experimental designs such as A/B split market testing to isolate impact (e.g. designing media plans with dark regions to enable simple measurement).

6. Working with publishers who can identify the exposure of their users on their platforms, and deliver surveys within their live environments ("polling"), will still be possible for single site analysis.

7. Other more custom approaches can be developed with purpose-built passive exposure tracking panels (e.g. using mobile metering), but volumes will remain low until management costs can be reduced

Which approach is most appropriate will depend on the activity an advertiser is looking to measure, feasibility of the different approaches in the market of measurement, the data sets and partnerships available in their market and to their brand, and the investment level available for measurement.

As the industry continues to change in the coming years other methods may also become possible.

Section 5. Overview of Current Non Third-Party Cookie Based Solutions

Advertisers will always need a means to connect with online users. They will need to reach people, both current and prospective customers, in relevant environments and engage them with content that resonates at scale. The digital advertising industry relies on this fundamental truth and it's unlikely to change as digital acquires more of the marketing budget. With that said, third-party cookies have been instrumental in advertising online for over 25 years.

The following section outlines some alternative approaches to the use of third-party cookies in digital advertising including:

- Identity-based solutions
- The use of other advertising data to make targeting decisions
- Contextual intelligence

We start by outlining the role of identity (cross-publisher identifiers) and the different identifiers used today.

5.1 Identity

The challenges of cross-publisher identifiers across the open web is existential for the industry, impacting the ability of brands to meaningfully reach audiences and publishers to fund the production of content.

For brands, cross-publisher identifiers impact both the efficiency and effectiveness of campaigns, allowing better frequency control, increased reach and more relevant messaging. This not only drives marketing effectiveness; it creates a better relationship with current and potential customers: more relevant messages and no annoying over-delivery of ads.

Publishers require identifiers to maximise the value of their ad inventory. A 2019 Google study showed that publisher ad revenue decreases by 52% when third-party cookies are not present in ad inventory. The implications of this are profound. People and society at large will not benefit from an ecosystem where publishers cannot properly fund their journalists, creatives, photographers, software engineers, and others involved in the production and delivery of content.

What are Advertising Identifiers?

Advertising identifiers, which come in a variety of formats, are a prerequisite to address a user for frequency capping or personalised/optimised advertising. Advertising identifiers can be either device or user-level, depending on the type identifier. Identifiers can have the following characteristics:

- **Persistent or Transient:**
  - Persistent identifiers exist across browsing sessions for enough time to effectively engage, frequency cap, and measure interaction, attribute conversions and optimise media spend.
  - Transient identifiers do not last long enough for the above use cases.

- **People-Based vs Technographic Identifier**
  - **Technographic Identifiers** include browser application (cookies), smartphones (Mobile Ad IDs), CTVs, or other web-enabled device identifiers.
  - **People-based identifiers** associate multiple web-enabled devices, including desktop, mobile and CTV to the same person.

- **Deterministic vs Probabilistic**
  - **Deterministic information** is explicitly declared by the person providing it.
  - **Probabilistic information** is an inference or guess about what information to associate to an identifier.

- **Directly-Identifiable vs Pseudonymous**
    - **Directly-identifiable information** can be used to pinpoint a distinct, natural person (such as home address, phone number or email).
    - **Pseudonymous information** means there are appropriate technical and operational processes within the organisation using the identifier to keep this identifier separate from an individual's identity.

- **Dynamic:** a single-use unique identifier, dynamically created for each transaction, containing no PII.

It is important to note that user addressability in digital advertising does not aim to identify an individual person with name, address or phone number but rather generate a persistent pseudonym to engage and optimise against when buying media or delivering ads.

Identifiers can be grouped into three different types:

- **Pseudonymous Universally Unique Identifier (UUID)**
    - Third-party cookies
    - Mobile Ad ID (MAID)
        - IDFA – iOS
        - AAID/GAID – Android

- **Pseudonymous, people-based deterministic identifier**
    - Based on user authentication (hashed email) plus first-party cookies
    - Often called 1P IDs, Common IDs, Stable IDs, Universal IDs, among other terms

- **Pseudonymous probabilistic identifier**
    - Based on statistical methods (=probabilistic)
    - Requires big scale of data to work properly – as more data touch points per user/person

The pseudonymous UUID

This class of identifier is most easily illustrated by a first-party cookie. The identifier is pseudonymous when it is not tied to an authentication event or PII. Many of these identifiers exist per-site as unique identifiers written to the page by the publisher or publisher systems, typically stored within a publisher first-party cookie and/or browser local storage under HTML5. Publishers enable the opt-out, persistence duration, and all other control mechanisms. If a user clears their browser cache or cookies these IDs are also removed.

You might wonder how this identifier can be unique even if not centrally managed or combined with PII. In fact, the total number of randomly generated UUIDs is so large that the probability of generating two identical UUIDs is very small.

Pseudonymous Deterministic Authenticated Identifier

This type of identifier uses an authentication event (usually an email address being entered into some form on a website) as the basis for the creation of the ID, hence "authenticated". Device associations for this type of identifier are based on personally identifiable information (PII) that has been encrypted, often through a process double of "hashing" and "salting." Hashing refers to changing an email to a random string of characters. Salting is adding additional characters to that string. Because these IDs are based on user-authentication across multiple sites and devices, the linking is deterministic, and because the resulting identifier is not directly related to the input value, they are also considered pseudonymous. Very importantly, these devices are user-level, offering omnichannel reach extension and frequency capping, typically to desktop and mobile devices, and increasingly to CTV.

With the deprecation of third-party cookies, this type of identifier, whether they are based on a login ID, email or phone number could potentially help solve the loss of third-party cookies and MAIDs in a multi-device, web, and app environments. Some of the most referenced identifiers in this category are ATS-based IDLs from LiveRamp and the forthcoming TradeDesk-sponsored Unified ID 2.0.

Pseudonymous Probabilistic Identifier

Some use cases, such as fraud detection, rely on pseudonymous identifiers generated via algorithms. These algorithms use passive identification signals such as IP addresses and the device's user agent string that are shared via the HTTP Protocol to infer the uniqueness of a user across websites. The process enables brands to access inventory and audiences across the open web, and measure and reduce the amount of their budget wasted on fraud.

This is commonly referred to as generating a statistical identifier. A legal basis under GDPR is required for this identification method, as well as user's consent under the ePrivacy directive when the algorithms use data actively retrieved from the user's device (such as available fonts and screen size).

5.2 Identity Solutions

5.2.1 CRM Data

Many advertisers and agencies have reverted to what they know best – the world of CRM – and of the "known" consumer. Although not without its challenges, CRM and email have seen a renaissance in this new privacy-conscious environment and have become increasingly important in the programmatic and digital landscape.

For years, the proprietary platforms have relied on their ability to accurately match a brand's CRM file to their persistent cross-device identifiers, creating opportunities for tailored, personalised advertising campaigns that were simply not available on the open web. This gave them a unique advantage, as we know, allowing the proprietary platforms to swallow the lion's share of the digital advertising market. Yet, the majority of consumers' time (upwards of 56 percent) is spent on digital media outside of the proprietary platforms.

As detailed in section 2, browsers are cracking down on third-party cookies and the open web is starting to shift to an environment in which premium inventory is infused with first-party, people-based identifiers. These identifiers can allow brands to activate media against their CRM files, mimicking the marketing techniques that were previously exclusive to the proprietary platforms.

This is nothing short of a massive paradigm shift which could expand the reach of brands across premium environments and omnichannel ad formats. However, this technique on its own does not allow them to engage in prospecting use cases.

Why Work with CRM and Email

Many advertisers have built and nurtured their CRM database over the years and used this to support retention, upsell and nurture campaigns through marketing automation. However, using these types of data sets to support digital, social and search activity did not become a mainstay of the media plan until relatively recently, in the case of search and social, and remains a rarity in the case of digital display (outside of the US). The rise in popularity of CRM over the past few years is certainly understandable, whilst its significance as a source of consumer data and identity within digital advertising moving forwards is almost inevitable, with clear and distinct benefits being:

1. The email address is relatively persistent. Where the cookie half-life could be anywhere from 7-30 days, most people use the same email address for a number of years, or at least months. This means that data can be stored and accumulated over time without loss.

2. The email address as an identifier is platform agnostic, unlike a third-party cookie, which are domain and therefore platform specific. This makes it an essential ingredient in connecting the consumer journey, attributing media effectiveness, and agnostically distributing target segmentation to activation platforms without relying as heavily on ID syncing and mapping tables.

3. For the most part, since the introduction of the GDPR, advertisers as well as agencies and other entities across the ad tech supply chain have been cleaning up their consented data sets. CRM derived through website form submissions and similar authenticated user action, which generally required a higher watermark to be met with respects to positive affirmation of content, has become the gold standard for consented, approved to use, marketing data.

Working with CRM Data

Operationally, working with CRM data is not without its challenges. Although many enterprise CRM, Customer Data Platform, and marketing automation platforms have for a long-time supported the direct integration and activation of email addresses within certain platforms - namely Facebook, Instagram, and Google Ads - the use of email within digital and programmatic display has been, and continues to be intermediated by "onboarding" solutions. These are able to map and transpose email addresses to digital identifiers, historically third-party cookies and/or mobile advertising IDs (AID and IDFA). Unfortunately CRM data does not support many organisations, who do not have direct relationships with the majority of their customers (like CPG).

Onboarding solutions develop their own ID graphs, principally connecting email addresses to digital identifiers through relationships that they maintain with partners including telecommunications companies, digital publishers, ecommerce platforms, and email service providers. Using an identity graph provider, buyers can match their offline audience to online people-based identifiers, which are activated across the programmatic ecosystem using an identity framework. They can then transact on these audiences using a unique deal ID. When consumers within that audience visit a premium, eligible publisher — and, critically, consent to share their data — buyers are able to bid on those users in real time (via the DSP of their choice).

Marketers will need to ensure they have a common cross-publisher identifier to measure the effectiveness of this people based advertising to drive success metrics, like visiting the brand's web property. Given many brands do not require emails to access their website, this is why cross-publisher identifiers do not compete but enhance the value of people-based engagement.

As a result, brands are able to boost engagement by serving more relevant adverts to users, publishers boost revenue flow, and consumers are given access to ads they actually want to receive (if and when they 'opt-in' to receiving such adverts).

Data Clean Rooms & Google Ads Data Hub

With the deprecation of the third-party cookie and the move towards a more privacy-safe environment, we have seen the rise of data clean rooms. These are essentially safe spaces where insights gleaned from platforms such as Facebook and Google, are commingled with first-party data from marketers, for measurement, attribution, and targeting. Google Ads Data Hub is one of the larger privacy-centric data warehouse initiatives providing customised analysis, alongside user privacy and high data security. It allows marketers to store ad server impression logs, and to combine these with other Google data sets across its marketing suite, as well as advertiser first-party data. Regrettably, unlike other clean rooms, no data is shared at an ID-level for syndication to engagement platforms beyond Google's own demand side platform. Although the advertiser data can be shared using a variety of identities, the clear focus has been on CRM and email, and most early cases have concentrated around this identifier class.

Data clean rooms can operate independently from Facebook and Google. Some onboarding providers offer them as an extension of their offering, and can be used to run statistical modelling on first-party data alone and/or statistical modelling on enriched first-party data (first-party data + ID provider third-party graph).

Limitations

There are some set-backs working with CRM and email, and it is not a perfect ecosystem. Markedly:

1. Data Cleaning - Typically email addresses and CRM data will need to be cleaned, normalised, hashed, and sometimes pre-segmented, prior to distribution to the onboarding solution, which can require additional data sciences/engineering resources depending on the size and complexity of the data set.

2. Match Rates – On sending to the onboarder, hashed CRM will then match to a predefined identity before exporting to the media platform endpoint. In the US match rates can reach as high as 80-90%. However, in Europe, average match rates range from 40-60% but can be lower depending on the type, age, and integrity of the data.

3. Technology Fees – Most onboarding solutions in Europe only offer their services under a SaaS-based license fee, with fixed, recurring cost, and minimum contract periods, making investment in an onboarding solution a relatively large-scale procurement decision.

4. Attribution Measurement - Many marketers do not require people to enter emails to access their website content. Accordingly, logged out pseudonymous cross-publisher identifiers are also required to effectively measure view-through and multi-touch attribution.

Overall, transparency to consumers will be key. Users on both the advertiser and publisher side of the equation should always be informed that their emails are being used for "addressability" cross-site.

5.2.2 First-Party Telco Operator Data

Telco operators have had a trusted, billing, relationship with their customers since the advent of the mobile phone, due to the services they deliver. In the case of mobile devices, this is a one-to-one relationship.

Since March 2014, operators have provided a safe and secure way for third-party businesses to identify and authenticate users via the GSMA's Mobile Connect secure universal service. Industries including banking, financial services, payments, and eCommerce use this service as it enables authentication, authorisation and secure identity verification, swiftly, globally, and cost-effectively.

This approach is now extending to programmatic digital advertising.

In particular, mobile operators currently offer several identity solutions:

- **Federated Identity** - a means for a single set of identity credentials to be used across multiple websites, rather than registering and remembering multiple credentials.
- **Second-Factor Authentication** - a second level of authentication, typically served via SMS code, when attempting to access content, services or carry out online transactions.
- **Mobile Digital Signature** - a digital identity established by using the secure environment within the SIM for running cryptographic operations. A number of governments around the world recognise mobile digital signature methodologies to be secure enough that they are recognised, in law, the same as a handwritten signature.
- **Identity Attribute Brokerage** - the matching of certain attributes of their first-party customer data behind the operator firewall.

This application of telco data in digital advertising allows for the continued creation of verified audiences for digital content providers and publishers and deterministic audience targeting for advertisers.

The real-time nature of a telco network enables use of a Telco Verified User ID and a Dynamic ID for audience transactions at an individual per ad request level. The Dynamic ID is distributed in the bid request and exchanged for the audience response pre-bid. This creates a suite of solutions for the advertising ecosystem:

- A telco-verified user ID
- A dynamic ID for audience activation
- Advertiser-focused first-party data activation
- Publisher analytics and profiling

For publishers, the use of a telco-verified ID can help address the growing number of so-called 'ghost' users; those consumers who browse publisher sites and apps without logging in and becoming verified. This anonymised web audience is substantial, but by using telco data, a publisher can understand their user-base and recognise a user when they return to their site or app, irrespective of the device used. This enables the creation of uniform audience IDs, across both authenticated and non-authenticated site visits.

These profiles are created on a per-publisher basis and are not a uniform ID (UUID). Publishers use these profiles to run their site analytics and power their own user profiles. This means they are therefore able to safely activate their own first-party audience data.

The Dynamic ID also enables a publisher to enrich their inventory with further telco-derived audience characteristics, thereby increasing the relevance of the advertising and value of these ad impressions.

Leveraging telco-verified audience data allows advertisers to reach real audiences, in real-time and at scale using verified data, which has been collected and consented to at first-party data owner level. This, in turn, ensures the data and the process used is compliant with all relevant regulations.

Using telco data to provide a dynamic identifier enables an advertiser to target specific audiences, activate against those audiences with their preferred DSP, and carry out frequency capping, measurement and attribution, all in a privacy-compliant manner.

5.3 Overview of the ID landscape

In the spirit of true collaboration, publishers have been working together to develop common and shared practices to make their properties easier to transact upon by sharing inventory and audience segments. Some examples include The Ozone Project, Pangea Alliance and European Publishers Council in EMEA. They are getting involved in creating standards across multiple properties to solve identity challenges and more closely aligning for their respective markets. These are often referred to as ID Consortiums or Shared ID solutions. They rely on first-party cookies as opposed to third-party cookies, hence why they are becoming an attractive alternative to third-party cookie targeting.

On average, the number of third-party cookies on a publisher's site is vast and all those individual cookies need to be matched in order to target advertising to individuals. A shared ID combines user identity from across multiple websites to allow publishers to transact on one shared ID (per user).

Example of a Consortium - IAB Tech Lab Rearc

Given the impending changes to third-party cookies and other identifiers, IAB Tech Lab is heavily focused on Project Rearc. Project Rearc is a global call-to-action for stakeholders across the digital supply chain to re-think and re-architect digital marketing to support core industry use cases, while balancing consumer privacy and personalisation. IAB Tech Lab is orchestrating a collaborative process to educate member and non-member stakeholders, and to facilitate global input into the development of new technical standards and guidelines driving "privacy by default" addressable advertising and measurement, which include tech standards and guidelines for many of the "solution" areas addressed in this paper.

Working with Multiple ID Solutions and ID Consortiums

There is, of course, the question of how to work with multiple IDs and ID consortiums. Prebid.org, an organisation of ad tech industry leaders that works with the ad tech community to provide solutions and open source products to push innovation, features a User ID Module as a core part of the Prebid open source header bidding software suite. For publishers who have installed Prebid on their site, the User ID Module is an optional part of that software stack. The User ID Module is used to generate, store, and transmit standardised, or "universal", IDs within the bid stream. The Module is open to standardised ID vendors so that they may submit their own sub-modules for publishers to electively use.

The universal ID sub-modules currently available within the Prebid User ID Module include:

- BritePool (BPID)
- Criteo ID for Exchanges
- Fabrick ID
- Halo ID
- ID+
- ID5 Universal ID
- IdentityLink
- IDx
- IntentIQ ID
- LiveIntent ID (NonID)
- LiveRamp IdentityLink (IDL)
- Lotame Panorama ID
- Merkle ID
- netID
- Parrable ID
- PubCommon ID (SharedID)
- Pub Provided ID
- Quantcast ID
- Tapad ID
- Unified ID (The Trade Desk)
- Verizon Media ConnectID
- Zeotap ID+ solution

The most up to date Prebid list can be accessed here.

Consistent Cross-Publisher Identifier Generation

For any of the IDs above that publishers enable within their Prebid installation the User ID Module will then, at the publisher's discretion, generate the respective IDs and then store those values within a first-party cookie. Prebid is then subsequently able to make these IDs available within the bidstream.

Consistent Cross-Publisher Identifier Transport (or Regeneration)

Ensuring the same identifier is associated with the same browser is important for remembering privacy preferences, as well as for addressing marketer use cases. Thus in addition to generating the pseudonymous identifier, these solutions need to transport (or regenerate) the common identifier across various publishers. One approach of regenerating the common cross-publisher identifier is relying on user emails as described above.

Storage

While most or all of the above listed universal IDs would normally be written to the page as third-party cookies, the fact that Prebid has domain level access to the page means that it is able to set a first-party cookie within the publisher's domain. This first-party storage (or "envelope") method is fully within the publisher's control and then enables these standardised IDs to be transmitted within the bidstream to participating DSPs without the reliance on third-party cookies.

Individual companies are also building on this solution. Multiple ID support is built in to Prebid and OpenRTB. Publishers can support as many of the above mentioned ID modules as they want to natively via these standards.

5.4 How to Evaluate ID Providers

We expect an influx of new IDs through the course of 2021, and blurring of the lines between an Identifier and Identity Infrastructure, which is the publisher side technology that informs how an identifier associates devices and sites to users.

In order for brands, publishers, and platforms to better understand the capabilities of Common IDs, we recommend asking the following questions to identity providers.

SCALE
Availability and scale by country
Current SSP integrations by region / country
Timeline of future SSP integrations by region / country
DSP integrations
List of publishers integrated with first-party addressability solution
Monthly active addressable users seen in Safari / Firefox / Edge
PRIVACY
PII: Is creation of your ID dependent on users providing PII (email, phone number, address etc.)?
Consumer choice: Does your company tie consumer preferences (opt-in/opt-out) to your ID, or is recording of these preferences dependent on legacy identifiers (such as third-party cookies)?
Consumer choice: Please list the consent frameworks your ID solution is integrated or compatible with.
CAPABILITIES
Technical: Can you explain how the solution works technically or provide a flow diagram?
Is the ID user-level?
Third-party cookie solution: Does the ID provide addressability in cookie-restricted browsers?
Third-party cookie solution: How does the ID provide addressability in cookie restricted browsers? What is the step-by-step workflow for propagating the identifier? *(provide technical description or links to documentation)*
IDFA opt-in: Will the ID provide addressability in iOS apps when the user has not opted into IDFA?
IDFA opt-in: If yes, how is ID able to provide addressability in iOS apps? What is the step-by-step workflow for propagating the identifier? *(provide technical description or links to documentation)*
CTV: Is the ID present in CTV supply?
CTV: If yes, with what SSPs?
CTV: If yes, how is the ID able to associate CTV devices to users? What is the step-by-step workflow for propagating the identifier? *(provide technical description or links to documentation)*
BENEFITS
What is the ID's value proposition statement? (Provide links to sales decks, one-sheets, and other marketing collateral)
What are the primary benefits of the ID?
What are the differentiators of the ID compared to others in the marketplace?

5.5 Other Data Available to Make Targeting Decisions, e.g., Engagement, Exposure

The use of data solutions providing predictive data, from the impact of an ad's presentation to key dimensions of consumer engagement, is a key alternative to drive campaign performance. Analysing data points in combination with a consumer's engagement, in real-time, allows engagement optimisation via metrics such as share of screen, video presentation, audible etc.

The element of this data in real-time is advantageous in comparison to current tools which can be deemed as either fast but simplistic, or sophisticated but slow. Predictive data correlated with digital advertising will enable brands to have clarity and confidence in their digital investment, aligning with their business goals.

As digital ad spend increases, these measures can help advertisers maximise ROI and drive real business outcomes, pinpointing underperforming areas of an ad at the impression source and making it possible to predict the propensity of a campaign to perform.

5.6 Contextual Targeting

Contextual targeting is not new in principle. Indeed, it is a tried and tested approach for marketers - a similar approach has been used in print media for decades where specific publications or editorial will be paired with relevant advertising to reach the right consumers at the time they are in the right mindset to be receptive to your product/service. However, contextual targeting has evolved considerably in the age of Big Data and AI. The incorporation of advanced statistical methods, machine learning and semantic analysis has the potential to provide surgically precise content classification to target specific topics and even content sentiment. Combined with the ability to execute instantly through programmatic pipes means contextual targeting is more than 'back to 1998'.

This is particularly pertinent in a privacy-first era where 94% of consumers say online data privacy is very important or important to them when browsing online content.

Regulations around consumer privacy and security like GDPR restrict the use of personal data that advertisers can collect and use for targeting, optimisation and analysis. In this context, advertisers could use contextual targeting at scale as a substitute for cookie-based targeting, since contextual targeting uses information about the content of the page, not bid or impression data. Marketers can go beyond broad contextual categories, using detailed semantic concepts, to get an understanding of where users are in the buying cycle, while not requiring their personal data.

Contextual targeting is not analysing previous browsing behaviour or historical content favourability. This means it does not rely on cookies to effectively match content to people in a current mindset. Instead it is focused on a deeper understanding of the context of the page. In the most basic form this can be done by seeking keywords on a page to classify that particular page. More advanced approaches can analyse and assess the relationship between the words on the page to deliver a deeper contextualisation relevant for advertisers. This is known as 'ontology'. Another way of describing this approach is "mindset marketing," a consumer-centric strategy in which advertisers design campaigns to match the mindset of the customers viewing them, based on the placement and content around each ad.

In technical terms, ontology stands for the rigorous and exhaustive organisation of language that is hierarchical and contains all the concepts, entities and their relations. This provides the opportunity to go beyond keywords and, ultimately, results in a greater targeting accuracy for advertisers campaigns.

However, for contextual engagement to be most effective marketers require cross-publisher identifiers to measure what happens after the exposure and to properly attribute credit to those publishers. For example, targeting the same contextual topic on two publishers without the real-time feedback called out above, would not provide marketers the insight as to which is driving more valuable behaviour on the marketers own web property. This is why contextual targeting is a core part of effective user engagement that relies on cross-publisher identifiers. In essence, engaging the right audience in the right context.

When considering cookie-free contextual solutions, five top considerations for success are:

1. Are you using tactical terms to improve your campaign's reach and relevance?

When creating your campaign, take the time to strategically plan the right terms, which will allow you to reach audiences that are actually interested in your products and who care about your offerings. While keywords are a good start, it's critically important for brands to choose contextual solutions which encompass the entire page, meaning not the keywords in isolation.

For example, an outdoor clothing retailer could place its ads around related content tied to camping, hiking, home fitness, and other outdoor activities. It might also find, however, that its ads are highly effective in other contexts, such as nature documentaries, travel advice, barbeque recipes, yoga blogs, or dog training. By analysing how your best prospects frequent and engage with specific context topics, you can better focus your media dollars.

2. Are you making sure your brand is protected from harmful environments?

Approximately 52% of brands have dealt with brand suitability issues more than once, leading to challenges with consumer perception. As this infographic shows, 62% of consumers state that they will stop using brands that appear next to harmful environments. Misaligned content can be conveyed as a deliberate indication of brand values.

Nowadays, brands don't want to be associated with topics or discussions that will hurt their reputations and destroy their brand images—and that is where context comes into play. The risk of negative exposure is critical in any campaign. Not only can you set your campaign to avoid the common brand suitability topics, but it's also smart to think about nuances in certain creatives that could spark offense. For example, a minivan that is featured in an ad about a car wreck is not brand-suitable.

3. Are you building custom contextual segments that align with the unique subjectivity of your brand and specific campaign objectives?

There are many ways to think about what the "right" context means. Here are some tips to determine what fits your brand:

- Aligning with customer needs—for example, the content you produce should align with your target audience.
- Aligning with personas/lifestyles—meaning that your content should relate to personal hobbies and activities (traveling, foreign culture, food interests, etc.).
- Aligning with equity-building content that reinforces broader brand objectives. For example, if a brand is endorsed by a major celebrity, aligning its advertising with content about that individual.

4. Are you using a contextual partner to help you automate segments in real-time?

Utilising a contextual partner that can assist with obtaining custom keyword segments in real-time will allow you to capitalise on popular trends as they unfold and appear next to new, brand-safe content as it's published. Here are the best questions to ask a contextual partner to get the best results:

- What is the value of using both people-based audiences and contextual audiences, and how do I use them interchangeably?
- How effective is contextual targeting in finding actual buyers? Can you tell me how your contextual segments perform?
- Are your segments supportive of common / standard taxonomies?
- How quickly can you identify trending content, and at what scale?
- How quickly can you make custom segments available for use?
- Are you able to build contextual segments that offer reach and scale?
- How do you guarantee that my message will appear in the right environments?
- Do you offer a full-page or page-level analysis of keywords?
- What is your approach to sentiment, homonyms and multiple languages?
- In what platforms are your contextual segments available?

5. Are you optimising and getting creative with your campaign?

Use related content terms to enhance your campaign. Doing so will allow you to reach new audiences in relevant environments, sparking interest and aligning messaging. You can also get creative by using real-life events and situations as a way to spice up your campaign.

Oreo is a great example of utilising context with their "Dunk in the Dark" campaign, which mimicked the power outage during the 2013 Super Bowl. This showed the power of quick thinking, and an understanding of the atmosphere in order to deliver a powerful message.

Deciding what is appropriate or not for a brand can be very simple to understand yet challenging to achieve. Being able to successfully locate and reach your audience will determine the success of your advertising campaign. Including contextual targeting in your next campaign can ensure that you're targeting audiences with relevant content in safe environments.

Section 6. How Stakeholders Can Contribute to the Solutions

Many groups and individual stakeholders are currently working on policy and technical solutions that will support a sustainable and healthy digital advertising ecosystem in a world with diminished access to third-party cookies.

Groups currently tackling these issues include technical standards organisations, such as IAB Tech Lab, the W3C and Prebid.org, as well as industry trade groups, such as the IAB Europe. Individual stakeholders include companies that are working on their own proprietary identity and accountability solutions.

How companies choose to engage with these efforts and solutions likely varies based on company circumstance. However, we've outlined some details of these efforts and initiatives below to provide some context for helping determine your strategy in this area.

6.1 Standards Organisations and Industry Trade Group Initiatives

Prebid.org

Formed in 2017, Prebid.org is an independent organisation designed to ensure and promote fair, transparent, and efficient header bidding across the industry. As of December 2020, Prebid.org has over 80 member companies.

Prebid.org manages the open source projects Prebid.js, Prebid Mobile, Prebid Server, Prebid Video, Prebid Native, as well as the Publisher-led User Identity module SharedID. Prebid.org is open to all companies who are part of the programmatic ecosystem, from ad tech vendors to publishers and others. Prebid.org drives standardised, transparent technology for advertising that will make it easier for buyers and sellers to transact at scale in a fully programmatic ecosystem.

Prebid.org's Identity Product Management Committee, which is chaired by publishers, is responsible for charting Prebid.org's role in the future of identity and coordinating implementation efforts.

Led by this committee Prebid recently announced the release of SharedID, a free, independent, transparent, open-source identifier. SharedID combines both a first-and-third-party cookie footprint and is combined with the PubCommon identifier, formerly owned and operated by Epsilon. This consolidated identifier is now owned and operated by Prebid.org.

W3C

The World Wide Web Consortium (W3C) is an international community that develops open technical specifications and standards to ensure the long-term growth of the Web. W3C aims to develop these technical specifications in a way that drives consensus and earn the endorsement by the W3C community. This is the forum in which the Google Chrome team has looked to engage feedback from industry on standards outlined in their Privacy Sandbox proposal.

There are a number of ways in which you can participate in these efforts. W3C invites the public to participate in W3C via discussion lists, events, blogs, translations, and other means. Participation in W3C Community and Business Groups is open to all. Participation in W3C Working Groups (and other types) is open to W3C Members and other invited parties. W3C groups work with the public through specification reviews as well as contributions of use cases, tests, and implementation feedback.

More information on how to engage can be found here.

IAB Tech Lab – Project Rearc

With impending changes to third-party cookies and other identifiers, Project Rearc is a global call-to-action for stakeholders across the digital supply chain to re-think and re-architect digital marketing to support core industry use cases, while balancing consumer privacy and personalisation.

IAB Tech Lab is orchestrating a collaborative process to educate member and non-member stakeholders, and to facilitate global input into the development of new technical standards and guidelines driving "privacy by default" addressable advertising and measurement.

There are a number of ways for your teams to participate in the discussion globally – from business, policy, and technology perspectives.

Non Tech Lab members can participate in the Rearc Taskforce, which gathers input from a diverse set of global stakeholders.

More in depth working groups open to IAB Tech Lab members currently consist of:

- Accountability Working Group, which will develop a framework to ensure adherence to privacy-centric practices for addressability; and
- Addressability Working Group, which aims to define technical standards for privacy-centric use of identifiers going forward
- Global Privacy Working Group, which seeks to streamline technical privacy standards into a singular schema and set of tools which can adapt to regulatory and commercial market demands across channels

More information can be found on how to engage in these efforts can be found here.

IAB Europe – Post Third-Party Cookie Task Force

IAB Europe in partnership with IAB France launched a joint initiative 'The Post Third-Party Cookie Task Force' in the middle of 2020. The taskforce is helping to ensure strong European input into reflections being conducted within the W3C and IAB Tech Lab's "Project Rearc" on the evolution of digital advertising and potential new paradigms.

Taskforce Working Groups

The taskforce currently has three working groups as per the following:

- Accountability Working Group
- Addressability Working Group
- W3C Working Group

Interested in joining the Post Third-Party Taskforce? Participation in the taskforce is open to all IAB Europe, IAB France and other National IAB corporate members.

More information can be found on how to engage in these efforts can be found here.

6.2 Private solutions

A growing number of companies have developed and brought to market solutions that provide identification capabilities without relying on third-party cookies. Most of them have built ID modules that are available in Prebid to facilitate the adoption of their identifiers. Some of these companies offer identifiers that can be used by ad tech platforms and publishers and passed through in the advertising value chain. Others have built identifiers that can only be used internally with their partners and clients and cannot be considered universal by definition.

A clear commitment to data protection, transparency and control for users should be key to all identity solution providers.

Neutrality is another key differentiator. Some companies who actively operate in the advertising ecosystem (buy-side, sell-side or data solution platforms) provide identification solutions as a complementary service to their core business. On the other hand, there are ID providers who are solely focused on creating an identification infrastructure for the industry to operate. Lack of neutrality can affect the adoption of an identifier as some ad tech platforms might avoid using a competitor's identifier. Adoption rate is a crucial metric for Identity solutions: the more publishers and platforms that use an identifier, the more effective and performant it gets.

Full list of ID providers in Prebid today:

- Audigent HaloId
- Britepool
- Criteo
- ID5
- IntentIQ
- LiveIntent
- Liveramp
- Lotame Panorama
- Merkle
- NetId
- Neustar FabrickId
- Parrable
- Pubcommon (owned by Prebid now)
- Quantcast
- Retargetly IDx
- SharedId (owned by Prebid now)
- Trade Desk UnifiedId
- Verizon
- Zeotap ID+

The most up to date Prebid list can be accessed here.

Proprietary Solutions

Many individual companies are working on developing alternative proprietary technologies and standards for supporting digital advertising use cases in a world without third-party cookies, such as those outlined in section 5 above.

6.3 Ensuring Ongoing Success of the New Paradigm

Whatever policy standards and technical solutions those in the digital advertising industry choose to adopt in a world without third-party cookies, there will be a need to demonstrate to regulators that the new paradigm aligns with consumers' privacy rights, granted under laws such as the GDPR.

What these engagement efforts look like will vary by circumstance and jurisdiction, but companies should look to engage through their local IABs who often have strong connections with local regulators and a history of successful engagement. For example, in 2019 the IAB UK successfully led industry engagement with the UK Information Commissioner's Office in response to their publishing of a report into ad tech and real-time bidding. More information can be found here.

Section 7 - Summary

This updated guide illustrates that over the last year, the industry has come together to work on a series of new solutions to help ensure that the digital advertising industry continues to function beyond the third-party cookie. There is still no conclusion as to what solution will be universally adopted by all. As it currently stands, 2021 will be all about testing, learning and adapting. Learnings have to be shared and collaboration continued to deliver relevant content to consumers and support quality European media.

The industry has a unique opportunity to evolve and advance over the next 24 months, we encourage all stakeholders to explore how they can get involved with relevant industry groups to contribute to and develop solutions for the industry.

On a local level, many national IABs have set-up task forces to discuss and feedback on solutions being developed, so get in contact with your local IAB to find out how to get involved. On a European level, IAB Europe has a dedicated task force, which brings IAB Europe corporate and national IAB members together to review and provide feedback on industry proposals such as those being considered in the W3C, IAB Tech Lab's Project Rearc, and Google Chrome's Privacy Sandbox.

This edition of the guide reflects the knowledge and information that we know today. As with our ever evolving industry, there will be more developments and advancements over the next 12 months. As such, the Programmatic Trading Committee (PTC) will continue to update the guide and release new editions to keep all stakeholders informed and inspired.

Contributors

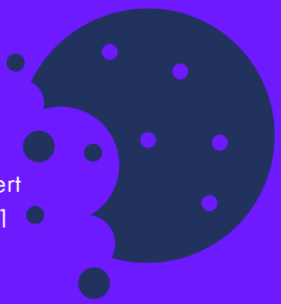
IAB Europe would like to thank the following contributors who helped to author this Guide.

adform	**Alex Berger, Senior Marketing Director, Buy-Side Products, Adform**
BBC GLOBAL NEWS LTD	**Emily Roberts, Programmatic Trading Manager EMEA, BBC Global News**
CNN	**Ben Hancock, Global Head of Programmatic Trading, CNN International**
DV | DoubleVerify	**David Goddard, Chair, IAB Europe Programmatic Trading Committee and Senior Director, Business Development, DoubleVerify**
IAS Integral Ad Science	**Akshay Bhattacharjee – Programmatic Solutions Specialist for the Nordics & CEE Region, IAS**
iab ireland	**Ian Maxwell, Converge Digital representing IAB Ireland**
iab france	**Thibault Montanier, Data Manager and Integration Specialist, Sirdata & Co-Chair of IAB Europe's Post Third-Party Cookie Taskforce**
iab TECH LAB	**Alex Cone, Senior Director, Product Management** **Jordan Mitchell, SVP, Head of Consumer Privacy, Identity and Data, IAB Tech Lab**
iab turkey	**Gokberk Ertunc, Programmatic Manager, OMD Turkey / IAB Turkey**

ID5	Valbona Gjini, Marketing Director, ID5
INDEX EXCHANGE	Sara Vincent, Senior Director, Strategic Partner Development, Index Exchange
LiveRamp	Zara Erismann, MD Publisher Europe, LiveRamp
Magnite	Garrett McGrath, Vice President, Product Management, Magnite
MediaMath	William Lee, Mgr, Product Policy & Comp, Chris Keenan, Regional VP, Business Development and Jamie Penkethman, Sr Director, Product Marketing.
novatiq	Tanya Field, Co-Founder & Chief Product Officer, Novatiq
OMD	Miles Pritchard, Managing Director - Data Management Solutions, OMD
ORACLE Data Cloud	Carlotta Zorzi, Global Brand Partnerships, Oracle Data Cloud
outbrain	Laine Rosa, Product Manager, Outbrain
PubMatic	Maria Shcheglakova, Marketing Director EMEA, PubMatic
united internet media	Alwin Viereck, Head of Programmatic, Ad Technology & Product, United Internet Media
xandr	Gabrielle Le Toux , Senior Marketing Manager, Xandr
YIELDBIRD	Szymon Pruszyński, Head of Growth, Yieldbird
zeta	Joshua Koran, Head of Innovation Labs, Zeta Global
ZEOTAP	Livia Busseni, VP Global Solutions Engineering Zeotap

Lauren Wakefield
Marketing & Industry Programmes Director
wakefield@iabeurope.eu

Helen Mussard
Chief Marketing Officer
mussard@iabeurope.eu



iab europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium

@iabeurope

/iab-europe

iabeurope.eu

iab europe