

2024
edition

identifiers explainer
guide and matrix



identifiers explainer guide and matrix has been developed by the iab australia data advertising council.

Gabbi Stubbs
Adobe

David Raitt
Azira

Claire O'Mahoney
Blis Media

Danny Tyrell
DataCo

Christian Williams
Equifax

Damian Quinn
Eyeota (Dun & Bradstreet)

Dylan Dharmadasa
Finecast

Lauren Dulhunty
Flybuys

Shaun Donnelly
Foxtel Media

Maddy Oldfield
Google

Tom Leahey
Hearts & Science

Jonas Jaanimagi
IAB Australia

Paul Hewett
In Marketing We Trust

Rick Knott
InfoSum

Natalie Hatch
Kinesso

Kate Steven
LiveRamp

Poorani Adewole
Mindshare

Vishal Shah
MiQ

Blake Talarico
Nine

Taylor Svarc
OMD

Phil Hammond
Paramount

Emily Smith
Paramount

Steven Zhu
REA Group

Tom Gilmour
REA Group

David Wise
RTB House

Virgile Edragas
Samsung Ads

Cameron Strachan
Southern Cross Austereo

Emily Smith
Seven

Greg Kearney
Suncorp

Isabella Spragg
The Trade Desk

Balraj Saini
TikTok

Simon Conyard
Wavemaker

Lorraine Donnelly
Yahoo

co- chair
Rachida Murray
Spark Foundry

co- chair
Moritz von Sanden
Audience360

overview

purpose

This document provides a very simple explainer of the various identifiers in the Australia market, including some recently updated technical best practices and an updated visual ID Matrix of the most popular available solutions for both ID providers and audience matching tools.

The IAB Australia Data Council is keen to provide this as a starting point of research into this fast-evolving space, for both buyers and sellers. This explainer has been supplemented by a fuller table of the individual providers available in Australia with more detailed information therein.



extra information

We have also included a simple intro, a glossary of terms and some suggested next steps for both buyers and sellers.

index

01 introduction	jump to →	pg 5
02 identifiers	jump to →	pg 9
03 deterministic data, probabilistic data, matching & encryption	jump to →	pg 17
04 iab tech lab id solutions guidance	jump to →	pg 22
05 working examples for both buyers & sellers	jump to →	pg 26
06 consolidation of PAIR & OPJA protocols	jump to →	pg 33
07 openRTB id provenance	jump to →	pg 40
08 considerations for buyers & sellers	jump to →	pg 46
09 id matrix	jump to →	pg 51
10 further reading	jump to →	pg 57
11 glossary of terms	jump to →	pg 59

[click to go to
index page](#) →

01 introduction

introduction

It has been some 3 years since the last ID guidance so the IAB Australia Data Council felt compelled to provide an update on the key related latest standards and best practices.

Our intent is for both buyers and sellers to have more confidence in making decisions related to how to approach leveraging these solutions. Identity solutions can harness a range of different signals to construct a comprehensive single-view of digital consumers. These signals can range from deterministic data, where the identity is known with certainty, to browser and device data, where identities are inferred based upon predictive patterns and correlations.

When our members are locally trying to navigate the various options available using hashed emails, device IDs, or probabilistic identifiers we wanted to provide an update to the original v1 guidance to continue to help simplify these processes through all of the relentless changes we are seeing. There have been some specific updates from IAB Tech Lab regarding ID solutions guidance, the forthcoming consolidation of the PAIR & OPJA protocols and OpenRTB updates to enable improved transparency on identifier sourcing and application within the bidstream.

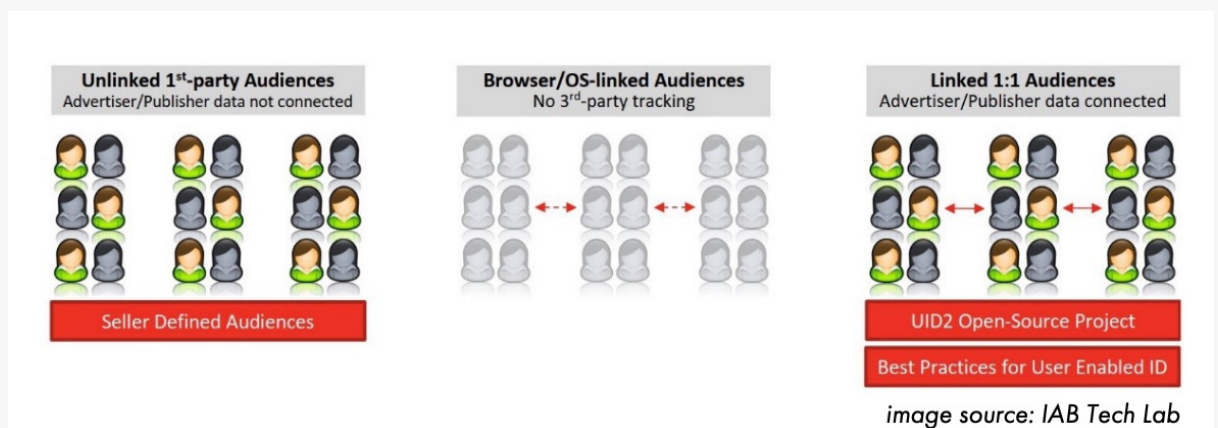
The majority of the original content from v1 remains, along with some new additional content sections. We have also included some links for further reading and an updated the matrix of the most popular ID Solutions available here in Australia in what we hope is a simple and useful format for interpretation. We've reduced the number of solutions as market forces have gradually but inevitably dictated which are locally the most utilised. Lastly, we've also split the solutions into two - one being solutions that will create IDs and the other being solutions that leverage them.

introduction

As a result of the ongoing deprecation of third-party cookies, recent privacy features in Apple's iOS environments reducing IDFA volumes and the resulting negative impact on the mechanics of digital advertising, in March 2021 IAB Tech Lab released a set of four standards which draw from existing standards in-market and included Best Practices for User-Enabled Identity Tokens Guidelines. These specifications have drawn a clearer focus on how one of the (three) future-proof approaches will be the use of identity service to competently link 1:1 audiences between publishers and advertisers. These services have traditionally kept the open internet free and to consumers through advertising and moving forwards will require either an explicitly opted-in device-based ID or secure, user-enabled ID from a login, email, etc. potentially connected to a clean room approach.

starting point

As a starting point for this explainer guide, we should define the meaning and details around 'identity' and 'identifiers', as these terms are often used liberally to refer to similar things.



They will also have to be secured and have highly transparent uses offering consumers a full suite of privacy-focused controls.

key considerations on privacy

With the Privacy Review in Australia now in full swing, it's more important than ever for industry to fully embrace the ongoing shift towards more privacy-centric and consumer-first approaches that fully respect individual rights, whilst still enabling effective advertising. Responsible data practices and responsible addressability build trust and will benefit consumers, publishers, tech vendors and marketers in the long term.

Below are some key considerations for industry regarding consumer privacy and the use of Personal Information (PI). Please note, these considerations are only, intended as a guide and are not legal advice. IAB Australia always recommends that our members seek legal advice based on the specific circumstances and business practices of the organisation.

- Understand whether, and the extent to which, data that you collect, or hold constitutes PI (noting that this definition may change in the next tranche of privacy reforms).
- Obtain clear consent before collecting and using data which is PI. Opt-in consent will be required in most cases.
- Be transparent about data collection and usage. All organisations need to clearly disclose what data they are collecting, how it will be used, who it will be shared with. Transparency and a clear value exchange with consumers builds trust.
- Give consumers full control and remit over their data. Provide easy opt-out options and allow consumers to access, correct, or delete their personal data upon request.
- Implement robust data security measures. Protect PI data through encryption, access controls, and other cybersecurity best practices to prevent data breaches.
- Comply with local privacy regulations in all countries that you do business in.
- Limit collection and retention of PI. Only collect the minimum amount of personal data necessary and don't retain it longer than needed.
- Use anonymisation and pseudonymisation techniques. De-identify personal data to protect individual privacy whenever necessary.
- Take extra precautions with sensitive PI, such as financial information and health data, and always comply with additional privacy obligations in relation to this type of data.
- Provide clear value to consumers in exchange for their data. Ensure consumers get clear and tangible benefits (e.g. personalisation or exclusive content and/or offers) in return for sharing their data.
- Respect consumer preferences. Adhere to any consent signals or do-not-track signals received and any other indications that users don't want to be tracked or targeted.
- Educate consumers. Help users understand how their data is used for advertising and the choices they have regarding privacy.

[click to go to
index page](#) →

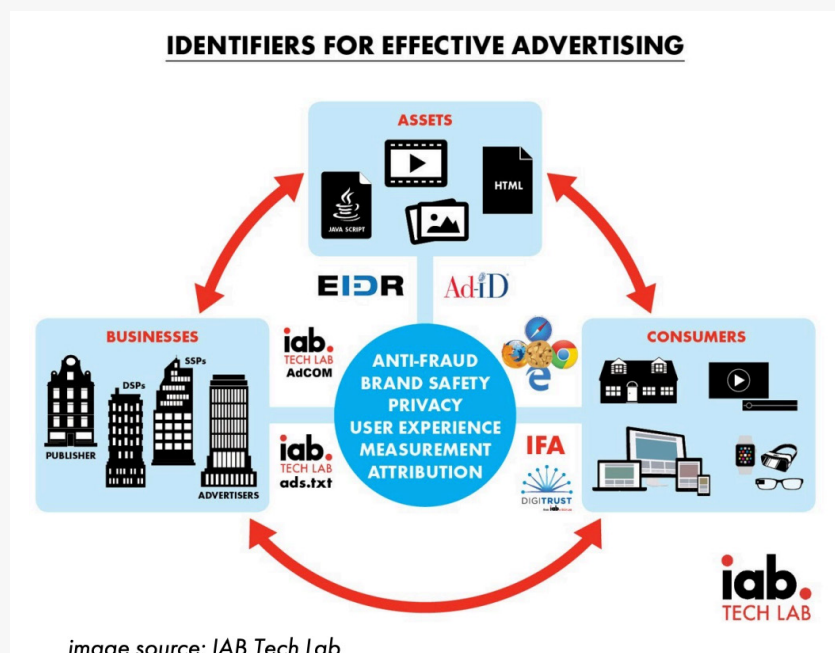
02 identifiers

what are identifiers

We'll start with identifiers, which are prolific and consumers can easily have hundreds or thousands of identifiers across all of their browsers and devices. We align to the IAB Tech Lab view that identifiers come in 3 types - consumer, creative assets, and the business entities involved in the supply chain. These identifiers are the core building blocks that help fight fraud, improve brand safety, deliver a better experience to consumers, and support measurement and attribution.

type of identifiers

We align to the IAB Tech Lab view that identifiers come in 3 types - consumer, creative assets, and the business entities types of involved in the supply chain.



identifiers by type

Consumer IDs

Identify individual users or a group of people within a household (all generally anonymously), but may ultimately be tied to devices or browsers, depending on the available data (such as logins) on various platforms. Examples are cookies, DeviceIDs or IFAs (Identifier For Advertising) such as GAID or IDFA on mobile devices. These are utilised for the purpose of understanding user behaviours and interests for targeting and personalisation, assessing where/when a person saw an ad (for measurement and attribution), and applying known privacy preferences consistently across sites, apps, and devices. This allows platforms to develop insights into users' needs and deliver a better experience by providing more relevant ads.

Asset IDs

Identify creative assets as they go through the advertising supply chain, to make it easier to understand what was or will be shown to a consumer, ensuring that the right content is delivered to the right individual (separating ads from competitors, age appropriate etc.), and enabling accurate measurement/tracking of which creatives were displayed where and who they were presented to. Asset IDs are also important to help with brand safety by tying the ID to metadata about the creatives.

Business IDs

Identify the various companies such as publishers, advertisers, and vendors that provide content and ads to consumers, and execute a range of other functions across the advertising supply chain. These IDs are used mainly to manage trust, reduce fraud, and improve transparency.

identity management

As consumers can have so many different identifiers across all their various browsers and devices, the real effort is in being able to manage and leverage these into a genuinely useful version for marketers and publishers. Cookies, for instance, have been a very useful short-term identifier as they can be used (for now) and shared fairly widely, but often for the purposes of true identity management they are simply too inferred and degrade too quickly. However, through the unification of the various identifiers and appended data points a persistent Individual ID can be created, which can be utilised as being a more meaningful and shareable and unified profile for each individual. This process is often referred to as Identity Resolution and the tools used to align the various identifiers and store them is known as an Identity Graph.

These persistent customer identities can also be supplemented with other data, including offline to build out a fuller and more accurate anonymised profiles to target, campaign manage and measure online advertising. Ultimately, all the various device-level identifiers are merely an enabler of advanced identity resolution solutions

examples of identifiers

IDFA (Identifier for Advertisers)

GAID (Google Advertising ID)

Cookies

Hashed email addresses

Phone numbers

CRM data

Financial Transactions

different identifier examples.

IDFA

Apple's Identifier for Advertisers is a device identifier assigned to users of Apple devices. It is used for anonymous tracking and identification of consumers.

GAID

Google's advertising ID is a device identifier assigned to users of Android devices. It is used for anonymous tracking and identification of consumers.

MAIDs

General term for a mobile advertiser ID, which is a unique string of digits identifying a specific mobile device.

cookies

Also called HTTP cookies, internet cookies, or browser cookies, are files stored on the hard drive of computers designed to hold a small, specific amount of data about a particular website or client. Their primary purpose is to identify the user so his or her web experience can be customised and to streamline the online surfing process by saving certain information such as email, home address, shipping information, username or password, or interests. We define 1st, 2nd and 3rd party further on.

hashed email addresses

As most people keep their personal email addresses forever and are ubiquitous, making emails a key future identifier in the future of digital marketing.

Hashing is a method of encrypting data, such as email addresses, into a hexadecimal string. Each email has its own unique hexadecimal string, made up of 32-character codes, that remains consistent no matter where the email is used as a login and is unique to each email address. This code cannot be reversed, making it completely anonymous. See also the definition of tokenization further on – including a comparison of tokenization vs. encryption.

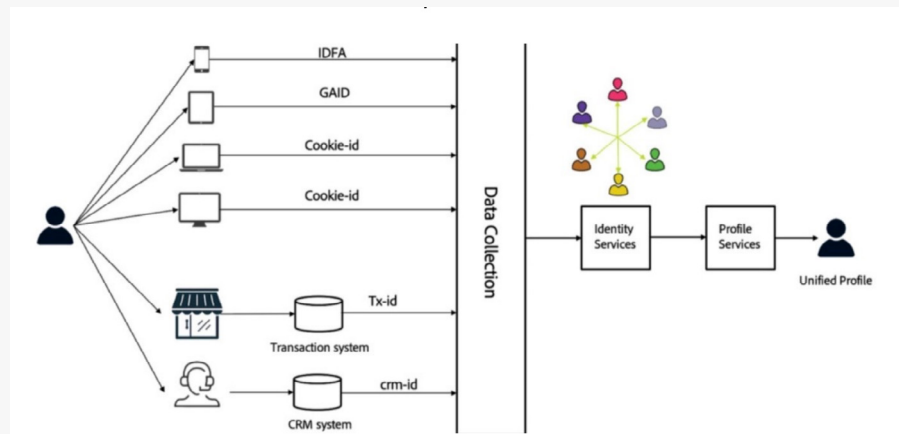
different identifier examples.

phone numbers

Mobile phone numbers, in particular, have more recently been commonly used as a consumer identifier for two-factor authentication as these phone numbers have increasingly become more reliably attached to individuals over the long term. As a sensitive piece of personally identifiable information (PII) data, phone numbers should also be securely hashed.

CRM data

A customer relationship management (CRM) database is all of the data about consumers that businesses capture and store within a CRM system. The different types of data stored inside a CRM database include data points such as: contact name, title, email address, social profiles, contact history, lead scoring, order history and personality traits. Most of this is personally identifiable information (PII) data and therefore very sensitive.



financial transactions

Similar to standard CRM data, however this also includes personally identifiable information (PII) data such as age, job, nationality, social status, place of residence - as well as income and consumption data, size of incomes, size of debts, different sources of income, credit/debit card purchases, standard inter-bank payments, loans and deposits.

identity resolution.

An identity resolution solution can permanently keep track of any preferences and consent signals from identifier to identifier, as well at each data touchpoint - thereby enabling effective and actionable insights for marketing and personalisation.



image source: CDP Institute

This enables management, via a single customer view, a consistent consumer experience as the updates and privacy controls can be made more seamless and persistent. With privacy reviews underway here in Australia this is increasingly a critical capability.

The unified approach is also the most effective technically for consistently and cleanly managing a consumer's digital privacy.

deprecation of third-party cookies

Google will eventually allow users to opt-out of out third-party cookies sometime in 2025. Since 2017, other popular browsers such as Apple's Safari and Mozilla's Firefox have already implemented some default blocking against third-party tracking cookies.

TOP 3 BIGGEST IMPACTS ON BUSINESS

MARKETERS

- 1** Reduced targeting opportunities
- 2** Loss of personalisation
- 3** Decrease in revenue

PUBLISHERS

- 1** More competition among publishers to demonstrate unique value
- 2** Reduced workforce due to revenue loss
- 3** Significant loss of programmatic revenue

source: Lotame global survey report "Beyond the Cookie Part 2" (October 2021)

03

deterministic data, probabilistic data, matching & encryption

deterministic & probabilistic matching

deterministic data

We align to the IAB Tech Lab view that identifiers come in 3 types - consumer, creative assets, and the business entities types of involved in the supply chain.

Deterministic data provides a reliable foundation for marketing operations as it is based on factual variables or declared consumer inputs, and a key advantage of deterministic matching is the resulting high degree of accuracy. However, not all applications and websites require users to login or provide specific information and it can lack scale for smaller publishers.

probabilistic data

Probabilistic matching isn't as accurate as deterministic matching but can utilise deterministic data sets to help refine the algorithmic efforts and improve the accuracy of insights.

One of the core advantages of using probabilistic matching over deterministic matching is scale, as you don't need to collect authenticated email addresses or other pieces of personal data to be able to identify them across different devices. It's also safer from a consumer privacy perspective. However, there are some disadvantages such as the accuracy of any resulting outputs and the lack of transparency in matching methodologies, as any algorithms used are often proprietary. This is especially valid if you are relying solely on probabilistic matching to identify, track, and target users across different devices and applications.

deterministic & probabilistic matching

deterministic data

The most prevalent method to deterministically match users is via email addresses.

Emails tend to be unique to consumers and can be identified and matched across a very wide range of data sets. Large data owners such as popular platforms (Facebook, Twitter, LinkedIn etc.) can deterministically match with ease, as they regularly require users to sign in with an email address and authenticate to access their services via various devices. Most vendors will regularly provide their overall match rates - and some may provide customisable match algorithms or confidence scores highlighting how likely the matches are accurate, based on their specific firstparty customer data and data quality profiles.

probabilistic data

Probabilistic data is data based on behavioural events such as online browsing behaviours and click-throughs.

Probabilistic data can be analysed and grouped by the likelihood that a user belongs to a certain demographic, socio-economic status or class. Algorithms are often leveraged to help in these processes and interrogate these behavioural patterns, device types and touchpoints to generate inferred interests or help to determine the probability of the user's age, gender or socio-economic status.

general top-level guidance for industry

- 1.** Thoroughly review your strategic requirements, both in the short and medium-long term
- 2.** Fully review and understand the data assets that you have access to. Consider whether you will need to leverage 2nd & 3rd party audiences
- 3.** from elsewhere - or if you have enough scale and quality to leverage only your own 1st party assets.
- 4.** Collaboratively agree upon the product & technical capabilities required to achieve your aims & work with your current technical vendors to understand their capabilities.
- 5.** Ensure that you consider both the technical capabilities required as well as scale, as both will be important in practice for the future.
- 6.** Consider fully reviewing any other options in-market that could meet your defined needs, benchmark your current solutions and have competent experts assess the options
- 7.** Consult fully on all of the related privacy requirements, future risks and considerations, across all the markets you are active in - both now and on an ongoing basis moving forwards.

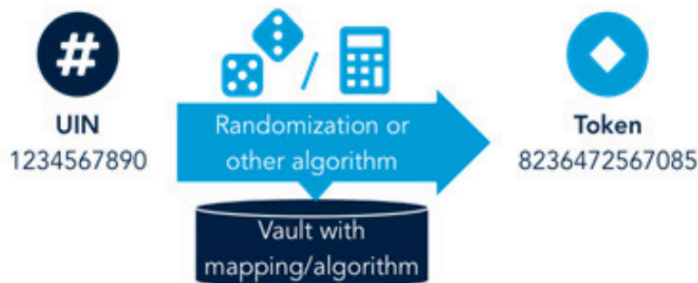
tokenization vs. encryption.

tokenization

increasingly it is becoming clear that legislators are taking very seriously the potential risks related to both the exposure and breach of any PII in the ad tech eco-system. As a result, the Tokenization of ID's is being seen as more future proof approach.

Both tokenization and encryption obscure personal data – however, tokenization is potentially operationally simpler and cheaper to implement than encryption, as decrypting the data isn't required in order to use it. Platforms such as Infosum and Karlsgate are examples of vendors enabling this approach and Unified ID 2.0 is preferring this approach as an ID solution.

Tokenization replaces personal data



- The only way to recover PII is through the vault (makes exchange difficult)
- In case of a breach, token provides no meaningful information
- Preserves format and functionality of data (i.e., tokens can be searched, viewed, etc.)
- Only works with structured fields (e.g., numbers text fields, etc.)

Encryption hides personal data



- Anyone with the key can decrypt the data (makes exchange easy)
- In case of a breach, encryption can be broken through brute force attacks
- Does not preserve format or functionality of data (e.g., it must be decrypted to view, search)
- Can be used to protect files and documents, in addition to structured fields

image source: The World Bank Group

04 iab tech lab id solutions guidance

iab tech lab id solutions guidance

The IAB Tech Lab Addressability Working Group published the initial version of the ID Solutions Guidance in late 2023 and updated the details therein in early 2024.

The guidance has been designed as an informational guide for advertisers, publishers, media agencies, data collaborators, & ad tech vendors to help simplify the landscape and better understand the scope and scale of ID solutions and the related technologies, so that they can evaluate different ID Solution partners.

The 3rd party cookie is historically the most widely utilised identifier available on web browsers, but this has already been disabled by Apple Safari browser and the Mozilla Firefox browser - and Google Chrome has also committed to at least giving consumers the option of opting out of their usage sometime in 2025. The other commonly used identifier was MAIDs (Mobile Advertising ID) for example the ID for Advertising (IDFA) from Apple iOS. While MAIDs are still available - app environments are taking actions to restrict their availability and usage. Apple's App Tracking Transparency feature (ATT) was released in 2021 and is a requirement for users to opt in for use of IDFA - and has already reduced availability down to between 30-40% on average in Australia depending upon the app. Google Android may well look to introduce similar restrictions in the future.

Overall, these developments result in the ongoing deprecation of the capability to identify consumers due to signal loss. Which means:

- A loss of cardinality in non identifier based signals, e.g. proxying IP address, simplifying User Agent, referrer URL deprecations.
- A need for development of alternative technologies and methods to identify consumers across the open internet. Identity (ID) solutions have emerged as a new category of technologies that enables advertisers and publishers to create personalised consumer experiences.

It's important to note that ID solutions enable universe to universe matching as:

- ID solutions provide real time audience activation, bidstream augmentation, campaign optimisation and frequency capping capabilities.
- ID solutions help with calculating reach, understanding audience insights and trends and determining attribution for campaign conversions.

iab tech lab id solutions guidance

The key content sections to the ID guidance are below, and each is exceptionally detailed and very thorough:

- Introduction: Why Identity Solutions
- What are Identity Solutions
- How are Identity Solutions used
- How are Identity Solutions Enabled
- How to Evaluate an Identity Solution
- How to determine ID Solution success

We have summarised a couple of the key elements of the content to highlight examples of the content for you to consider, but highly recommend accessing the full guidance via the link below:

<https://iabtechlab.com/wp-content/uploads/2024/05/Identity-Solutions-Guidance-FINAL.pdf>

how identity solutions are commonly used

Insights and Campaign Planning

For a marketer, understanding when and where they can find consumers who are likely to purchase their product or service is critical. Since ID solutions identify unique consumers across different channels of advertising, they can underpin all aspects of campaign planning namely:

- Universe-to-Universe Matching to uniquely match audiences between two companies, typically buyer and seller audiences in advertising.
- Audience Discovery to find new audiences matching buyer requirements.
- Pre-campaign Insights for e.g. total reach for marketer's target audience and past performance.
- Media Mix Modeling (MMM).

iab tech lab id solutions guidance

how identity solutions are commonly used

Targeting and Activation

Reaching households/users/devices within a target audience segment requires an identity “currency” to associate audience attributes with site traffic to match against an audience segment. Identifying traffic on a publisher website and connecting to an advertisers’ targeting audience can be powered by IDs provided by Identity Solutions.

- Audience Activation refers to capability to buy or sell impressions for a given audience segment.
- Bidstream Augmentation where third party providers are added to bid stream to resolve available IDs and enrich the data for bid decision maker.
- Campaign Optimization to control and direct advertising spend where it is most effective and has highest return.
- Fraud Detection to stop ad buys on suspected invalid traffic sources.

Reporting and Attribution

Having access to unique user IDs is extremely helpful in several reporting and attribution purposes. Accurate post-view and post-click attribution conversion reporting requires understanding each unique consumer’s actions. Availability of an ID for each consumer lends to the accuracy of reporting and calculations on households/users/devices “exposed” to the campaign ads. IDs provided by Identity Solutions can underpin several aggregation metrics, and reach and frequency calculations, alongside other analytics for advertising campaigns.

- Campaign Reporting like total reach and frequency.
- Audience Insights & Trends.
- Attribution to understand who viewed and clicked the ad and where as well as which actions resulted in a purchase.

Note: While ID solutions can help achieve the above outcomes, organisations should still fully assess each ID solution they intend to use, and ensure that their particular needs are met.

05

working examples for both buyers & sellers

working examples for both buyers & sellers

how identity solutions are commonly used

Below are two visual example workflows from the guidance demonstrating how user IDs can be propagated and used by players in the digital ad supply chain.

Buy side Audience Activation via an SSP using Deal IDs:

This option is commonly used when a publisher or advertiser wants to activate their audiences using an ID solution provider, but the DSP they are using does not yet support their chosen ID solution.

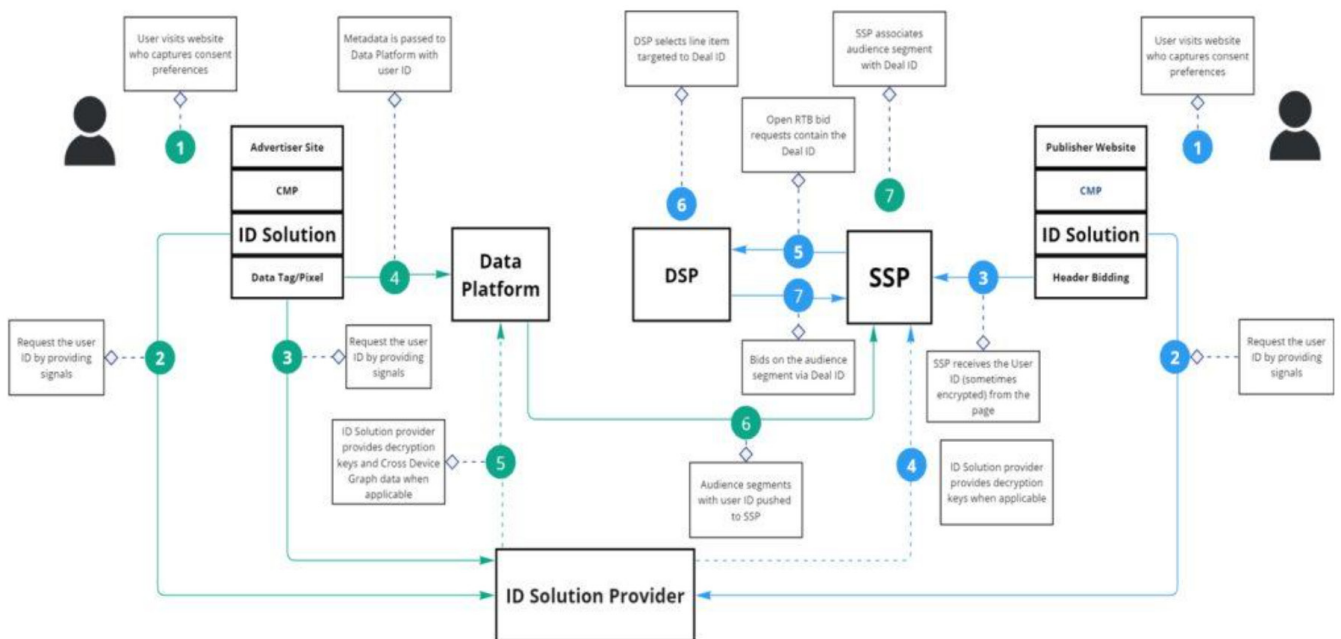


image source: IAB Tech Lab

buy-side user id distribution & activation - steps

- User goes on to an advertisers' web page or application.
- Where applicable, the advertiser captures the user's consent preferences and makes them, along with other signals including hashed email, IP address etc available to the ID provider. The ID provider responds with a user ID which the advertiser stores client and/or server side.
- If the advertiser is working with a data platform, the data platform can call the ID provider and retrieve the user ID.
- The user ID can either be used as a basis to build audience segments or alternatively stored alongside the data platform's own first party user ID and used to communicate segments to their ad tech partners.
- If applicable, the data provider can retrieve decryption keys from the ID provider to decrypt the ID.
- The Data Platform can push audience segments alongside the ID provider's user IDs to a SSP. This is commonly via file transfer or server-side API.
- The SSP/publisher associates a deal ID with the segment.

sell-side user id distribution & activation - steps

- User goes onto a publisher's web page or application.
- Where applicable, the publisher captures the user's consent preferences and makes them, along with other signals such as hashed email, IP address etc available to the ID provider. The ID provider responds with a user ID for consenting users.
- The SSP picks up the user ID.
- The SSP retrieves the decryption keys from the ID provider where applicable and decrypts the user ID and assesses whether any deals are eligible.
- SSP sends the encrypted user ID and applicable deal IDs in the OpenRTB bid request to the DSP.
- The DSP evaluated the eligible campaigns to serve.
- The DSP returns a bid response to the SSP.



buy-side audience activation in a dsp

This example demonstrates how an advertiser or brand can use an identity provider to activate their audience in a DSP e.g. a retargeting campaign. The approach would be similar for a publisher using a DSP to execute an audience extension campaign.

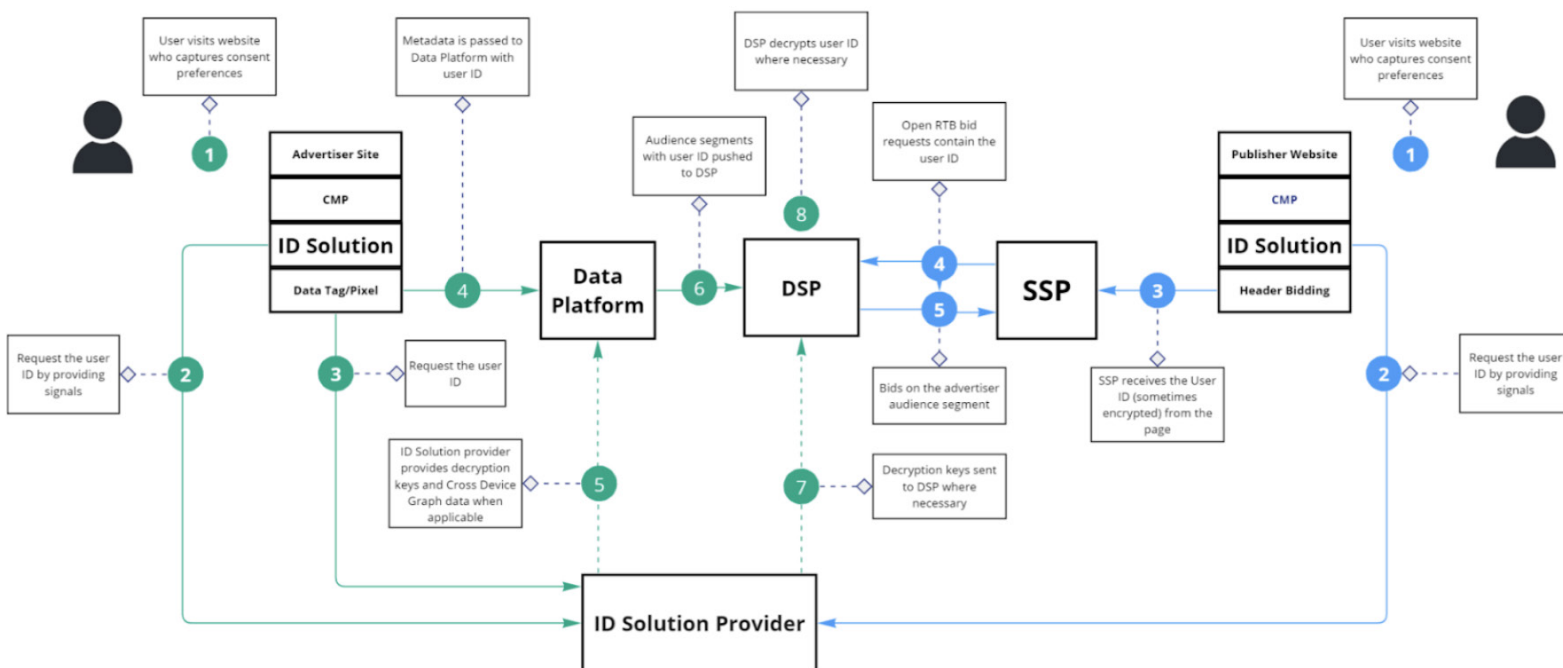


image source: IAB Tech Lab

buy-side user id distribution & activation - steps

- User goes on to an advertiser's web page or application.
- Where applicable, the advertiser captures the user's consent preferences and makes them, along with other signals including hashed email, IP address etc. available to the ID provider. The ID provider responds with a user ID which the advertiser stores client and/or server side.
- If the advertiser is working with a data platform, the data platform can call the ID provider and retrieve the user ID.
- The user ID can either be used as a basis to build audience segments or alternatively stored alongside the data platform's own first party user ID and used as a means to communicate segments to their ad tech partners.
- If applicable, the data provider can retrieve decryption keys from the ID provider to decrypt the ID.
- The Data Platform can push audience segments alongside the ID provider's user IDs to a DSP. This is commonly via file transfer or server side API.
- The DSP can retrieve decryption keys from the ID provider if applicable.
- The DSP can decrypt the user IDs sent both in the bid request and also from the Data Platform and determine which campaigns are eligible to serve and subsequently return a bid response.

sell-side user id distribution - steps

- User goes onto a publisher's web page or application.
- Where applicable, the publisher captures the user's consent preferences and makes them, along with other signals such as hashed email, IP address etc available to the ID provider. The ID provider responds with a user ID for consenting users.
- The SSP picks up the user ID and passes it to the DSP in an OpenRTB bid request.
- The DSP returns a bid response to the SSP.

To access the IAB Tech Lab ID Solutions guidance please simply click the link below:

click to jump →

06 **consolidation of PAIR & OPJA protocols**

iab tech lab pair protocol

The PAIR (Publisher Advertiser Identity Reconciliation) is a privacy-centric approach which has recently been donated by Google to IAB Tech Lab in 2024 in order to enable advertisers and publishers to reconcile their first-party data for advertising use cases without the reliance on third-party cookies. PAIR relies on commutative cryptography which makes it possible to match the multiple-encrypted join keys (IDs, PII) without decrypting to cleartext. This is particularly powerful as a means to interoperate between clean rooms owned by different administrative parties.

The original version of PAIR was released by Google in late 2022 - and was originally designed (as per the image below) to give advertisers the ability to more closely connect with their known audiences through DV360, while avoiding tracking individuals across the web.

publisher advertiser identity reconciliation PAIR workflow

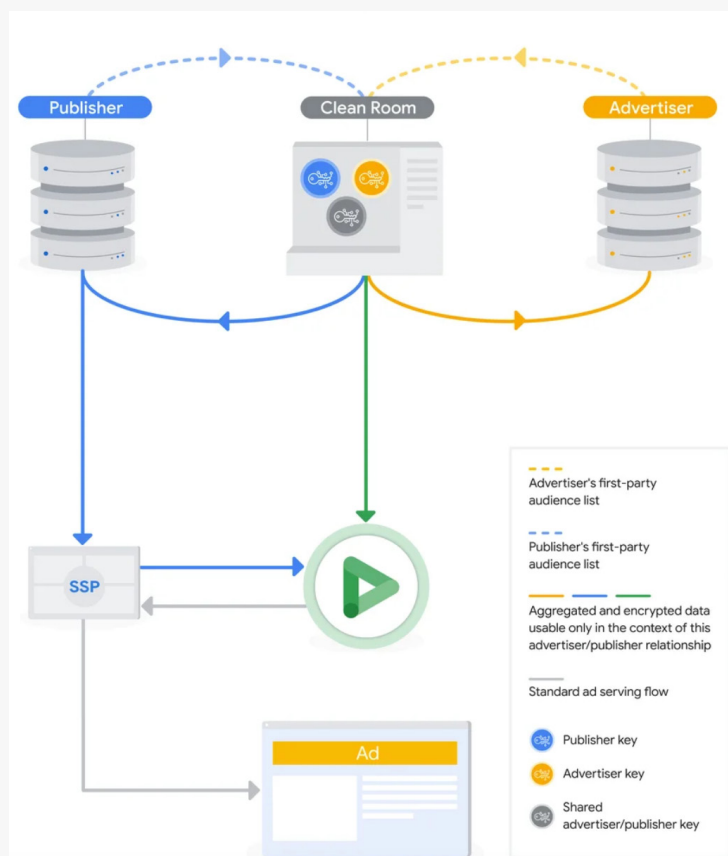


image source: Google

iab tech lab pair protocol

the coming together of opja and pair

In 2023 IAB Tech Lab published the Open Private Join & Activation (OPJA) specifications to help standardise the process for private and secure first-party data matching and using the results in programmatic advertising.

Both OPJA and PAIR aim to enable publishers and advertisers to match their first-party audiences and then to use OpenRTB to activate them with the help of SSPs and DSPs. However, OPJA stores encrypted labels with the SSP - whilst PAIR stores encrypted identifiers with the DSPs.

Moving forwards, IAB Tech Lab PAIR will be the only IAB standard moving forward and it will be governed by the shared design goals of both OPJA and PAIR. These updated and aligned protocols were released in late September 2024 in draft for public comment until 25th October 2024, and will be governed by the shared design goals of both OPJA and PAIR as per the below:

Design Goal 1: Security of Personally Identifiable Information. The solution protects the end user's PII data throughout the operation using cryptographic protection. No participant in the data exchange (e.g., publisher or advertiser) can act alone to access or exfiltrate cleartext sensitive information.

Design Goal 2: Privacy of User Identity. The solution prevents each participant from learning the identity of end users that are not part of their own contributed input data set.

Design Goal 3: Privacy of Audience Membership. The solution prevents each participant from learning which end users they contributed are members in the computed overlap. It should be difficult or impossible for the real-time bidding stack (e.g., SSP and DSP) from reverse engineering user identities in a particular audience.

Design Goal 4: Privacy of User Context. The solution limits or eliminates cross-learning between publishers, advertisers, and the real-time bidding stack. Information that was learned about a user in one context can not be used in another.

IAB Tech Lab PAIR will describe the data clean room processes and the privacy enhancing technologies (PETs) that enable a matching operation between two parties, as well as the supporting mechanisms for using the output of the operation to activate matched audiences in programmatic advertising.

iab tech lab pair protocol

industry considerations & needs

The ongoing decline in the availability of traditional identifiers like third party cookies to identify consumers and personalise advertising disrupts the necessary use cases of growth marketing to sustain and grow advertising spend by advertisers. At the same time this has far reaching consequences for publisher revenues and implications for advertising technology providers.

Advertisers and Marketers - need to keep engaging current and potential customers who have engaged with their brands as well as any potential new customers. They want to use their authenticated first party data to reach these consumers across different media channels. In order to do so in a privacy-safe manner will be critical moving forwards in order to uphold their privacy policies and protect their customer's data whilst still maintaining a competitive advantage.

Publishers and Media Owners - need to keep growing revenues whilst improving user experiences, consumer privacy and security. As advertisers pay more for authenticated consumers, it has a direct impact on publisher revenue. Publishers will want to maintain competitive advantage by not leaking their data to others while transacting in the programmatic supply chain. Publishers also have concerns about data leakage when sharing conventional identifiers like device IDs or IP addresses in bid requests, a risk that persists with certain universal identifier solutions. If a DSP or advertiser can obtain any such identifier usable across various publisher inventories, the construction of audience segments leveraging increasingly valuable first-party data sets from publishers becomes feasible. Hence, publishers have reservations about permitting the targeting of their first-party data elsewhere, PAIR effectively mitigates this risk by ensuring that advertisers cannot access valuable first-party publisher data. While PAIR boasts universal operability across all devices, the identifiers generated with PAIR function solely within a single publisher/ advertiser relationship, making it inapplicable beyond that specific context.

Ad Technology companies - need to continue to support their customers to find the right audiences at the right time. The ongoing loss of traditional identifiers requires that advertising technology platforms and data providers look for ways to continuously evolve how they facilitate personalisation and audience-targeted programmatic advertising. This can be achieved by providing more robust methods and techniques for audience targeting to their sell side and buy side clients whilst also delivering on the obligations related to both privacy and performance.

iab tech lab pair protocol

why use pair

PAIR enables advertisers to use their first-party data to activate matching audiences that they have in common with publishers using advanced cryptographic encryption methods (in particular, without the use of third party cookies and without either side sharing its raw audience data with the other side).

Outcome-oriented benefits include:

- The ability to continue to support valuable targeting workflows.
- Improved reach for existing audience amid a shifting privacy landscape.
- Use across multiple SSPs.

Data protection benefits include:

- Control over first party data by preventing:
 - Data pooling
 - Data leakage
 - Insights leakage
- Raw first-party audience data is protected by privacy enhancing technology that leverage advanced encryption methods.

how pair works

The PAIR protocol leverages an encryption process where an input string has consecutive encryption keys applied to it, e.g. a publisher key 'Kp' and Advertiser key 'Ka'. In this process, regardless of the order in which the keys are applied, the output string remains the same so it can be used for matching purposes.

iab tech lab pair protocol

the pair process

PAIR protocol implementation has two distinct steps:

Offline: This is carried out in a Data Clean Room where the commutative cipher process is carried out to create a list of audiences to be used for activation in the programmatic supply chain. (steps 1-9 below)

Online: This is the use of an audience list created as a result of the offline process in bid request and bid response by the publisher and advertiser using their vendors - Supply Side Platform (SSP) and Demand side Platform (DSP). (step 10 in the table below)

Below is a very brief outline of the protocol, roles of Advertiser, Publishers, SSP, DSP and Data Clean Room. The protocol documentation (once released by IAB Tech Lab) will describe each of these in much greater detail as well as the data clean room operations, key generation, matching process, APIs for interoperability and privacy & security considerations.

Step 1: Setup

Step 2: Encryption Key generation

Step 3: Generate Advertiser and Publisher encrypted identifiers

Step 4: Share encrypted lists

Step 5: Data Clean Room generates the PAIR ID

Step 6: PAIR Lists shared

Step 7: Data Clean Room generates matched identifiers

Step 8: Evaluate Match Rates

Step 9: Publisher ID shared with DSP

Step 10: Programmatic Activation

iab tech lab pair protocol

PAIR considerations: security, privacy, scale

The PAIR protocol will be a privacy centric approach that uses the first party data including personal information of consumers from advertisers and publishers and involves sharing the data in a Data Clean Room as well as with other participants of the programmatic supply chain like DSP and SSP. The use of a commutative cipher provides the initial foundations for security and privacy in the protocol, with much more to come.

The overall intention of this initiative is to develop the PAIR protocols it into an open standard that enables interoperability between data clean rooms and allows all DSPs to adopt the protocol for enhanced privacy-safe audience targeting. As part of this effort, IAB Tech Lab will be updating the PAIR prebid module so it can be leveraged by all Data Clean Rooms and DSPs, as well as publishing open-source reference implementation to support adoption by publishers.

We also expect OPJM standards to be released by IAB Tech Lab for measurement and attribution sometime in late Q4 2024. As the industry continues to shift towards privacy-safe solutions, IAB Tech Lab remains the key global source for addressability standards that help advertisers and publishers adapt and thrive. IAB Australia will continue to work hard to keep local industry and our members fully updated on these types of critical technical updates through blog articles, handbooks, explainers and our in-person events.

To access the PAIR protocol simply visit by clicking link below

click to jump →



[click to go to
index page](#) →

07 **openRTB id provenance**

openrtb - id generation provenance & clarification

More recently some SSPs and publishers have been leveraging probabilistic mechanics to link disparate devices to a single individual, without having a direct identity linking them together. This 'bridging' methodology can be used to apply DSP user IDs to requests from browsers that do not have 3rd party cookies enabled.

Amid signal loss in the programmatic market, bridging has been used to help maintain addressability as a privacy-safe process used to match publisher first-party audience identity signals with static signals from second parties to help provide further insights into audiences. This subset of ID resolution is key as digital advertising heavily relies on these signals.

Historically however, DSP IDs have only been pinned to a cookie. Any bridging of IDs from a cookie-enabled browser to another browser, no matter how reliable the methodology, is not in-line with traditional programmatic buying expectations - who will usually expect a single, 1:1 cookie sync process between an upstream partner and downstream (DSP) partner.

Most ID service providers are fully transparent about their methods, collaborating with industry players and defining specific identifier formats. This ensures that DSPs and buyers can understand the nature of the identifiers used. However, not all vendors may follow these practices. Some industry observers have raised concerns about the discrepancy between the ID in the bidstream and the ID on the browser. Without transparency into how the bidstream ID is derived, buyers and buy-side platforms cannot accurately model attribution and optimisation.

Hence, IAB Tech Lab have worked to update the OpenRTB specs (without disabling bridging) to ensure that buyers have the ability to see where it's happening. It was clear that improved transparency on identifier sourcing and application within the bidstream was required. Specifically, the industry demanded explicit declaration of id sourcing versus inferring patterns by historical id enrichment or offline agreements between partners. Unanimously publishers and their partners acting in good faith are more than happy to provide this level of transparency.

openrtb - id generation provenance & clarification

For any non-traditional cookie syncing behavior, the updates extend the eid object to ensure that any identifier listed within the object includes the necessary provenance details, such as eid sourcing methodology and which entity set the eid. These declarations provide explicit transparency beyond what is currently found in the eid object. With this change, the ID Provenance sub-group, an offshoot of the Programmatic Supply Chain Working Group also proposed the buyervuid object remains explicitly used for browser-based cookie sync values between the buyer and seller unless other arrangements have been explicitly agreed to, and all other methods of id settings and retrieving should be specified with the eid payload.

Unless prior arrangements have been made between the buyer and the seller directly, the value in the 'user.buyervuid' field is expected to be derived from a real time cookie sync and value in device.ifa field is expected to be derived from an advertising ID call to the Operating System. For an Exchange to properly disclose that an ID substitution has occurred by a publisher, they must propagate the Match Method (mm) value, as sent by the publisher, on the Extended Identifier (eid) they send to the DSP, regardless of how the SSP determined the DSP's ID.

If a linkage is made by any party (e.g. a SSP to a DSP cookie ID) based on an incoming EID where mm does not equal 1 or 2, then the ID sent to the recipient must inherit the mm value of the incoming Extended Identifier (EID). For example, if a SSP receives an ID based on any kind of matching (mm values 3,4,5,6), then even if the ID they send to the DSP is based on a cookie exchange, it must also indicate that matching occurred (i.e. mm values 3,4,5,6).

openrtb - id generation provenance & clarification

match methods

Enum	Value	Definition
0	Unknown	Unknown
1	No Match	The associated ID came directly from a 3rd-party cookie or OS-provided resettable device ID for advertising (IFA). No matching has occurred.
2	Browser Cookie Sync	Real time cookie sync as described in Appendix: Cookie Based ID Syncing
3	Cross-Domain/Authentication	ID was derived from linkage based on user authentication across multiple browsers, applications and/or devices (e.g. email or hashed PII)
4	Cross-Domain/Device Inference	ID is inferred from linkage based on non-authenticated features across multiple browsers or devices (e.g. IP address and/or UserAgent)
5	Property-Specific Authentication	ID pertaining to a user on a single web property (e.g. GUID, SharedID, user login or other hashed PII) or application (this may include session IDs) on a single device
6	Property-Specific Inference	ID pertaining to a user on a single web property that was derived from a linkage based on non- authenticated features or provided by any party that is NOT the device OS or application, corresponding to a single device (this may include session IDs)
500+	Vendor Specific	

Items in the EID array with mm values of 1 or 2 are generally optional/informational, but some buyers may find it useful for sellers to provide them.

For more information and to access the latest Open RTB specs click the link below:

[click to jump →](#)

openrtb - id generation provenance & clarification

best practices for disclosing ID matches

The updated specs contain three new fields to show which company has created a bridged ID, which vendor inserted the ID and which has enabled the match:

inserter

The party that's putting the ID into the bid request.

Typically a Publisher or an SSP. In other words, the party that made the decision to put the id in the bidstream. In the case of header bidders, the inserter is the Publisher.

source

The party that defined/created an ID. In the case of universal or alt-IDs, it's the domain of the party who defined/created the ID itself.

In the case of cookie IDs, it's the domain of the party who the cookie belongs to.

matcher

The party that created the match included in the ID array, this could be a device graph vendor, or the publisher themselves

The March 2022 release of OpenRTB 2.6 promoted a popular extension for Extended Identifiers (EID), to the mainline of the specification. The Extended Identifiers object can contain one or more IDs from a single source or a technology provider. In early February 2024, the IAB Tech Lab created a workstream across SSPs, Publishers, DSPs, ID providers, and others to define updated standards this kind of transparency requires. The OpenRTB updates aim to explicitly codify how the market operates today, in addition to supporting future scenarios where a seller may provide multiple Extended Identifiers, and a buyer can bid based upon their preferences.

For more information and to access the latest Open RTB specs click the link below:

click to jump →

iab tech lab

transparency standards

IAB Tech Lab has recently released draft specs to enable yet further transparency to the supply chain by enabling publishers, agencies and brands to declare the identity services they work with. The approach aligns with the other transparency standards, in the .json file being stored at the root domain for easy manual access by humans and readable by machines & crawlers (as you can with ads.txt, sellers.json and buyers.json). By knowing exactly which identifiers are used by which publishers, id-sources.json should help provide greater clarity into ID adoption. Brands and agencies could map out which publishers work with which identifiers and match these against their own audiences, which will themselves be associated with different identifiers. This will help them figure out where in the publishing landscape they can locate their addressable audiences.

the id-sources.json standard aims to:

Provide a standard way for companies to declare which user identity sources they use. Work like the other supply-chain transparency standards as a participant hosted, structured declaration that machines can read. Ease ad campaign execution between advertisers, publishers, and their chosen technology providers by making it explicitly clear who supports what.

For the full set of specifications simply [click here](#)

click to jump →

08 **considerations for buyers & sellers**

considerations for buyers & sellers

We've included some considerations here for both buyers and sellers should you be in the process of assessing an ID vendor for your needs. Feel free to see this as a practical checklist as you go through the process.

consent and privacy:

It is critically important to understand how your ID provider will help you comply with any evolving regulatory requirements of privacy and relegated regulations, as well as how they prioritise consumer transparency and controls. Always perform full due diligence with respect to your regions of operation and your own privacy policies.

Some suggested questions for ID vendors are:

- Does the ID solution provider have a privacy policy?
- What are the governance and control structures and mechanisms deployed by the ID Solution provider?
- Does the ID solution privacy policies, governance and control mechanism align with your privacy policy?
- How does the solution ensure that consumers' privacy preferences are respected in the advertising value chain? What guardrail have they deployed for this purpose?
- How does the solution support data subject rights requests e.g. data deletion?
- Does the ID solution provider deploy privacy enhancing technologies (PETs) in their processing of user IDs thus preventing unauthorized de-identification or reverse engineering of user personal information?

considerations for buyers & sellers

quality

The quality of an ID solution can be assessed in a number of ways based on identifier characteristics as well as ID solution provider capabilities. Consider the below capabilities in your assessments:

id lifetime

Is the average and lifetime distribution of the user IDs provided by your solution adequate to fulfill your use case? For example, if you are using an ID provider to build an audience that you want to target with an ad campaign with a given frequency cap over a 30 day period - is the average lifetime of the user ID sufficient for you to achieve your goal?

precision

Precision is a measurement of how many user IDs are given to the same user ID. This may be a browser based ID, people based ID depending on the provider. This is a subjective measurement since it will depend on what truth set the ID provider is being evaluated against but learning more about an ID provider's own precision metrics and truth sets may inform your decision.

id graph stability

Graph stability is an important consideration when evaluating an ID solution. If a user ID moves from one Individual ID to another or indeed an individual moves from one household ID to another, this can negatively impact use cases such as targeting, optimisation and measurement. Whilst some movement is expected, it is recommended that you discuss graph stability with your ID solutions provider.

interoperability

This is a key consideration when choosing your ID solution. A key question to ask is whether the ID solution is adopted by your key strategic partners or will it open the door to new partnerships?

Since IDs are a currency to communicate user identity through the digital ad supply chain, it is recommended to review vendors that have the capability to translate or decode these IDs into a language that is understandable by yourself and your strategic partners. This will ensure increased reach and scale for advertisers and effective monetisation for publishers.

scale & adoption

Advertisers should consider the publisher adoption of an ID Solution since that dictates the addressability of the global digital audience. It is important to evaluate whether the ID Solution has sufficient scale in the channels and markets that you operate in. Publishers should also consider the buy side adoption of an ID Solution. Will implementing the solution make your audience more addressable to your strategic buy side partners and bring new ones therefore increasing bid density and yield?

considerations for buyers & sellers

costs

Most ID solution providers are free for publishers looking to distribute user IDs across their user base or enrich bid requests to improve scale of addressability. Vendors that want to make use of a real time ID, access an identity graph or associated real time services, are generally charged either a subscription model or usage fee. Commonly a monthly fee is charged with the amount reflective of the products or services the vendor is subscribing to.

Usage based fees is when a fee, often based on a CPM value, is charged based on usage. Usage is calculated based on how many times the ID solution service was used and can thus depend on the use case, e.g. how many times an ID Solution service was used to inform a buying decision. Additionally, costs of an identity solution may be absorbed into an audience targeting CPM attached to a media campaign. Separate vendor agreements or fees may not be applicable for buyers in this case.

data leakage

One critical concern for publishers has been that of data leakage. Publishers may want to consider whether their ID solutions provider can protect them from data leakage. For example, perhaps the ID solution may be able to empower the publisher to control which vendors are able to access user IDs on their properties

publisher yields & improved consumer experience

Whilst an increase in overall revenue and CPM yields will always be the ultimate criteria for publishers in evaluating any new investment in technology, there are some other measures that can be monitored to start assessing the success of an investment into ID solutions.

Publishers might have to work with the supply side platform partners and exchanges to help them gather these insights, alternatively, some ID Solutions offer analytics tools such as a prebid analytics module that can help gather some insights. Look to measure the incremental improvement with programmatic auctions that include an ID Solution on downstream match rates, fill rates and yield improvements.

Examples of improved yields come from increased:

- Average Bid CPMs
- Average Winning Bid CPMs
- Bid Density (Valid Bids/Auctions)
- % Bid Response Rate

Lastly, try to measure impacts on user experiences such as site load or bounce rate and look to review any new demand partners added due post ID solution integration.

considerations for buyers & sellers

beyond ad buying returns

While ROAS and ROI remain the ultimate measure of success for advertisers, there are some key operational criteria and measures that can be monitored for reviewing future success with an ID Solution.

Look for improved targeting and activation metrics including higher addressable audiences, better match rates and improved de-duplicated incremental reach.

Operationally, frequency management and optimisation should be much improved and for measurement metrics look for incremental conversions, higher ROAS, brand lift & VCR and also a reduction in any fraud/IVT data from your verification partners.



click to go to
index page →

09 id matrix

identity providers

provider	id solution	Primary Utilisation	Data Sources	Base Identifiers	Consent Type	Availability & Addressability	Interoperability	Prerequisites
AdFixus	AdFixus Identify	Syncs anonymous users into a common and durable 1st-party cookie.	Global publishers & advertisers	Deterministic, decentralised, double encrypted data	1st party unauthenticated and consensual	Yes, via AdFixus Match Room	N/A	Majority ownership of domain/s
Adform	Adform ID Fusion	Connects all types of identifiers - first-party IDs, cookies, UIDs, MAIDs, PPIDs across both web and in-app	Global publishers, advertisers & data suppliers	Probabilistic & deterministic data	Authenticated & consensual 1st party	Yes, via Adform DSP and SSP	Yes	Adform DSP and/or SSP
Azira	Azira ID	Universal identifier across both web environments and in-app.	Global publishers + online & offline data partners	Hashed emails, phone numbers and postal addresses	1st, 2nd & 3rd party	Yes, via Azira Allspark	Yes, via Azira Allspark	Must have a common identifier within any datasets
Criteo	Criteo Shopper Graph	Connects shopper IDs with commerce data.	Global publishers, advertisers & data suppliers	Probabilistic & deterministic data	1st, 2nd & 3rd party	Yes, via Criteo Media Platform	Yes via RampID & Unified ID 2.0	Participation in Criteo's First-Party Data Collective
ID5	ID5 Universal ID	Universal identifier across both web environments and in-app.	Global publishers	Probabilistic & deterministic data	1st, 2nd & 3rd party	Global ad tech	Via Unified ID 2.0 in EU (not in ANZ)	Can meet GDPR compliance requirements
InMobi	UnifiD	Enables identity resolution for mobile app publishers and developers.	Global publishers & data suppliers	Probabilistic data	2nd & 3rd party	Yes, via all major DSPs & SSPs	Via Unified ID 2.0	Ability to sync
LiveRamp	RampID	Universal identifier across both web environments and in-app.	Global publishers & data suppliers	Hashed emails & phone numbers	1st, 2nd & 3rd party	Yes, via all major DSPs & SSPs	Interoperable with most global identifiers	Publishers must have access to user authentications
Lotame	Panorama	Probabilistic universal identifier across both web environments and in-app.	Global publishers & data suppliers	Probabilistic & deterministic data	1st, 2nd & 3rd party	Yes	Interoperable with most global identifiers	Ability to sync
Prebid	SharedID	Designed to support ways of establishing pseudonymous IDs for header bidding.	Global publishers & ad tech vendors.	N/A	1st, 2nd & 3rd party	Yes	Yes	Requires prebid.js integration
Unified ID 2.0	Unified ID 2.0	Open source universal identifier across both web environments and in-app.	Global publishers, advertisers, data providers and DSPs.	Salted and hashed email or phone number.	Authenticated and consensual 1st party	Yes	Interoperable with most global identifiers	Must agree to abide by UID2 ecosystem terms. Source code donated by The Trade Desk
Yahoo	ConnectID	Universal identifier across both web environments and in-app.	Owned & Operated and Partners	Hashed emails, hashed phone number, tokenised	1st, 2nd & 3rd party	Yes, via Yahoo DSP & major SSPs	Interoperable with most global identity providers.	Publishers implement directly, via SSP or LiveRamp. Brands use 1PD via an ID provider.

audience matching tools

provider	Audience Matching Platforms	Primary Utilisation	Data Sources	Base Identifiers	Consent Type	Availability & Addressability	Interoperability	Prerequisites
Google	Customer Match	Enables audience creation & targeting across Google’s platforms.	Owned & Operated	Hashed PII	Authenticated & consensual 1st party	Search, Shopping, YouTube, Gmail & GDN	N/A	All Customer Match customers are vetted with very clear requirements
Meta	Facebook Custom Audiences	Enables audience creation & targeting across Facebook and Instagram.	Owned & Operated	Hashed PII	Authenticated & consensual 1st party	Only across owned & operated	N/A	All Custom Audiences customers are vetted with very clear requirements
Microsoft	Microsoft Customer Match	Enables audience creation & targeting across the Microsoft Advertising Network.	Owned & Operated	Hashed PII	Authenticated & consensual 1st party	Microsoft Advertising Network	N/A	Active Microsoft Advertising account with administrator access to Customer ID & Account ID.
Salesforce	Salesforce Data Cloud	Connects agnostic identifiers to a common profile for downstream activation.	Global publishers, advertisers & data suppliers	Hashed PII	Authenticated & consensual 1st party	Yes, via clean room integrations & mutual Data Cloud connections.	Yes	Global publishers, advertisers, data suppliers stipulate integration preferences
Snapchat	Customer List	Enables audience creation & targeting across the Microsoft Advertising Network.	Owned & Operated	Hashed PII	Authenticated & consensual 1st party	Across Snapchat	N/A	Any customer data provided must be hashed using SHA-256 encryption.
TikTok	Custom Audiences	Enables audience creation & targeting across TikTok.	Owned & Operated	Hashed PII	Authenticated & consensual 1st party	Across TikTok	N/A	Minimum of 1,000 total matched users in a Custom Audience to use it in an ad group.



descriptions for the identity providers matrix

This matrix of ID providers has been collated and completed by the IAB Australia Data Council. An explanation of each of the columns and the information they contain is below:

provider	which entity owns the ID solution?
id solution	what is the product name of the ID solution, offered by the provider?
consent type	what is the relationship to the entity that has gathered consumer consent for the utilisation of these signals (i.e. is it a first, second and/or third party relationship)?
data sources	from where the data is sourced and what is the status of ownership?
availability and addressability	how, or within which types of activation platforms, is the solution made available for the purposes of addressability for the purposes of digital marketing?
base identifiers	from which types of identifiers are these solutions built upon?
interoperability	is this solution interoperable with other identity solutions in-market?
prerequisites	are there any requirements, limitations or considerations for potential customers that are reviewing this solution?
audience matching tools	specialised tools that enable clients to identify and target specific segments of their audiences using first-party data, allowing marketers to create custom audience segments to deliver targeted advertising to those segments across various digital channels.
primary utilisation	refers to the main or predominant use of data, resources, or platforms for advertising purposes.

[click to go to
index page](#) →

10 further reading

further reading

data advertising: state of the nation 2024

to reading →

data collaboration platforms explainer

to reading →

1st party data handbook

to reading →

iab tech lab - id solutions guidance

to reading →

iab tech lab pair - update

to reading →

id provenance in openrtb

to reading →

pair protocol (draft) for advertisers & publishers

to reading →

[click to go to
index page](#) →

11 glossary of terms

glossary of terms

first party data

this data is collected directly from consumers interacting with your assets, both online and offline. For example, in-store purchasing habits stored in a CRM or behaviours people exhibit on your website.

second party data

this data is collected directly from consumers interacting with your assets, both online and offline. For example, in-store purchasing habits stored in a CRM or behaviours people exhibit on your website.

third party data

is collected from an external source that doesn't have a direct relationship with the people it's collecting data about. For example, a third-party data company might pay publishers to put their pixel on their site and then use that information to piece together online profiles.

zero party data

is an increasingly used term for first-party data which consumers are intentionally and openly opting into sharing with business entities. Technically and legislatively, this remains first-party data and any distinction is effectively redundant, other than for product marketing purposes.

data clean rooms

these solutions enable businesses with legitimate access to large amounts of first-party data to safely and securely keep and update that information without directly accessing the raw data, negating the risk of ever exposing the consumer data. Thereafter, other companies (second parties) can bring their own data and campaign insights from one clean room and compare it with another, again without directly exposing customer data. Most companies offering clean rooms can also run machine learning modelling over data sets, giving advertisers actionable insights into their audiences without the personalised data ever being revealed.

glossary of terms

addressability

ability or extent of capability to uniquely identify, reach, and deliver personalised messages to specific individuals or audience segments across digital channels and devices.

audience activation

the process of connecting advertiser target audiences with publisher audiences for targeting through digital advertising channels

data leakage

the unauthorised or unintended collection and use of audience data by third parties, without the publisher's knowledge or consent.

identifier

a unique code or string used to recognise and track individual users, devices, or ad assets across digital platforms and channels. A unique value is assigned to a device, browser or user for associating with a unique person - or else to identify a group of devices and browsers or users and assign a unique value for associating a with a unique household.

identity graph

this links various identifiers associated with an individual consumer across different devices, channels, and platforms to provides a single unified view for real-time targeting and personalisation purposes.

match keys

match keys are unique values that can be used to join and match two different data sets. In digital advertising these are usually a consumer identifier.

PETs

privacy enhancing technologies (PETs) are technology solutions that use one or more of the privacy technologies (differential privacy, secure multi party compute and on device learning) to accomplish complex data processing functions in digital advertising without revealing the individual, household or device level personal information to parties that do not already have them. Data Clean Rooms are an active example of a PET.



[click to go to
index page](#)

