

May 2020

A GUIDE TO THE POST THIRD-PARTY COOKIE ERA

Contents

<u>Introduction</u>	2
<u>Section 1 - Background Information</u>	3
<u>Section 2 - The Three Contributing Factors to the Depletion of the Third-Party Cookie</u>	6
<u>2.1 The Legal Environment related to Consent and Tracking</u>	6
<u>2.2 Browser Gatekeeping</u>	7
<u>2.3 Ad Blocking</u>	11
<u>Section 3 - The Impact on Stakeholder usage of Proprietary Platforms</u>	12
<u>3.1 Proprietary Platforms and Advertisers</u>	12
<u>3.2 Proprietary Platforms and Publishers</u>	13
<u>3.3 Proprietary Platforms and Consumers</u>	13
<u>Section 4 - The Impact on Ad Verification and Measurement</u>	14
<u>4.1 Ad Verification</u>	14
<u>4.2 Measurement</u>	14
<u>Section 5 - Overview of current Third-Party Post-Cookie solutions</u>	16
<u>5.1 Identity</u>	16
<u>5.2 Identity Solutions</u>	17
<u>5.3 Other Data Available to Make Targeting Decisions, e.g. engagement, exposure</u>	22
<u>5.4 Contextual Intelligence</u>	23
<u>Section 6 - How to Contribute to the Solutions</u>	26
<u>6.1 Independent Industry Solutions</u>	26
<u>6.2 Private Solutions</u>	27
<u>6.3 Browser Initiatives</u>	27
<u>6.4 Regulatory Solutions</u>	28
<u>Section 7 - Summary</u>	29
<u>Contributors</u>	30

Introduction

This Guide has been developed by experts from IAB Europe's Programmatic Trading Committee (PTC). It provides background to the current use of cookies in digital advertising today and an overview of the alternative solutions being developed. As solutions evolve, the PTC will be updating this Guide on a regular basis to provide the latest information and guidance on market alternatives to third-party cookies.

The Guide will also provide answers to the following questions:

- What factors have contributed to the depletion of the third-party cookie?
- 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?

Key questions for each organisation to consider in preparation for a post-third-party cookie advertising ecosystem include:

- How does my company currently use third-party cookies?
- What alternative solutions may be suitable for my business?
- How can my company get involved in contributing to developing an industry wide solution?

Section 1 - Background Information

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 65% of the remaining browser usage, it is expected that this change will essentially end the use of third-party cookies. As the headlines are suggesting 'the cookie has crumbled'.

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**. They are used for cross-site tracking, retargeting and ad-serving.

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 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 must be 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. We expand on MAIDs in section 3.

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

- Frequency capping is largely based on third-party cookies so this feature will no longer be available in its current form.
- Third-party data currently being used for audience targeting will become unusable.
- Retargeting and most forms of dynamic creative targeting will become unworkable
- DMPs (data management platforms) cannot create identity linkages in the same way they do today.
- Last 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 and targeting 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, httponly, 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 it.

Advertiser Example

Even if an advertiser writes a retargeting cookie on his own www.advertiser.eu domain as a first party, this information cannot be accessed later on during ad delivery on publisher website e.g. mail.com in order to deliver a personalised product ad, since from mail.com 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.

Targeting Data

In case an identifier to associate with exists, user-centric data can be highly beneficial to each campaign KPI. Targeting data 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 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.

Agencies will mostly take care of the conceptual workload both for creating technology plans for advertisers and ensure planning and buying continue in an audience activation manner. It is important for **advertisers** 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 targeted 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 targeting.



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 key developments in digital advertising over the last two years which have contributed to the decision to deplete the third-party cookie:

1. The legal environment related to consent and tracking
2. Browser gatekeeping
3. Ad blocking

2.1 The Legal Environment related to Consent and Tracking

Individuals have a fundamental right to data privacy, and a right to know how their data is used and shared. They have the right to determine if their data can or cannot be used for advertising. On the other hand, publishers need to be able to finance content services and journalists, especially when advertising typically accounts for a large proportion of their revenue.

There is no singular overarching law regulating online privacy worldwide. Instead, a patchwork of regional, federal and state laws apply in various jurisdictions. In the second half of the 20th century, a number of countries, in Europe in particular, took the lead working on early laws and regulations aimed at controlling the use of personal information. In 1995, the European Union (EU) Data Protection Directive (Directive 95/46/EC) was adopted. The following section focuses on existing laws that currently impact cookies, consent, and tracking across the internet; but it should be emphasised that the legal landscape is continuously evolving on this topic.

EU's ePrivacy Directive

The ePrivacy Directive (Directive 2002/58/EC) requires consent for the non-essential storing of information or accessing of information stored on end-user devices, irrespective of whether such information can be considered personal data.

As a result of the implementation of the ePrivacy Directive, obtaining consent for the collection of personal data through cookies for the purpose of online advertising and analytics has – in many EU Member States – centred around the idea “consent banners”, a banner placed at the top or bottom of the page containing disclosures with a consent request. Importantly, with the entry into force of the GDPR, the notion of consent in the context of the ePrivacy Directive evolved to match the stricter requirements for valid consent adopted under the GDPR. For cookies to be stored and accessed in compliance with this reinforced definition, consent must be prior, freely given, specific, informed, withdrawable and unambiguous.

In 2017, a proposal for the new ePrivacy Regulation was published, to ensure further harmonisation of the rules. While it remains unclear when it will exactly be adopted, one can expect it in the coming years.

EU's General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was adopted in 2016 and came into force in the EU on 25 May 2018. GDPR works in parallel with the ePrivacy directive and takes user privacy online even further. GDPR regulates the processing of personal data. It applies to companies based in the EU but also to companies all over the globe offering goods and services to people based in the territory of the EU, or monitor the behaviour of individuals located within it. It's important to note that online identifiers, such as cookies, and device identifiers, are examples of personal data under the GDPR. Moreover, online advertising is explicitly called out in the law. Therefore, the GDPR unambiguously establishes the principles of data protection in the digital advertising context.

The requirements to disclose and gather consent for third parties brought about by the EU's updated privacy rules have led to the adoption of tools such as IAB Europe's Transparency and Consent Framework, which is an open-source, cross-industry standard created to facilitate GDPR and ePrivacy Directive legal compliance. It standardises how websites make the information disclosures required by the GDPR, how the sites collect and log users' choices, how they communicate those choices to their third-party technology partners, and what those partners may and may not do as a consequence.

California Consumer Privacy Act (CCPA)

The CCPA was introduced as a State Law in California which came into effect on 1 January 2020, and gives users the right to access, delete or opt-out of personal data sharing with third parties at any time. It also considers some cookies to be personal data. California is the first state in the United States to pass such a law. However, there are around a dozen other individual state laws currently in various stages of review and legislation. A federal law seems unlikely in the near future.

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

1. Users are more aware than ever of the rights in regard to personal data and the online business model which is underpinned by their data being processed, used, and shared.
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.
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.

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, companies are proactively offering increased privacy protections, as a competitive advantage.

[Market shares of browsers in Europe](#) leave little room for interpretation. Chrome (62%) is the by far 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, where the regional shares equal the EU wide ones.

Change in gate keeping behaviour of the three given browsers are therefore the most impactful to the market.

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

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 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.

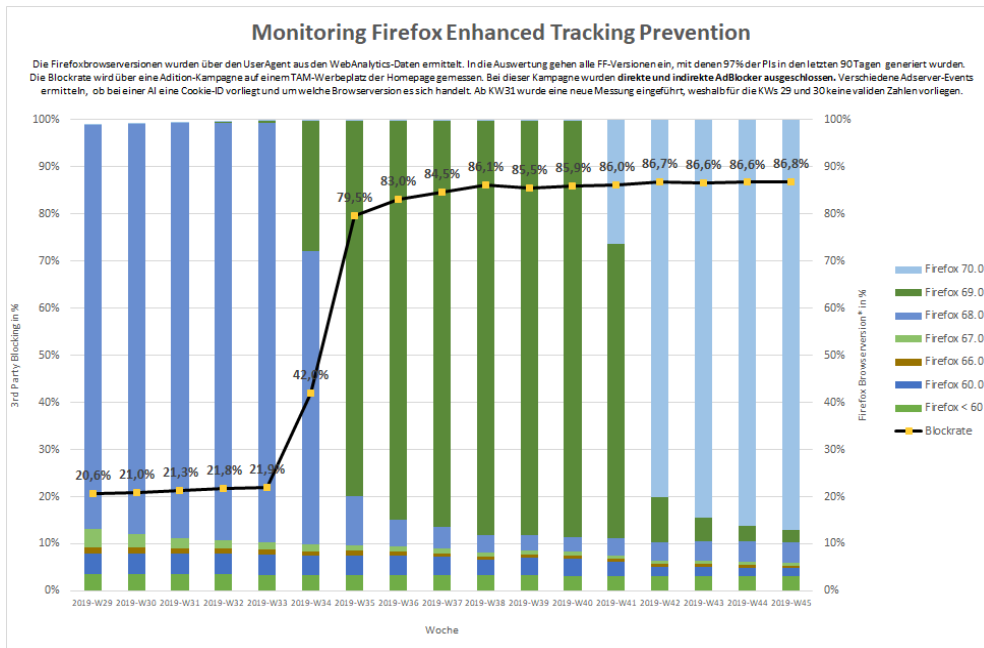
Mozilla describes the feature as the following: Simplified content blocking settings give users standard, strict, and custom options to control online trackers. A redesigned content blocking section in the site information panel (viewed by expanding the small "i" icon in the address bar) shows what [Firefox 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 3P tracking cookies, but allow the calls.

Third-party cookie blocking rate measured for Mozilla Firefox in 2019



Safari (Apple)

Amongst all browsers, Safari has the longest history with these types of privacy 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 bad 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.

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 labeling 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 labeled with “SameSite=None” and “Secure”, making it mandatory to ensure those cookies are read via HTTPs.

In January, [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, together with other stakeholders in an industry-wide effort, is providing for the digital advertising industry to take, relying on anonymised signals (that are not cookies) and five application programming interfaces. 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).

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. The best 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 worldwide 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 (use 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 most prominent example is Safari’s “Intelligent Tracking Prevention” (ITP).

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 at scale 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 will be able to offer targeting based on a substantial amount of first-party data. However, in return for accessing the wealth of data, Proprietary platforms may impose restrictions in control and transparency to buyers.

Our industry shouldn't think about "solving" for the loss of third-party cookies or countering the dominance of Proprietary platforms. These technical changes are primarily happening for the benefit of consumers and to reflect the direction of privacy laws globally.

3.1 Proprietary Platforms and Advertisers

However, 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:

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, view 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: 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 these platforms. In addition, it hampers the ability for buyers to use 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 who may be keen to minimise their reliance on the proprietary platforms. In fully aligning with these platforms that control the vast majority of advertising spend, publishers may find themselves at the whims of policies and product decisions that may restrict their independence and innovation. The loss of third-party cookies may add another challenge to their monetisation.

One way publishers can offset the impact of the loss of third-party cookies is by establishing more first-party data through subscriptions or logged in users. But some publishers are running into obstacles with this effort and others are not able to enact such a strategy. According to a [Digiday Research survey](#), 63% of publishers are facing challenges converting audiences to a paid subscription product.

The option of an ad-supported business model is important to nearly all publishers, even those who successfully offer ad-free subscriptions. A hybrid approach of healthy advertising flows from both the open internet and the proprietary platforms will keep publishers in good financial shape to focus on their core business - creating premium and trusted content that will keep consumer's happy and deliver engaged audiences to advertisers.

3.3 Proprietary Platforms and Consumers

Without the choice of an open internet, consumers will have to increasingly pay to consume premium content. 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.

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 platforms. In doing so, they will realise the power they already wield to successfully reach their 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 Ad Verification and Measurement

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

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. Opportunity to see, or 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

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 Third-Party Post-Cookie 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. 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 solutions
- The use of other advertising data to make targeting decisions
- Contextual intelligence

We start by outlining the role of identity and the different identifiers used today.

5.1 Identity

The challenges of identity across the open web are too big an issue for one side of the industry, let alone one company, to solve. It is something everyone needs to come together on to build the right solution.

Most will say this is a publisher issue, as their revenues fell and ad dollars flowed to the proprietary platforms where users were known. However, identity severely affects advertisers as well because campaigns—specifically their efficiency—suffer when marketers can't target their desired audiences and are forced to turn to more competitive environments.

What are Advertising Identifiers?

Advertising identifiers, which come in a variety of formats are a key prerequisite to address a user for frequency capping or personalised/targeted advertising, since all user-centric data is associated with it. They aim to be a reliable holistic representation of a user and their digital touchpoints:

- Reliable = persistent
- Holistic = multi-device reality
- Representation = addressable (pseudonym)
- Inventory spanning

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 target and optimise against when buying media or delivering ads.

Identifiers can be grouped into three different types:

1. Anonymous Universally Unique Identifier (UUID) - Operating System (e.g. IDFA, AAID)
2. Pseudonymous deterministic identifier - Login (e.g. account/mail based)
3. Pseudonymous probabilistic identifier

The Anonymous UUID

The UUID is the oldest type of identifier and can be considered anonymous, since typically it is based on a timestamp only and not directly related to any personal identifiable information (PII).

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.

Many of the programmatic advertising vendors such as SSPs, DSPs or ad servers have used UUID in their third-party cookies.

Pseudonymous Deterministic Identifier

The second type of identifier is considered pseudonymous since it uses personal identifiable or related information, even if that information was “hashed”. Furthermore it is deterministic, since the PII is typically a login id or email address, which can always be used to reproduce the ID.

These kinds of identifiers, whether they are based on a login id, email or phone number are very likely to replace the given anonymous UUID in a multi-device, cookieless, web and app environment.

Pseudonymous Probabilistic Identifier

The probabilistic identifier uses a wide range of (data) signals on a device such as operating system version, browser version, fonts installed, plugins, ISP, connection type, user agent strings or others to statistically predict a unique user. There is always the risk of false positives or negatives.

The advantages of these kinds of identifiers are their independence of browser storage and potential multi-device ability. Nevertheless, browsers can restrict the ability of advertising to execute methods also referred to as “fingerprinting” by limiting the data points being exposed to scripts which perform probabilistic identification.

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 the 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 those 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.

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 set 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, which are able to map and transpose email addresses to digital identifiers, historically third-party cookies and/or mobile advertising IDs (AID and IDFA).

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).

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). Collectively, these efforts allow independent and premium buyers and sellers to compete with the proprietary platforms at scale, levelling the industry playing field.

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, which are essentially safe spaces where insights gleaned from the platforms such as Facebook and Google, are commingled with first-party data, from advertisers 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, allowing advertisers 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. No data is shared at an ID-level, and analysis is usually done at a level of aggregation in order to mitigate privacy concerns. 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.

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 export 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.

5.2.2 Mobile Advertising IDs (MAIDs)

It is unsurprising that in today's complex and privacy-first advertising ecosystem, cookies are no longer deemed fit for purpose. Much of the critique points to their lack of ability to deliver value to mobile activity - the app. With mobile ad spend in the UK alone now accounting for 80% of all programmatic digital display ad spend (source: eMarketer) and with that figure only set to rise, it is clear that using alternative solutions at scale is already long overdue.

Enter the MAID - the Mobile Advertising ID. Unlike cookies, a MAID is an identifier that is provided by the mobile device's operating system and is transparently designed with advertising in mind. This means that as a solution, MAIDs offer a reliable, pseudonymous, stable and safe identifier of mobile activity and a more permanent way to meet compliance with privacy legislation and protect consumer privacy.

As the cookie is phased out, publishers and brands will increasingly look to MAIDs as a means to craft a more complete picture of their customers and measure the results of digital campaigns. What was once dubbed 'the real world cookie' will gain cadence as brands realise new opportunities in location data. Brands are already using location data-driven products to better understand their audiences, personalise the messages delivered to them based on their interests, and measure in-store visitation results, and we expect to see more marketers turn to location as part of a holistic strategy.

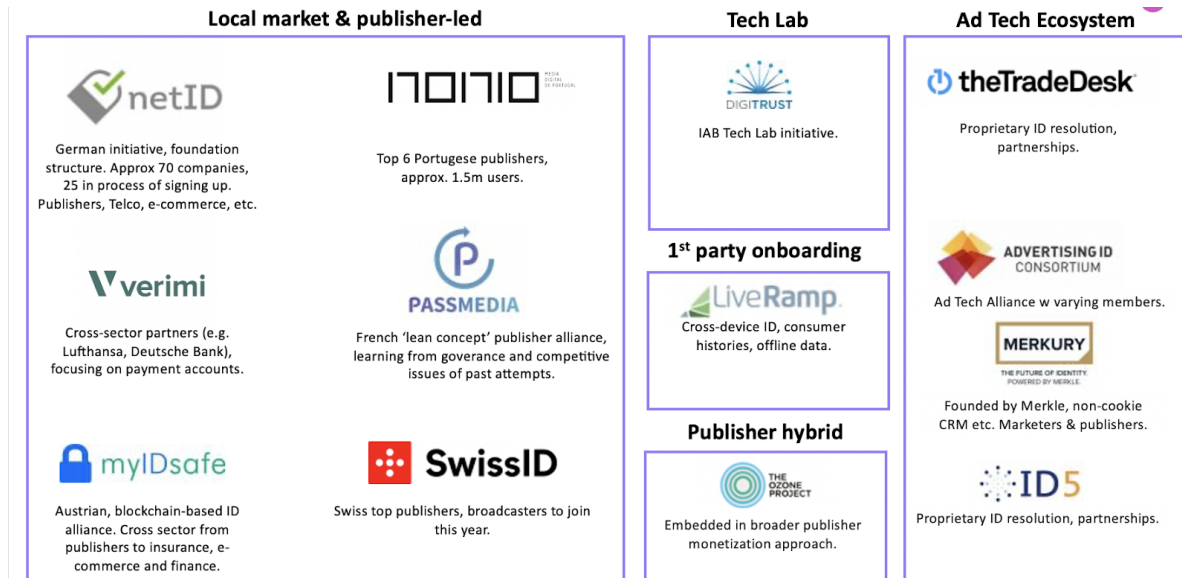
5.2.3 Overview of the ID Landscape

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 and Pangea Alliance 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).

There are many ID solutions being developed, some of those are included in the graphic below.

Overview map created in March 2020



Example of a Consortium - IAB Tech Lab DigiTrust / Rarc

DigiTrust is a standardised ID and neutral namespace service operated by IAB Tech Lab on a shared-cost, shared-benefit basis. DigiTrust was founded by ad tech platforms and premium publishers collaborating to deploy and support a standardised cookie-based user token in order to reduce the need for ID syncing and improve match rates across proprietary third-party cookies, while at the same time improving publisher revenues, advertiser reach and consumer experience. DigiTrust, like most cookie-based solutions, is negatively impacted by the deprecation of third-party cookies.

Given the impending changes to third-party cookies and other identifiers, IAB Tech Lab is entirely focused on Project Rarc. Project Rarc 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.

Working with Multiple ID Solutions and ID Consortia

There is, of course, the question of how to work with multiple IDs and ID consortia. 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 are:

- BritePool
- Criteo ID for Exchanges
- DigiTrust (IAB)
- ID5 Universal ID
- LiveIntent ID
- Parrable ID
- PubCommon ID
- Unified ID (The Trade Desk)
- LiveRamp IdentityLink

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.

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. For example the PubMatic Identity Hub is a software management layer built on top of Prebid’s User ID module that allows publishers to support multiple IDs for each ad impression, thereby ensuring that buyers can recognise the publisher’s audience and bid more on its inventory, maximising publisher revenue and buyer campaign performance.

5.3 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 targeting 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.

5.4 Contextual Intelligence

Contextual intelligence or 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 create insights at scale. Combined with the ability to execute on these insights instantly through programmatic pipes means contextual targeting is more than 'back to 1998'.

This is particularly pertinent in a privacy-first era. 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. 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 for 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.

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 your keyword list. Leveraging the right terms 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 & expand to relevant adjacent content also.

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.

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. Misaligning 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 context partner to help you automate the segments in real-time?

Utilising a context partner can assist with obtaining custom keyword segments in real-time. This 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 context 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?
- How quickly can you identify trending content, and at what scale?
- How quickly can you make custom segments available for use?
- 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?
- How do your contextual segments perform?

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 intelligence in your next campaign can ensure that you're targeting audiences with relevant content in safe environments.

Section 6 - How to Contribute to the Solutions

Contributing to shaping solutions differs widely from advertiser, publisher, technology vendor and from role to role in an organisation. The majority of solutions are open to public commentary and contribution. However, impact and influence of that input, as well as breadth of access varies widely. We've broken these down into four high level categories; regulatory solutions, independent industry solutions, private solutions, and browser initiatives.

With most digital advertising technology solutions, the primary barrier is browser dominance, market fragmentation and speed of adoption. The single biggest thing advertisers and publishers can do to contribute is vote with their feet by driving adoption.

It's also paramount that organisations interested in getting involved look both at industry-specific solutions and more industry universal solutions and organisations outside the immediate scope of the digital advertising space. In the same way high profile data breaches unrelated to digital advertising contributed to GDPR and concerns about privacy, other broad concerns about the behavior and performance of the web such as the open web vs. paywalls (etc.) may inform initiatives driven by groups like W3C or browser-based solutions.

6.1 Independent Industry Solutions

The most accessible and open to contribution, content, and formative participation are independent industry solutions. These initiatives, such as IAB Tech Lab's Project REARC are community and partner driven. With fewer concerns about being leveraged for special interests, and a central community-driven approach they provide the most dynamic and powerful opportunity to get involved. These solutions also tend to serve as a baseline and general conduit in both directions; both into regulatory solutions through the educational bodies and advocacy wing of the organisations putting forward the solution and through providing best practice and standards / frameworks (e.g. [The IAB Europe Transparency & Consent Framework](#)) or core ideation for further adoption and specialisation in derivative private solutions. Clearly defining and stating explicit needs, while contributing manpower or resources and external endorsement and adoption of these initiatives is essential in helping them succeed.

While structure varies from organisation to organisation, many follow a similar approach to the IAB Tech Lab in which members can participate in the creation of specifications and development of tools.

Typically, a public/external comment period is included free of charge or on an invite basis. With participation in final decision, potential development, and execution then shaped by workgroups driven by paid membership. These memberships can be price prohibitive for some organisations or individuals but also serve to accelerate development and facilitate investment commitment.

Primary examples of this are initiatives driven by groups like the IAB Tech Lab Project Rearc and associated working groups and task forces and W3C led Improving Advertising Business Group.

6.2 Private Solutions

Private solutions benefit from an ability to more rapidly and fluidly field potential solutions. They often give individual high-profile stakeholders more ability to shape development and policy. These are, however, also more risky as concerns over preferential data or code neutrality can limit adoption. Competition between parallel private solutions also risks adding complexity and technology layers. Contribution to private solutions comes in a wide range of forms with a mixture of non-profit and profit-based models being explored. In some limited cases code repositories are made available and then opened to comment through platforms like GitHub and raised issues can be paired with code contributions. Others are largely operated as commercial black box enterprises. While yet others are split between an internal (private) and external (public) fork. PreBid.js and its role in driving Header Bidding serves as a prime illustration of how this can work when managed well. However, risk of acquisition, competitive market concerns or loss of the primary sponsor makes these more challenging.

Primary examples of this are independent initiatives like ID5, BritePool, non-profit independent initiatives like European NetID and corporate sponsored initiatives such as LiveRamp, Live Intent, the 5th Cookie, Parrable and The Trade Desk's Unified ID.

6.3 Browser Initiatives

Browser initiatives mirror regulatory solutions in that they should be seen and approached from an industry perspective, and from a broader pan-industry, user privacy centric perspective. The ability to contribute and to shape the narrative is highly dependent on each of these. The most high impact point of involvement in shaping the future evolution of the web is done through the W3C and its related standards. These standards can be inherited by and adopted by the majority of browsers. The W3C accepts input through multiple channels including open discussion and more restrictive premium member based Working Groups (more information on participation is available [here](#)).

In addition to the W3C's high level guidance and approach to setting standards, the majority of browser based initiatives are confined to three primary code trees; Google, Firefox, and Safari. The ability to contribute is highly subjective and in some cases include an open source and private commercial offering such as Chromium/Chrome, (Chromium Google's Open Source Browser, Chrome and the Chrome Privacy Sandbox owned by Google, Safari owned by Apple, and Gecko Quantum from Mozilla which powers FireFox). While decisioning inside Apple and Google is done in a predominantly black-box fashion that excludes the ability to contribute, Chromium and the Privacy Sandbox are being developed in a fashion that more closely resembles independent industry initiatives and utilises a mixture of dedicated Chromium related input tools as well as the possibility of adding input directly on the code [via GitHub](#). Mozilla's Gecko also uses a hybrid approach with [community contribution](#) but lacks a tool similar to the Privacy Sandbox to facilitate tailored advertising.

Primary examples of this are the W3C Standards which informs browser approaches to privacy and cookie management across Chromium, Gecko Quantum, and Safari leading to eventual standards adoption by individual browsers.

6.4 Regulatory Solutions

More broadly limited to a narrow pool of experts from various fields, the ability to contribute to these on an individual organisational level is more limited. While informing and participating in discussions surrounding evolving best practices is important from all aspects of the industry, the typical advertiser, publisher or tech vendor will largely be limited to reactive commentary. A central theme through most of these regulatory initiatives and inspired solutions are driven by privacy considerations, including privacy-by-design principles. Here, the most impactful approach for the average organisation is to focus on targeted education, and driving a strong consumer-driven approach which focuses on a clear value exchange between consumer, brand, publisher and technology facilitator.

Primary examples of this are regulatory schemes such as data protection authorities like the ICO and regulation development such as GDPR, and the CCPA.

Section 7 - Summary

This Guide reveals the key contributing factors to the depletion of the third-party cookie; developments in the legal environment related to consent and tracking; browser gatekeeping and ad blocking. The industry is embracing this change and the Guide reveals the steps being taken to ensure digital advertising will continue to function beyond the third-party cookie.

It is clear this impacts all stakeholders in the ecosystem, whether you're dependent on cookies or not, from buyers through to publishers and needs the industry to work together to ensure digital advertising continues to deliver relevant content to consumers and support quality European media.

There are a number of solutions tabled and in development including:

- Making the most of your first-party data and identifying opportunities with logged in environments.
- Finding environments where your message will resonate with the right consumers at the right time, using contextual targeting solutions.
- Using other data points to drive your media decisions, by reducing wastage where your ads are shown to non-human, low interaction or brand unsafe environments.
- Exploring the huge volumes of users on cookieless platforms like in-app & tablet browsers - each of which have been somewhat neglected in a cookie world.
- Your brand and message is unique - drive your tech partner and publisher to really understand objectives and measure them in real-time.

There is no one size fits all and different businesses will need to evaluate the solutions that best fits their needs.

Get involved

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 will shortly be launching a new task force which will bring 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 Sandbox. The Task force will be led by IAB Europe Technical Director Patrick Verdon who represents IAB Europe in the W3C's Improving Web Advertising Business Group. Patrick and other IAB Europe colleagues will also input into the Project Rearc Taskforce and "Addressability" and "Accountability" Working Groups.

Find out more about joining IAB Europe [here](#).

Contributors

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



Alex Berger, Senior Marketing Director,
Buy-Side Products, Adform



Emily Roberts, Programmatic Trading
Manager EMEA, BBC Global News



Ben Hancock, Global Head of
Programmatic Trading, CNN International



Ian Maxwell, Converge Digital
representing IAB Ireland



David Goddard, Chair, IAB Europe
Programmatic Trading Committee and
Senior Director, Business Development,
DoubleVerify



Ross Webster, Managing Director, Europe,
Foursquare



Jordan Mitchell, SVP, Head of Consumer
Privacy, Identity and Data, IAB Tech Lab



Sara Vincent, Senior Director, Strategic
Partner Development, Index Exchange



Miles Pritchard, Managing Director - Data
Management Solutions, OMD



Gokberk Ertunc, Programmatic Manager,
OMD Turkey / IAB Turkey



Ben Geach, Senior Director, Global
Product Strategy, Oracle Data Cloud



Laine Rosa, Product Manager, Outbrain



Maria Shcheglakova, Marketing Director
EMEA, PubMatic



Garrett McGrath, Vice President, Product
Management, Rubicon Project



Alwin Viereck, Head of Programmatic & Ad
Technology, United Internet Media



Gabrielle Le Toux , Senior Marketing
Manager, Xandr



Kristanne Roberts, Global Development
Director, Insights Division, Kantar



Szymon Pruszyński, Head of Growth,
Yieldbird


Marie-Clare Puffett


Marketing & Business Programmes Manager
puffett@iabeurope.eu

Helen Mussard

Marketing & Industry Strategy Director
mussard@iabeurope.eu

iab europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium

 @iabeurope

 /iab-europe

iabeurope.eu

 iab europe