March 2022

# A GUIDE TO THE POST THIRD-PARTY COOKIE ERA

iabeurope.eu

iab.europe

# Table of Contents

## Table of Contents

# INTRODUCTION

In May 2020, IAB Europe released its initial '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 the IAB Europe 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 sought to keep the Guide up to date to provide the latest information and guidance on market alternatives to third-party cookies. The first update was issued in February 2021 and this latest update provides 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?

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 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 2019, Chrome announced a new initiative (Privacy Sandbox) “to develop a set of open standards to fundamentally enhance privacy on the web” by developing new digital advertising tools to protect people’s privacy and prevent covert tracking, while supporting a thriving ad-funded web. In January 2020 Chrome announced its plans to phase out support for third-party cookies in Chrome within the next two years. In June 2021 Chrome announced an update to the timeline and has made a public timeline available on privacysandbox.com. The new timeline means Chrome’s support for third-party cookies is expected to be phased out in 2023. Their announcement to phase out support for third-party cookies will change the way cross-publisher based advertising operates.

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 these third-party cookies are primarily used for cross-site tracking and retargeting, they can also be used to improve some ad serving capabilities with frequency capping, creative sequencing, and optimisation.

Given the match rate issues, many in the industry had been expecting the discontinuation of third-party cookies as a natural evolution of digital media, and one that has long been on the agenda. Eliminating third-party cookies 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 bring to how a campaign is served and delivered. It will in turn help to understand that alternative ways of reaching an audience can be achieved.

Firstly, web (desktop and mobile-enabled websites) and in-app should be separated. Cookies are a web-only technology. For in-app, ad identifiers such as IDFA, AAID, or MAIDs, which are provided by the operating system, are currently used for identification.

From an advertising perspective, there are a number of use cases outlined below that are currently supported by cross-site identifiers such as third-party cookies. Without cross-site identifiers, these use cases would not work the way they do today and will require new privacy-preserving technologies to support them in the future.

- Frequency capping, dependent on cross-publisher identifiers.
- Syndicating marketers' first-party data to a publisher.
- First-party publisher data for audience extension.
- Audience-based dynamic creative optimisation (DCO).
- DMPs (Data Management Platforms) identifier linkages.
- View-through or multi-touch attribution.

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 to persist data on the browser client system. In simple terms, web storage is a further development of cookies, allowing greater capacity for storage and more efficient developer APIs. However, 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 that can hold data, but it is not an identifier in 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 ad server.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 these alternative solutions 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, 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 objective is to control the media spend per user.

The absence of frequency capping can significantly decrease the user experience. The removal of third-party cookies dramatically deteriorates the ability of the buy-side to control that aspect of a campaign.

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

Digital Brand Marketing campaigns use socio-demographic (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. In particular, they 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 and collaboration between publishers, agencies, and advertisers will be critical.

**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 building new relationships with the buy-side. In addition to supply path optimisation, they will need to provide 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 govern 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 EU instrument primarily regulating the processing of personal data in the electronic communications sector, i.e. by telecommunications providers. The ePrivacy Directive (ePD) is essential to the digital advertising industry because of its rules on cookies. The ePrivacy Directive stipulates that member states must create rules that require website operators to inform the user concerned about the use of cookies and obtain their consent to use (most) cookies. In 2017, a proposal for a new ePrivacy Regulation to replace the Directive was published to ensure further harmonisation of the rules and direct applicability to EU citizens.

Following the ordinary legislative procedure, the European Parliament adopted its report on the ePrivacy Regulation back in October 2017. On 10 February 2021, The Council of EU signed off on its version of the ePrivacy regulation, marking the beginning of the negotiations with the EP during the Portuguese presidency. The agreement constituted a significant milestone towards getting an updated regulation in place and trilogues to come in 2022.

Whereas, the current form proposed Regulation does no longer include the text that would mandate browsers and other software providers to provide the option to prevent data collection through cookies et al. actively and to force users to choose as to their privacy preferences during installation. The absence of this provision (Article 10) could still be obfuscated by similar language in the Council text, which in practice reinstates the removed Article 10 provision.

The proposal has also been an opportunity for the European Parliament to include consent as a condition for accessing a service. The European Council adopted a very opposite position by recognising the rights for '*services provided in accordance with the freedom of expression and information including for journalistic purposes*'. The European Parliament's position underscores the importance of so-called *conditionality* for the continued sustainability of online media businesses.

## Digital Services Act (DSA)

The EU's Digital Services Act has been promised as a landmark piece of legislation to strengthen the single market and protect citizens and their rights. But since the European Commission first proposed it in December 2020, the legislation has been debated and discussed, and some policymakers intend to vastly expand its scope and change the way we operate online.

In January 2022, the European Parliament (EP) adopted its position that includes provisions with several changes to the Commission proposal, including further obligations to consent and access to services, that will take away the right of publishers to independently hold a dialogue with the user, asking them for consent in case a software privacy setting is set. The adopted text includes as well a ban on targeted advertising to minors and the use of special categories of personal data. Some of these provisions give cause of concern and raise fundamental questions about the implementation and functioning of the ad-tech ecosystem as it is today.

As of the Council, its agreed position on the proposal for the DSA is closer to the European Commission's text but amends its scope, including search engines, rising protection on minors and adding obligations to market places, search engines and very large online platforms.

Having the European Parliament's text been adopted, trilogues negotiations have begun to reach a compromise text with the objective to reach a provisional agreement under the French Presidency. The question is, how will the final text look after the Interinstitutional negotiations?

## Digital Markets Act (DMA)

The Digital Markets Act proposed by the European Commission in December 2020 at the same time as the DSA. The DMA has the purpose of ensuring the well-functioning of the internal market by promoting effective competition in digital markets with a fair and contestable online platform environment.

In December 2021, the European Parliament approved a plenary vote on the Internal Market and Consumer Protection's (IMCO) DMA report, adopting its position on the DMA.

The text approved by the EP expands the DMA scope by including more key digital services to the regulation - i.e. web browsers, voice assistants, and connected TVs. The text also includes a ban on the so-called "*dark patterns*". The current adopted text narrows the scope in terms of which size and type of business this regulation covers. Now the text will leave out of scope the vast majority of companies that are not giant tech companies.

The Council agreed its position back in November 2021 with a text similar to the original text proposed by the European Commission in December 2020 and introducing further obligations to core platforms services that will allow users to unsubscribe from them. The process of reaching a compromise text started in January 2022 with the trilogue negotiations with the same objective as the DSA of reaching a provisional agreement under the French Presidency.

**Ongoing regulatory body investigations (CMA, ICO, DG COMP)**

The industry can expect some new developments in the investigations from CMA, ICO, and DG COMP. The outcome of those investigations might impact the implementation phase or timeline of deprecation of third-party cookies on the Chrome browser**.**

The United Kingdom's Competition and Markets Authority has been investigating emerging Google proposals for almost a year now. In May, it published the initial commitments that the company promised to follow in the further development of the Privacy Sandbox. After the publication, there was a month-long consultation period, during which the interested parties could submit their comments and concerns. CMA heard from over 40 parties, demanding the commitments to be strengthened in selected areas. The CMA commitments were accepted in February.

The commitments include:

- ensure that the CMA's role and the ongoing CMA process are mentioned in Google's key public announcements;
- instruct its staff not to make claims to customers which contradict the commitments;
- report regularly to the CMA on how Google has taken third party views into account;
- address concerns about Google removing functionality or information before the full Privacy Sandbox changes, including delaying the enforcement of its Privacy Budget proposal, and offering commitments around the introduction of measures to reduce access to IP addresses (Gnatcatcher);
- clarify the internal limits on the data that Google can use;
- provide greater certainty to third parties developing alternative technologies;
- improve the provisions on reporting and compliance, including appointing a CMA-approved monitoring trustee;
- provide for a longer duration of 6 years from the date of any decision to accept Google's modified commitments.

These commitments are available in full in the report. The consultation period is planned to end on December 17th 2021. Acceptance of these commitments will result in closure of the investigation and proceed to the oversight period.

One day before the CMA's report, the UK's Information Commissioner published an Opinion as a warning to companies designing new methods of online advertising to comply with data protection laws. While the CMA report focused solely on the Privacy Sandbox developed by Google, this opinion is much broader and touches all third-party cookies alternatives. The ICO wants to influence the emerging proposals while they are still at the early stages of development to avoid "window dressing" and actually give people control over their personal data. The commissioner clearly emphasised the will to improve the current state and not accept the alternatives maintaining the status quo. At the conclusion of the opinion, the commissioner proposed a list of recommendations for the industry:

- Demonstrate and explain the design choices;
- Be fair and transparent about the benefits;
- Minimise data collection and further processing;
- Protect users and give them meaningful control;
- Necessity and proportionality – the benefits are not disproportionate to be a risk to privacy rights;
- Lawfulness, risk assessments and information rights – the solution meets the requirements of appropriate lawful basis;
- Special category data – the solution addresses the potential of processing special category data.

**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' personally identifiable information (PII) to enable users to:

- Know what PII is collected;
- Know whether and to whom their PII is disclosed;
- Opt-out of its sale;
- Access any PII collected; and
- Request deletion of PII 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 personal data 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 domicile in Brazil) and material scope.

Under the law, organisations must establish a legal basis to process personal data and users are granted 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.

Changes implemented by browsers such as Chrome, Firefox, Edge and Safari (and the impending changes in Chrome) to prevent the use of third-party cookies and first-party cookie workarounds alter the way in which other parties, such as publishers, advertisers, and ad tech companies can collect and use personal information/data therefore have an 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. At that time, many third-party tracking companies had used redirects as a workaround to Safari's restrictions on third-party cookies. For example, a user would visit a news website, be redirected to the tracking website where it could place a cookie, then be redirected back to the website. As the redirect was instantaneous, the user was not aware of this happening. Apple's machine learning would detect this behaviour, based on user interaction with the tracking website.

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: Eliminated several workarounds, such as employing localStorage or using the JavaScript Document.referrer property. Made client-side first-party cookies expire after 24 hours, so that all "script writable" website data (primarily LocalStorage) will expire after 7 days.
- June 2020: Webkit announces App-Bound Domains, a new, opt-in technology. The App-Bound Domains feature takes steps to preserve user privacy by limiting the domains on which an app can utilise powerful APIs to track users during in-app browsing. As a result, it limits the possibility of cross-domain user tracking in in-app browsers.
- November 2020: Webkit announces it will be releasing its CNAME-cloaking defence feature to ITP in Safari 14 on macOS Big Sur, Catalina, and Mojave, iOS 14, and iPadOS 14. All cookies created by a third-party CNAME-cloaked HTTP response will be set to expire in 7 days. This limits the ability of domains to use third-party cookies as first-party cookies.
- June 2021: Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8. In the Mail app, Mail Privacy Protection stops senders from using invisible pixels to collect information about the user. The new feature helps users prevent senders from knowing when they open an email, and masks their IP address so it can't be linked to other online activity or used to determine their location. Intelligent Tracking Prevention is getting even stronger by also hiding the user's IP address from trackers. This means they can't utilise the user's IP address as a unique identifier to connect their activity across websites and build a profile about them.

These updates resulted in ITP 2.3 limited targeted advertising and made attribution difficult within Safari.

Note: ITP applies to all apps in the app store. ITP also applies to the Apple search ads system (created to promote apps in the app store). Find more information about Limit Ad Tracking and Personalised Ads here.

**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.

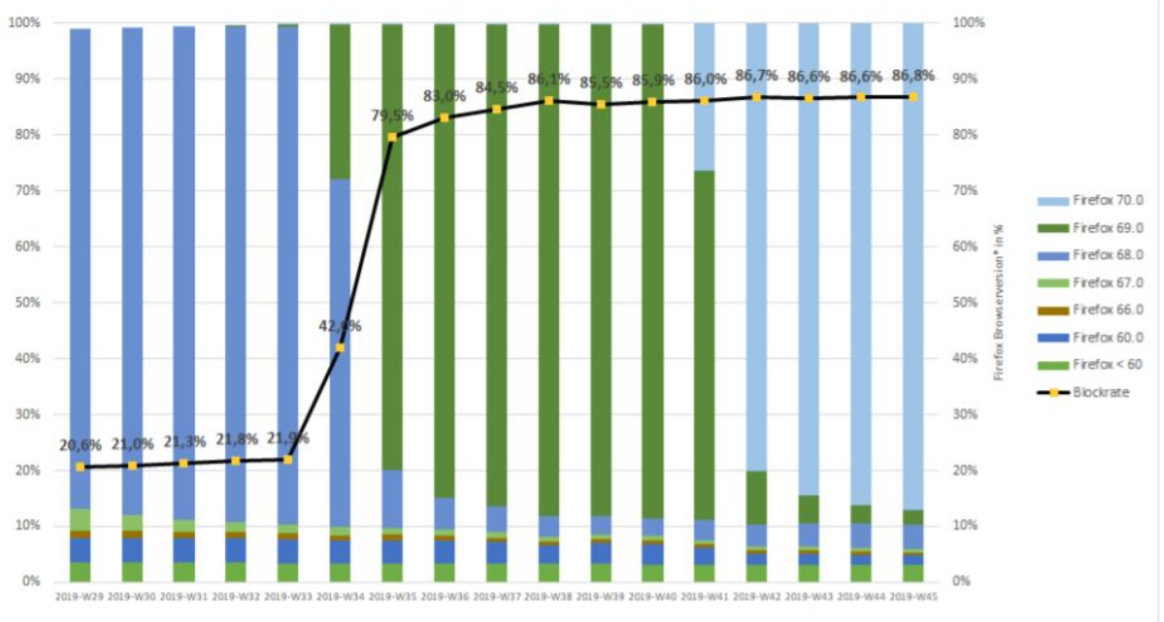


**Figure 3:** *Third-party cookie blocking rate measured for Mozilla Firefox in 2019*

The functionality of ETP was then updated as follows:

January 2020: Firefox 72 blocks third-party fingerprinting resources. Firefox 72 protects users against fingerprinting by blocking all third-party requests to companies that are known to participate in fingerprinting. This prevents those parties from being able to inspect properties of a user's device using JavaScript. It also prevents them from receiving information that is revealed through network requests, such as the user's IP address or the user agent header.

August 2020: Firefox 79 includes protections against redirect tracking. With Enhanced Tracking Protection 2.0, firefox will block a new advanced tracking technique called *redirect tracking*, also known as *bounce tracking*. ETP 2.0 clears cookies and site data from tracking sites every 24 hours, except for those with whom the user interacts on a regular basis.

January 2021: Firefox 85 limits the use of Supercookies. Supercookies can be used in place of ordinary cookies to store user identifiers, but they are much more difficult to delete and block. Over the years, trackers have been found storing user identifiers as supercookies in increasingly obscure parts of the browser, including in Flash storage, ETags, and HSTS flags. Changes to Firefox 85 have reduced the effectiveness of cache-based supercookies by eliminating the ability of the tracker to use them across different websites.

February 2021: Firefox 86 Introduces Total Cookie Protection.Total Cookie Protection, works by maintaining a separate “cookie jar” for each website user visit. Any time a website, or third-party content embedded in a website, deposits a cookie in the user's browser, that cookie is confined to the cookie jar assigned to that website, such that it is not allowed to be shared with any other website. Total Cookie Protection makes a limited exception for cross-site cookies when they are needed for non-tracking purposes, such as those used by popular third-party login providers. Only when Total Cookie Protection detects that the user intends to use a provider, will it give that provider permission to use a cross-site cookie specifically for the site you’re currently visiting. Such momentary exceptions allow for strong privacy protection without affecting the user's browsing experience. In combination with the Supercookie Protections announced in January, Total Cookie Protection provides comprehensive partitioning of cookies and other site data between websites in Firefox. Together these features prevent websites from being able to “tag” a user's browser, thereby eliminating the most pervasive cross-site tracking technique.

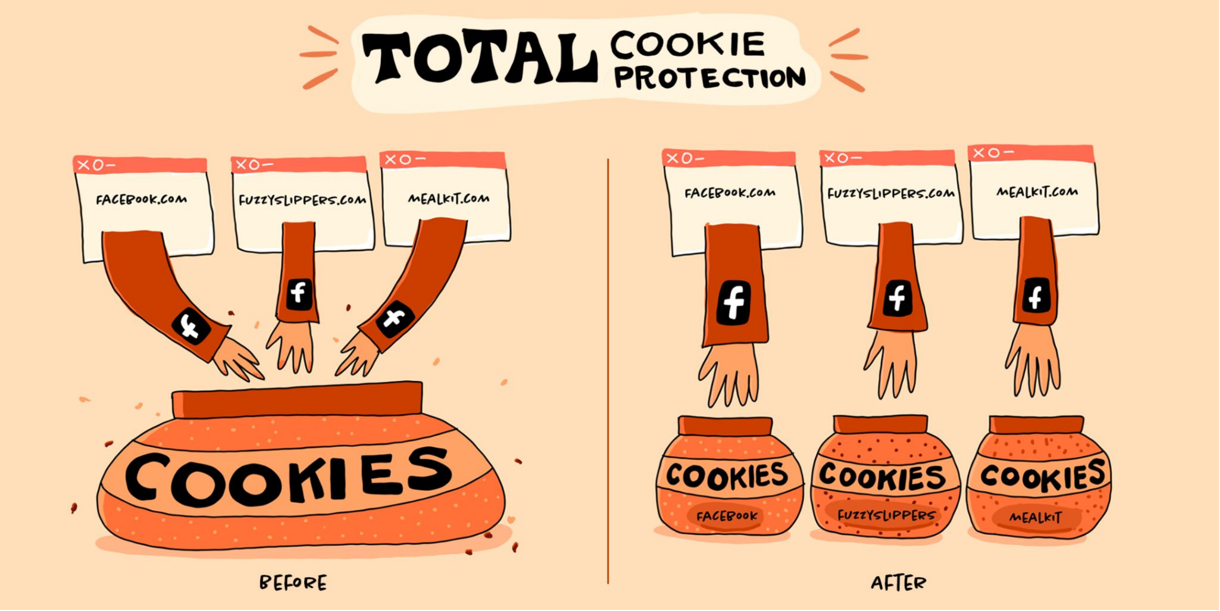


***Figure 4:*** *Total Cookie Protection. Source: https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/*

March 2021: Firefox 87 trims HTTP Referrers by default. Firefox by default trim path and query string information from referrer headers to prevent sites from accidentally leaking sensitive user data. The HTTP Referrer header often contains private user data: it can reveal which articles a user is reading on the referring website, or even include information on a user's account on a website.

March 2021: Firefox 87 introduced a new privacy feature called SmartBlock. SmartBlock intelligently fixes up web pages that are broken by its tracking protections.

April 2021: Firefox 88 reduces window.name privacy violations. Tracking companies have turned window.name property into a communication channel for transporting data between websites and enabling cross site tracking. Firefox started to clear the window.name property when the user navigates between websites.

June 2021: Firefox 89 blocks cross-site cookie tracking by default in private browsing. Since Firefox 86, Total Cookie Protection has been available for users who have ETP Strict Mode enabled. With Firefox 89 the same protection was extended to Private Browsing windows.

July 2021: Firefox 90 introduces SmartBlock 2.0 for Private Browsing. SmartBlock 2.0 ensure that the user can still use third-party Facebook login buttons to sign in to websites, while providing defences against cross-site tracking.

August 2021: Firefox 91 Introduces Enhanced Cookie Clearing. New version of Firefox Strict Mode lets users easily delete all cookies and supercookies that were stored on their computer by a website or by any trackers embedded in it.

October 2021: Firefox 93 features an improved SmartBlock and new Referrer Tracking Protections. With the release of version 93, Firefox started to ignore less restrictive referrer policies for cross-site requests, such as 'no-referrer-when-downgrade', 'origin-when-cross-origin', and 'unsafe-url'. Firefox started to always trim the HTTP referrer for cross-site requests, regardless of the website's settings. For same-site requests, websites can still send the full referrer URL. This makes it impossible to bypass the blocking of tracking by cooperation of websites with tracking companies.

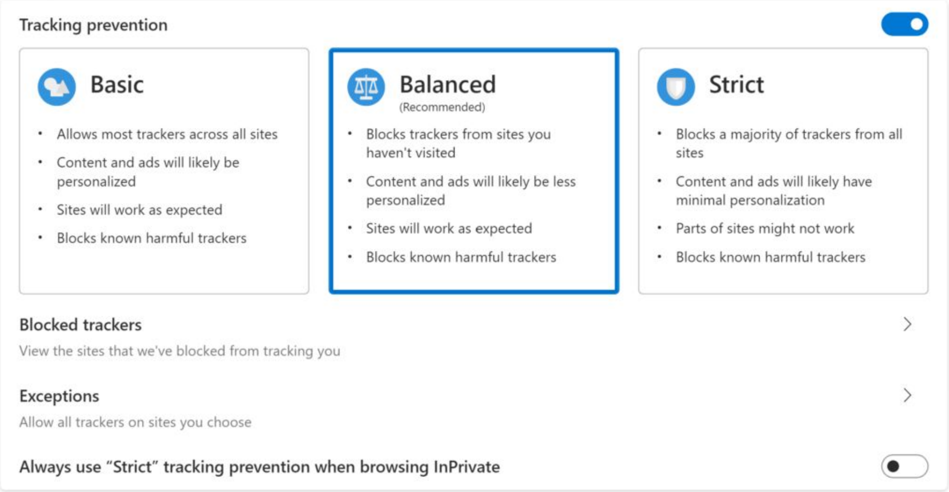
October 2021: Tim Geoghegan from ISRG, Christopher Patton and Christopher Wood from Cloudflare, and Eric Rescorla from Mozilla (CTO of Firefox) published a Privacy Preserving Measurement draft proposing a protocol for privacy-preserving measurement. The drafted proposal is based on the concept that a large set of clients depend on a small set of servers, which compute aggregate statistics over a client's inputs without learning the inputs themselves. In the draft, the authors propose and discuss the flow and the roles involved in it, as well as the risks and potential mitigations to them. This paper is of special significance, as it is the first large proposal with a key representative from Mozilla involved (CTO of Firefox), indicating which direction the company wants to follow.

January 2022: Collaboration between Meta and Mozilla - Ben Savage (Meta), Erik Taubeneck (Meta), and Martin Thomson (Mozilla) published an IPA proposal for advertising attribution that goes beyond existing solutions and introduces potential interoperability between browser vendors. This proposal aims to take significant parts from other proposals like Privacy Preserving Measurement.

## 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.



Tracking prevention

**Basic**

- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

**Balanced**
(Recommended)

- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

**Strict**

- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Blocked trackers
View the sites that we've blocked from tracking you

Exceptions
Allow all trackers on sites you choose

Always use "Strict" tracking prevention when browsing InPrivate

**Figure 5:** Microsoft Tracking Prevention (MTP). Source:https://blogs.windows.com/msedgedev/2020/10/26/safety-privacy-cyber-security-awareness-month/

January 2021 MTP updates: With Microsoft Edge 88 users can control which sites they share location, camera, and microphone access with. Users can review, edit, and reset site permissions, as well as see which permissions have recently changed. The option to delete only the third-party cookies was introduced.

**Chrome (Google)**

Chrome announced in May 2019 a change in cookie labelling to improve some aspects of privacy and security.  In February 2020 Chrome started rolling out a new security feature that required third-party cookies to be labelled with "SameSite=None" and "Secure". When the SameSite=None attribute is present, an additional Secure attribute must be used so cross-site cookies can only be accessed over HTTPS connections.

In August 2019, Chrome announced a new initiative (known as Privacy Sandbox) "to develop a set of open standards to fundamentally enhance privacy on the web" by developing new digital advertising tools to protect people's privacy and prevent covert tracking, while supporting a thriving ad-funded web. In January 2020 Chrome then announced its plans to phase out support for third-party cookies in Chrome within the next two years.  In June 2021 Chrome announced an update to the timeline and has made a public timeline available on privacysandbox.com for when third-party cookies would be phased out and replaced by privacy-preserving alternatives. The Privacy Sandbox represents an alternative pathway that Chrome, is proposing for the digital advertising industry to take.  Chrome has proposed several APIs which can be viewed and adopted by the ecosystem which address the following use cases: fight spam and fraud on the web; show relevant content and ads; measure digital ads; strengthen cross-site privacy boundaries; and APIs which address covert tracking techniques such as fingerprinting and network-level tracking. More information on the APIs can be found through privacysandbox.com and developers.chrome.com.

From March 2021 until July 2021 Chrome ran an origin trial for the first version of 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.  Chrome has been evaluating the feedback from the earlier origin trial of FLoC before advancing to further ecosystem testing.

The FLEDGE proposal (First "Locally-Executed Decision over Groups" Experiment) is a proposal for remarketing use cases.On 27 January 2022 Chrome published a proposed testing plan for FLEDGE, the Privacy Sandbox proposal to support remarketing and advertiser-defined audiences. This proposal for a first-origin trial is designed to reduce complexity and enable developers to begin testing the core features, with additional features and requirements added in over time. The Attribution Reporting API offers a way to measure when user action (such as an ad click or view) leads to a conversion, without using cross-site identifiers.

Chrome has made available a number of origin trials for Privacy Sandbox APIs in 2021 as outlined at privacysandbox.com/timeline and its origin trial page. In addition, a monthly blog Progress in the Privacy Sandbox offers a way to stay up to date on latest developments.

## 2.3 Ad Blocking

Ad blocking in a browser is a capability which removes tracking scripts and 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 being 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 adblock 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.

## 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 and 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. If advertisers are investing most of their budget in these platforms, they could 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, due to fewer buyers understanding the value of their bidding on specific advertising slots, which in turn impacts overall revenue.

It is 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.

A large number of advertisers will need to adapt their use cases such as frequency capping and audience targeting in absence of this cross-site identifier, but should be able to utilise privacy preserving technologies (either directly or through their adtech providers) to support them in the future.

Many publishers still have a reliance on audience extension, whereby publishers use their first-party data across a network of premium publishers.
However, when support for third-party cookies is phased out, publishers will need to consider how this, and other use-cases that rely on cookies that are set in a third party context, can be delivered utilising alternative privacy preserving technologies.

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 and transparency.

### 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 platforms. 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. Still, this should be achieved while maintaining the feel of transparency and control for the user.

# 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 one of the latest significant changes in the industry, ad verification and measurement can certainly adapt to a post third-party cookie world and has already started to do so.

## 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. Working with telco-verified transient identifiers can extend the advertising process to measure audience interaction and determine action outcomes.

5. 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.

6. 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).

7. 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.

8. 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 evolve in the coming years other methods may also become possible.

### 4.3 Attribution

The way in which measurement will change will also affect how advertisers will run attribution. Some bids will come with no identifiers, some with one and some with more than one. How can an advertiser deduplicate and attribute the frequency by which each user was exposed to a campaign?

Modelling will certainly be part of it but what is currently being used is not flexible enough to sustain the environment described above. Advertisers will need to test and try new models or a combination of them in order to achieve a meaningful result on how their campaigns are affecting users.

Certain identifiers that rely on emails should be more reliable than others and could be complemented by other IDs such as telco-verified transient activation IDs that reach “ghost” users and thus deliver attribution scale.

Increased fragmentation of data will make  attribution even harder and without some agreement within the industry or with publishers, advertisers will struggle more than they do now to make sense of the impact of their campaigns.

Measurement is a crucial point for the survival of the open web. Programmatic as a channel has evolved to become more measurable, and the spend more accountable. With the demise of third-party cookies, attribution and measurement models built on the analysis of personal information will no longer work.

However, there are many routes to measurement. The use case of attribution measurement can be performed without third-party cookies; various tools and techniques are now available or being developed. For instance, consortiums of adtech and publishers are building new identifiers based on hashed emails, and Chrome has proposed the “Privacy Sandbox initiative” which redefines a way for marketers to interact with users without the identifying  information ever leaving the browser.

# SECTION 5. OVERVIEW OF CURRENT ALTERNATIVE SOLUTIONS

Advertisers will always need a means to connect with their audience. 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 has continued to hold true as digital has grown to dominate the modern marketing budget. Third-party cookies have played an instrumental role in supporting the growth of digital advertising for over 25 years. However, with the rapid discontinuation and replacement of reliance on third-party cookies in progress, this is set to evolve. Currently, the dominant alternative for the third-party cookies are first-party ID based solutions. However, in addition to first-party IDs, there are a wide range of different concurrent technologies all of which serve as essential tools in evolving a digital landscape where third-party cookies cease to be the dominant tool for cross-site tracking, retargeting, and ad serving in digital advertising.

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 and the different identifiers used today.

## 5.1 Identity

The challenges of 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, 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. 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 and digital services. Any loss in the ability to frequency cap, and provide relevant advertising also diminishes the overall user experience on the web, and encourages further fragmentation and barriers to access such as paywalls.

Luckily, while the third-party cookie has long been the most used tool for facilitating these benefits, new technologies are rapidly surfacing that strike a balance between privacy and relevance, delivering the opportunity for advertisers to reach relevant audiences without compromising web users' privacy or ability to control their interactions.

**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 and optimised advertising. Advertising identifiers can be either device or user-level, depending on the type of identifier. Identifiers can have the following characteristics:

- **Persistent, Semi 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.
    - Semi-persistent identifiers are generally first-party cookies that may or may not link to a persistent identifier for consistent customer recognition:
    - Transient identifiers, within a closed ecosystem, used for activation purposes can be linked to semi-persistent identifiers for delivery against the above use cases, e.g. telco-verified transient IDs.

- **People-Based vs Technographic Identifier**
    - **Technographic Identifiers** include browser applications (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 / Inferred**
    - Deterministic information is explicitly declared by the person providing it e.g. emails or logins.
    - Probabilistic / inferred information uses multiple data points statistical methods to associate a device with an identifier. They use commonly known criteria such as IP address, operating system, geo etc.

- **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 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 (such as hashed email), publisher first-party IDs/storage, or telco verification
    - Often called first-party IDs, Common IDs, Stable IDs, Universal IDs, among other terms

- **Pseudonymous probabilistic / inferred identifier**
    - Based on statistical modelling methods
    - Requires sufficient data scale to work/train properly – as more data touch points per user/person increase the potential accuracy and relevance

**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.

## Pseudonymous Deterministic Authenticated Identifier

This type of identifier uses an authentication event (usually an email address being entered into some form on a website) or a verification event - usually linked to a telco network verification request - as the basis for the creation of the ID, hence “authenticated” or “‘verified’”. Device associations for this type of identifier are based on personally identifiable information (PII) that has been anonymised, often through a double process of “hashing” and “salting.”

Hashing refers to changing an email or MSISDN (Mobile Station Integrated Services Digital Network - i.e. a mobile phone number) to a random string of characters which cannot be reversed. Salting is adding additional characters to that string. Additional encryptions and encoding may then also be applied for these IDs, including platform-level encoding. Because these IDs are based on user-authentication or verification 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 an  email or phone number, could potentially help solve the loss of third-party cookies and MAIDs in multi-device, web, and app environments. For a comprehensive list of ID solutions available, please refer to the list on page 68.

## 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 consent under the ePrivacy directive when the algorithms use data actively retrieved from the user's device (such as available fonts and screen size). Furthermore, this is considered by many, including every major browser, to be fingerprinting and explicitly prohibited for advertising purposes.

## 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 harder to do 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.

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 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 relatively rare 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/or accumulated over time without loss.

2. The email address as an identifier is platform agnostic, unlike a third-party cookie, which  is 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 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 difficult due to cookie sync issues and a lack of open web publisher authentications.

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 or open exchange. When consumers within that audience visit an 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). Some onboarding solutions remove the need for the third-party cookie or MAID and rely entirely on publisher authentication to make the connection.

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

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. 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 setbacks 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 licence 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.

In recent years, this secure approach to identity has been extended to programmatic digital advertising.

Mobile operators offer several identity solutions:

- **Single-Sign-On (SSO)** - a means for a single set of identity credentials to be used across multiple websites, rather than registering and remembering multiple credentials.
- **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.
- **Publisher or Brand Audience Verification** - verification of consented first-party publisher cookies to create accurate, real-time cross domain and cross device, privacy compliant user profiling to address the challenges of the newly anonymised web.
- **Audience Activation** - a transactional and anonymous method of matching consented first-party audience data, within publishers or brands own properties and the open web, to improve advertising effectiveness without any PII data entering the ad tech ecosystem.

This application of telco intelligence in digital advertising allows for the continued creation of verified audiences for publishers and brands 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 intelligence, , 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 data privacy regulations.

Using telco intelligence 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, European Publishers Council in EMEA, and Advertising ID Consortium. 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).

Shared IDs should be encrypted, and should require secure APIs or hosted applications to leverage. The different entities that transact on shared IDs should only be able to share or overlap protected data if all parties involved in the transaction are permissioned, which enables publishers, platforms, and marketers to transact programmatically on a people-based identifier ethically and securely at scale.

Furthermore, shared IDs should be neutral and interoperable, in a trusted and verified, privacy-conscious manner. Technology should be compatible and support an open ecosystem that is trusted, open and neutral.

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

- BritePool (BPID)
- Criteo ID for Exchanges
- Fabrick ID
- Halo ID
- ID5 Universal ID
- IDx
- IntentIQ ID
- LiveIntent ID (NonID)
- LiveRamp RampID) (formerly known as IdentityLink)

- Lotame Panorama ID
- Merkle ID
- netID
- Novatiq Hyper ID (previously Snowflake ID)
- 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 into Prebid and OpenRTB. Publishers can support as many of the above mentioned ID modules as they want to natively via these standards.

### Use Cases for Working with Multiple IDs

There are several use cases where brands and publishers would choose to work with multiple IDs. Two that stand out are:

a) **Global operations**: universal ID scale across supply could vary across global regions, where some IDs might have a stronger footprint in some countries as opposed to others. Brands and publishers with global businesses could consider choosing preferred IDs on a country by country basis.

b) **Authenticated and non-authenticated traffic**: We can assume that a large portion of site visitors will not be authenticated. So even the most scaled authenticated ID won't be able to reach users who have contributed and consented to the use of their email address in targeting. Inferred IDs and Telco verified IDs can reach non-authenticated users, with consent. Publishers and brands will need to consider ID solutions for both authenticated and non-authenticated audiences.

## 5.4 How to Evaluate ID Providers

We have seen an influx of new IDs and a 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.

For brands, choosing which universal ID to build audience segments off of is a critical decision. For publishers, ID integration comes with development cost and potential impact on page performance.

Brands can use the following methodology to evaluate IDs. This methodology is important for publishers too, as they need to understand the drivers behind brand decision making.

a) **Availability in global regions**: the first step is understanding ID prominence in countries where brands and publishers seek to reach their customers

b) **Capabilities by data targeting type:**

   **i)** Offline first-party data: what type of information from a customer database can an ID onboard and activate? All authenticated IDs are based on emails. Telco verified IDs are associated to an obfuscated phone number which enables a link back to a first party cookie. In addition, businesses may need to determine if an ID can also be associated with other information such as phone number, physical address, first and last name, etc…

   ii) Site visitors: to enable retargeting, an ID needs to allow brands to create an identifier on owned properties without using third-party cookies. This requires brands to integrate identity infrastructure just as publishers do. Brands that do retargeting but lack authenticated users should consider inferred IDs or Telco verified IDs that don't rely on email.

   iii) Third-party data: Brands that target new customers need to ensure that universal IDs can be used in audience segments from their preferred third-party data vendors.

In order for brands, publishers, and platforms to better understand the capabilities of universal 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 |
| Does the vendor’s technical design conflict with browser vendors proposals aiming to mitigate cross-site tracking,fingerprinting or network-level tracking (e.g tacking by VPN service or ISP vendor)? |
| Can anonymous ‘ghost’ web users be identified and activated? |

| **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 |
| How is privacy protection enabled? Are there patented solutions with proven applications? |
| How does your solution correspond with https://webkit.org/tracking-prevention-policy/? |
| How does your solution correspond with the draft of Target Privacy threat model under W3C? |

| **CAPABILITIES** |
|---|
| Technical: Can you explain how the solution works technically or provide a flow diagram? |
| Is the ID user-level? Is it Dynamic and in real-time? |
| **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 the 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) |
| **Accuracy:** How accurate is the targeting? Is it deterministic or probabilistic? |
| **Interoperability:** Does the ID solution stand alone or work in combination with other authenticated IDs? How flexible is the solution? |
| **Future-Proof:** How robust is the solution if further changes to the programmatic ecosystem or regulatory environment occur? |
| **Cross-platform:** Does the ID work across both web and app properties on both mobile and desktop? |

| **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? |
| Is the ID easy to deploy? |
| **Consumer Experience:** How easy is it for the consumer to understand and manage how their data is being used? |

### 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.

DSPs provide contextual details regarding the impressions won and attributed to a conversion, typically page-level information (domain, country code, etc.), bid-level information (bid price, creative size, seller name, etc.) and browser-level information (device type, family browser, family OS etc.)

The information is then linked to a DSP user id, which is normally hashed or zeroed by the DSP in GDPR zones.

The exact content of campaign logs provided by each DSP is accessible in their technical documentation and can be provided under request.

The ad tech economy is diversified and technology abundant. For example, developments in AI are here, and their methods rise above the need to invade user privacy to create performance and scale for advertisers. Instead, AI will use the plentiful, harmless, non-user-specific metadata from bid requests on websites to create better alignment between brands and consumers. The technology is poised not simply to remedy the limitations of the cookie and personal identifiers, but also to untangle the unfortunate relationship between privacy and performance in marketing.

Machine learning and artificial intelligence are key to making the most of these new data sources and filling the gaps left by third-party cookies. These tools will be able to process cohort data for example, that has been anonymised following anonymisation procedures such as K-anonymity or differential privacy, making it impossible to drill down to a specific user’s details. They will also help model and predict user behaviours based on the analysis of readily accessible, abundant data points available routinely from non-user-specific interactions with webcontent. This will help deliver efficiency and scale for advertisers and their supply chains.

## 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'. More advanced methods make use of autonomous deep learning and advanced Natural language processing, going beyond a mere statistical analysis of word distributions in textual content. This way, groups of words are identified that share common semantics and thus create data-inherent structures of meaning, or topics, appearing in the content and making them available for targeting. Another way of describing these approaches 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. Topics, on the other side, consist of terms that tend to co-occur together across a large amount of documents. This provides yet another way of surpassing the restrictions of single keywords and enables targeting on a more abstract semantic level. In consequence, this approach allows for larger reaches as keywords are not matched directly but through the semantics they convey.

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 near a story 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 (travelling, 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.

For more information on Contextual Advertising, please refer to the IAB Europe Guide to Contextual Advertising

# 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 varies based on company circumstance. However, we’ve outlined some details about these efforts and initiatives below to provide some context to help 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 earns the endorsement by the W3C community. This is one forum in which the Chrome team has looked to engage feedback from industry on standards outlined in the Privacy Sandbox. The recently formed Private Advertising Technology Community Group is one example where ads proposals will be discussed and where browsers, ad tech vendors, publishers and marketers can discuss the solutions.  There have also been discussions on Privacy Sandbox APIs in GitHub.

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.

Most essential groups from the perspective of current development:

1. Privacy Community Group - develop privacy-focused web standards and APIs to improve user privacy on the web through enhanced browser behaviour

2. Improving Web Advertising Group - identify areas where standards and changes in the Web itself can improve the ecosystem and experience for users, advertisers, publishers, distributors, ad networks, agencies and others

3. Private Advertising Technology Community Group - incubate web features and APIs that support advertising while acting in the interests of users, in particular providing strong privacy assurances.

4. Web Incubator Community Group - venue for proposing and discussing new web platform features

## Proposals referring to advertising

| Name | Use Case | Active Contributors |
|---|---|---|
| FLEDGE API | Targeting, Ad delivery | Criteo, Google, Magnite, NextRoll, RTB House |
| Topics API | Targeting | Google |
| Core Attribution API | Reporting | Google, Yahoo Japan |
| First-Party Sets API | Group multiple websites owned by same entity under 1st party cookie label | Google |
| Parakeet | Targeting, Ad delivery | Microsoft |
| Private Click Measurement | Reporting | Apple |
| Interoperable Private Attribution (IPA) | Reporting | Meta, Mozilla |
| Federated Credentials Management | Preserve email-based Single Sign On service without cross-site tracking | Google |
| Trust Tokens API | Fight spam and fraud | Google, Yahoo Japan |
| Gnatcatcher | Fight IP fingerprinting | Google |

## 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 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 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:

- Akamai
- Admixer
- Adtelligent
- Audigent
- AMX RTB
- Britepool
- Criteo
- Deepintent
- DMD
- Epsilon
- FLoC
- ID+
- ID5
- IDx
- IntentIQ
- Intimate Merger
- Justtag
- Kinesso
- LiveIntent
- Liveramp
- Lotame Panorama
- MediaWallah
- Merkle
- Navegg
- NetId
- NextRoll
- Neustar FabrickId
- Novatiq
- Parrable
- Pubcommon (owned by Prebid now)
- PubProvided
- Quantcast
- Retargetly IDx
- SharedId (owned by Prebid now)
- tapad
- Trade Desk UnifiedId
- Turstpid
- Verizon
- Yahoo
- 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.

# SUMMARY

2021 was another turbulent year in terms of the conversation about third-party cookies. On 24 June 2021, Chrome announced a delayed timeline for phasing out third-party cookies, which was extended to 2023. Chrome's delay reflects the need for the industry to learn and adapt to the new technical landscape.

The need to better control third-party cookies became evident with the increasing conversation about data collection and consumer privacy, portrayed in many legislation acts such as the GDPR, or CCPA. Everyone in the industry supports the need to better protect the privacy of the user, however the big changes come with challenges for advertisers and publishers.

In this updated guide, we examine how the industry has been dealing with the upcoming changes, what new technologies have emerged, and how advertisers and publishers can best learn, prepare, and thrive in the post-third-party cookie era.

When it comes to publishers, the answer to the question "what's next?" is fairly straightforward: first-party data. Many publishers, especially the ones with premium content, logged in users, and any sort of subscriptions, already have valuable information about their users that can be a huge asset in attracting potential advertisers.

Advertisers, on the other hand, will need to learn to function without some of the features of the programmatic landscape they've grown accustomed to. We know for sure that features such as frequency capping, cross-publisher identifiers, or even DMPs will not be available in their current form for much longer. Furthermore, the way the advertisers measure exposure to their campaigns is directly affected, and we present a list of available solutions, which can be used in place of third-party cookies for exposure and attribution measurement.

The industry is becoming more and more familiar with solutions such as advertising identifiers, which the advertiser can use on device or user-level to aid with frequency capping and /or targeted, optimised advertising.

Moreover, some already well-known solutions are experiencing a rebirth. Solutions such as contextual targeting, CRM, and email, are looked at from a different perspective and the industry is wondering how they can use what they already understand and have to hand, to a new advantage.

Finally, the industry has a unique opportunity to evolve and advance over the next 24 months and beyond, and 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 give 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 and IAB Tech Lab's Project Rearc.

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.

# UPDATE CONTRIBUTORS

*Disclaimer: IAB member company employees contributed to this report as members of IAB Europe's Programmatic Trading Committee. IAB member company employees did not provide all of the information regarding their company's business or activities. The overall content and perspectives reflected in this report are the work of the Committee not IAB member companies specifically.*

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

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

Xara McDonald, Solutions Engineer, Amobee

David Goddard, Vice President Business Development, DoubleVerify

Emmanuel Josserand, Sr Dir. Brand, Agency and Industry Relations, Freewheel

Ben Geach, Consulting Lead, gTech Professional Services, Google

Jamie Penkethman, Identity Product marketing, Index Exchange

Elżbieta Kondzioła, Online Sales Director, LOVEMEDIA and Łukasz Włodarczyk, VP of Programmatic Ecosystem Growth & Innovation, RTB House, representing IAB Poland

# UPDATE CONTRIBUTORS

Ines Talavera de la Esperanza, Public Policy Officer, IAB Europe

David Okubo, Global Communications Manager, Liveramp

Garrett McGrath, Senior, Vice-President, Product Management, Magnite

Ferdinand David, VP, Product Policy & Compliance Lead, , MediaMath

James Kerr, Regional Counsel and Data Protection Officer, EMEA and APAC, MediaMath

Tanya Field, Co-Founder & CPO, Novatiq

Rémi Lemonnier, Co-Founder & President, Scibids

Patrick Jähnichen, Global Director Product, Data and Machine learning, ShowHeroes Group

# UPDATE CONTRIBUTORS

| | |
|---|---|
| YIELDBIRD | Zuzanna Zarebinska, Strategy Analyst, Yieldbird |
| ZEOTAP | Florian Lichtwald, Managing Director, Chief Business Officer, Zeotap |

# PREVIOUS CONTRIBUTORS

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

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

Akshay Bhattacharjee – Programmatic Solutions Specialist for the Nordics & CEE Region, IAS

Ian Maxwell, Converge Digital representing IAB Ireland

Thibault Montanier, Data Manager and Integration Specialist, Sirdata & Co-Chair of IAB Europe's Post Third-Party Cookie Taskforce

Alex Cone, Senior Director, Product Management Jordan Mitchell, SVP, Head of Consumer Privacy, Identity and Data, IAB Tech Lab

# PREVIOUS CONTRIBUTORS

Gokberk Ertunc, Programmatic Manager, OMD Turkey / IAB Turkey

Valbona Gjini, Marketing Director, ID5

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

Zara Erismann, MD Publisher Europe, LiveRamp

Garrett McGrath, Vice President, Product Management, Magnite

William Lee, Mgr, Product Policy & Comp, Chris Keenan, Regional VP, Business Development and Jamie Penkethman, Sr Director, Product Marketing.

Tanya Field, Co-Founder & Chief Product Officer, Novatiq

Miles Pritchard, Managing Director - Data Management Solutions, OMD

# PREVIOUS CONTRIBUTORS

Carlotta Zorzi, Global Brand Partnerships, Oracle Data Cloud

Laine Rosa, Product Manager, Outbrain

Maria Shcheglakova, Marketing Director EMEA, PubMatic

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

Gabrielle Le Toux , Senior Marketing Manager, Xandr

Szymon Pruszyński, Head of Growth, Yieldbird

Joshua Koran, Head of Innovation Labs, Zeta Global

Livia Busseni, VP Global Solutions Engineering, Zeotap

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

**Marie-Clare Puffett**
Senior Manager, Marketing & Industry Programmes
puffett@iabeurope.eu

iab europe
Rond-Point Robert
Schumanplein 11
1040 Brussels
Belgium

@iabeurope

/iab-europe

**iabeurope.eu**