

## Identity Solutions

Guidance

Please email [support@iabtechlab.com](mailto:support@iabtechlab.com) for questions, public comments and feedback. This document is available online at <https://iabtechlab.com/idsolutions>

## About this document

In the programmatic ecosystem, identifying consumers across their various media interactions has been a keystone for marketers to find customers at scale across the global open web, supporting the growth of large and small publishers alike. Recent developments- both regulatory changes and actions taken by large platforms- operating systems and web browsers, have resulted in diminished availability of traditional consumer identifiers like 3rd party cookies and mobile identifiers e.g. Apple's ID for Advertising (IDFA).

This has created a need for development of alternative technologies and methods to identify consumers across the open internet. A new category of technology offerings called Identity (ID) solutions have evolved to address this need. As the use of ID solutions grows, the industry must understand what they are, how they are integrated into the workflows and what is their utility. This document describes:

- What are the different types of ID solutions and how do they differentiate
- What are the attributes of these ID Solutions
- A high-level view of how ID Solutions work
- A suggested framework for choosing and evaluating ID Solutions

This document is intended to be an informational guide for advertisers, publishers, media agencies, data collaborators, & ad tech vendors to demystify the landscape, better understand the scope and scale of ID solutions and the technology, so that they can evaluate different ID Solution partners.

This document is developed by the IAB Tech Lab [Rearc Addressability Working Group](#).

**Note:** *The use of words or phrases "Privacy", "Private", "Security", "Control", "Processing", "Personal Data", "PII" in this document is generic and does not refer to definitions in any specific regulation e.g. GDPR or CCPA.*

*Throughout the document the word or phrases "ID", "user ID", "Consumer ID", are used interchangeably referring to a unique identifier associated with a user of a service.*

### License

Identity Solutions Guidance and Recommended Practices document is licensed under a [Creative Commons Attribution 3.0 License](#). To view a copy of this license, visit [creativecommons.org/licenses/by/3.0/](https://creativecommons.org/licenses/by/3.0/) or write to Creative Commons, 171 Second Street, Suite 300, San Francisco, CA 94105, USA.

## **Significant Contributors**

Abhishek Sen, *NumberEight*; Anissa Connor, *ID5*; Brooks Dobbs, *The Trade Desk*; Chris Watts, *NumberEight*; Eli Heath, *Lotame*; Emma Raz, *NumberEight*; Giovanni Gardelli, *Yahoo*; Jamie Zoufal, *The Trade Desk*; Jay Rakhe, *Experian*; Keith Kilpatrick, *InMobi/Glance*; Melissa Ng, *Google*; Shabneez Khan, *InMobi/Glance*

## **IAB Tech Lab Lead**

Shailley Singh, EVP Product & COO, IAB Tech Lab

Miguel Morales, Director Addressability & Privacy Enhancing Technologies (PETs)

## About IAB Tech Lab

The IAB Technology Laboratory is a nonprofit research and development consortium charged with producing and helping companies implement global industry technical standards and solutions. The goal of the Tech Lab is to reduce friction associated with the digital advertising and marketing supply chain while contributing to the safe growth of an industry.

The IAB Tech Lab spearheads the development of technical standards, creates and maintains a code library to assist in rapid, cost-effective implementation of IAB standards, and establishes a test platform for companies to evaluate the compatibility of their technology solutions with IAB standards, which for 18 years have been the foundation for interoperability and profitable growth in the digital advertising supply chain. Further details about the IAB Technology Lab can be found at <https://iabtechlab.com>.

## Disclaimer

THE STANDARDS, THE SPECIFICATIONS, THE MEASUREMENT GUIDELINES, AND ANY OTHER MATERIALS OR SERVICES PROVIDED TO OR USED BY YOU HEREUNDER (THE “PRODUCTS AND SERVICES”) ARE PROVIDED “AS IS” AND “AS AVAILABLE,” AND IAB TECHNOLOGY LABORATORY, INC. (“TECH LAB”) MAKES NO WARRANTY WITH RESPECT TO THE SAME AND HEREBY DISCLAIMS ANY AND ALL EXPRESS, IMPLIED, OR STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, ERROR-FREE OR UNINTERRUPTED OPERATION, AND ANY WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. TO THE EXTENT THAT TECH LAB MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW. THE PRODUCTS AND SERVICES DO NOT CONSTITUTE BUSINESS OR LEGAL ADVICE. TECH LAB DOES NOT WARRANT THAT THE PRODUCTS AND SERVICES PROVIDED TO OR USED BY YOU HEREUNDER SHALL CAUSE YOU AND/OR YOUR PRODUCTS OR SERVICES TO BE IN COMPLIANCE WITH ANY APPLICABLE LAWS, REGULATIONS, OR SELF-REGULATORY FRAMEWORKS, AND YOU ARE SOLELY RESPONSIBLE FOR COMPLIANCE WITH THE SAME, INCLUDING, BUT NOT LIMITED TO, DATA PROTECTION LAWS, SUCH AS THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (CANADA), THE DATA PROTECTION DIRECTIVE (EU), THE E-PRIVACY DIRECTIVE (EU), THE GENERAL DATA PROTECTION REGULATION (EU), AND THE E-PRIVACY REGULATION (EU) AS AND WHEN THEY BECOME EFFECTIVE.

## Glossary

<i>Addressability</i>	Ability or extent of capability to uniquely identify an individual or a device between data sets of two or more parties in a given context e.g. targeting individuals with advertisements
<i>Audience</i>	Group of people with a common set of characteristics whom an advertiser wants to show an ad. More specifically this is a list or group of customers or individuals that is most likely to purchase a given product or service from an advertiser
<i>Audience Activation</i>	A process of connecting advertiser target audience with publisher audience for targeting them through digital advertising channels
<i>Bid Density</i>	Bid density is the volume of bids that are recorded on a publisher's inventory. Higher bid density means more competition among bidders for the inventory, which drives seller RPM higher
<i>Brand Lift</i>	Brand lift refers to the measurable rise in consumer perception of a brand after a marketing campaign
<i>CCPA</i>	The California Consumer Privacy Act (CCPA) is a state-wide data privacy law that regulates how organizations handle the personal information (PI) of California consumers
<i>Crosswalk</i>	A table that maps identifiers from one identity space to another. For example from Liveramp RAMPID to Experian LUID.

<i>Data Leakage</i>	Data leakage typically occurs when a brand, agency or ad tech company collects data about a website's audience and subsequently uses that data without the initial publisher's permission.
<i>Downstream match rates</i>	Match rate between DSP match and publisher requests
<i>First Party (1P)</i>	First party, in digital advertising context is a publisher or an app developer that has direct relationship with the user i.e. a publisher who's website the user has asked to visit by typing in browser url address for the website domain or by tapping on an app owned by the app developer on a mobile device.
<i>First-party data sets</i>	Data acquired by an organization as a result of an individual's interaction with the organization either online on their website or mobile app or connected device or offline in their physical locations or by mail or phone. Also called first party (1P) data
<i>Frequency</i>	The number of times a viewer is exposed to the same ad during a campaign.
<i>GDPR</i>	The European Union general data protection regulation (GDPR) governs how the personal data of individuals in the EU may be processed and transferred
<i>Identifier</i>	A mechanism to assign a unique value to a device or a browser or a user for associating with a unique person or to identify a group of devices and browsers or users and assign a unique value for associating a with a unique household

<i>Identity Graph</i>	An identity graph provides a single unified view of customers and prospects based on their interactions with a product or website across a set of devices and identifiers. An identity graph is used for real-time personalization and advertising targeting
<i>Identity Partner or Provider</i>	An organization that maintains an individual, household or device level unique identification that can be used to perform a match between two or more organizations' data sets
<i>IVT</i>	Invalid traffic (IVT) is the technical term for advertising impressions generated by bots or any form of nonhuman traffic.
<i>Machine Learning</i>	A mechanism and technology by which a computer can be trained to use existing data and learn how to perform a specific task
<i>Martech</i>	Short for Marketing technology, describes a range of software and tools that assist in achieving marketing goals or objectives.
<i>Match keys</i>	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
<i>Mixed Media Modeling (MMM)</i>	Media mix modeling (MMM), sometimes referred to as marketing mix modeling, is an analysis technique that allows marketers to measure the impact of their marketing and advertising campaigns to determine how various elements contribute to their goal, which is often to drive conversions

*Multi-touch attribution (MTA)*

MTA is a method of attributing credit to different touch points in a customer's interaction (for e.g different media channels where the customer viewed or engaged with an advertisement) with the advertiser that resulted in a customer action (for e.g. purchase of goods or services).

*Onboarding*

Process of setup and configuration to bring an organization's data or processes into a well defined system e.g. a Data Clean Room.

*Personalization*

Mechanism by which products and services (including but not only advertisements) can be delivered to an individual according to the characteristics or attributes of that individual's demography, interests, behavior, location or other expressed intent and information about the individual

*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

*Post cookie*

A common and popular term to describe the state of addressability after the loss of traditional identifiers

*Rate of decay or copy wear out*

Rate of decay or Copy/advertising wearout is a term that describes the decline in effectiveness or selling power of an ad campaign after exposure to the consumer



<i>Reach</i>	It is the number of people (or households) exposed to a given medium at a given point in time.
<i>ROAS</i>	Return on Ad Spend (ROAS) is a measure of total returns from an ad campaign arrived at by calculating the total revenue earned and direct expenses. It does not include other expenses and does not tell if a paid campaign is profitable for the advertiser
<i>ROI</i>	Return on Investment (ROI) is a measure of overall return on investment arrived at by calculating total profit and all expenses- both direct spend on an ad campaign as well as other expenses. ROI determines how profitable is an ad campaign
<i>Third party (3P)</i>	A party to an interaction that has no direct relationship with the individual involved.
<i>Traditional identifiers</i>	Commonly used mechanisms like 3rd party cookie on the browser or Identifier for advertisers on mobile/ device platforms (for e.g. IDFA on iPhone , Android Id on Android devices) to uniquely identify a device or a browser typically used for associating a user or a household.

## Table of Contents

<b>About this document</b>	<b>2</b>
<b>Glossary</b>	<b>5</b>
<b>Introduction: Why Identity Solutions</b>	<b>11</b>
<b>What are Identity Solutions</b>	<b>13</b>
Identity	13
Deterministic vs Probabilistic	14
Identity Resolution	15
ID-based Solutions	17
<b>How are Identity Solutions used</b>	<b>20</b>
Insights and Campaign Planning	20
Targeting and Activation	20
Reporting and Attribution	20
<b>How are Identity Solutions Enabled</b>	<b>22</b>
Publisher and Advertisers	22
Prebid User ID Module	22
Client Side Javascript Implementation	23
Server Side Implementation	23
Identity Resolution / Cross device graphs	23
Ad Tech Vendors	23
Example 1 - Buy side Audience Activation in a DSP	24
Example 2 - Buy side Audience Activation via an SSP using Deal IDs	25
Data Clean Rooms	26
Interoperability	26
Consent and Privacy	27
<b>How to Evaluate an Identity Solution</b>	<b>28</b>
Trajectory of availability of components	28
Scale and Adoption	28
Quality	29
Interoperability	30
Cost	31
Approach to Privacy	32
Data Leakage	32
Use Cases	32
<b>How to determine ID Solution success</b>	<b>33</b>
Advertisers	33
Publishers	34

## Introduction: Why Identity Solutions

Access to consumer data has revolutionized how marketers and publishers understand, recognize, and engage consumers. In digital advertising's early days, the connectivity and portability of that data, using identifiers freely available from web browsers and device platforms, enabled marketers to find customers at scale across the global open web, supporting the growth of large and small publishers alike.

The 3rd party cookie, a widely used identifier available on web browsers, has already been disabled by Apple Safari browser and Google Chrome has announced that it will be completely phased out by the second half of 2024. The other commonly used identifier was the Mobile Advertising ID (MAID) for e.g. ID for Advertising (IDFA) from Apple iOS. While MAIDs are still available on both platforms- Apple and Android- platforms are taking actions to restrict the availability and usage, e.g. Apple's introduction of App Tracking Transparency (ATT), a requirement for users to opt in for use of IDFA, has already reduced availability to around 30% as per one [media report](#) and Android is expected to introduce similar restrictions in future. Together, these developments result in:

- Deprecation of capability to identify consumers
- Loss of cardinality in non identifier based signals, e.g. proxying IP address, simplifying User Agent, referrer URL deprecations

Decline in ability to identify consumers and properly group other attributes disrupts the necessary [use cases](#) to sustain and grow advertising spend by advertisers. This has far reaching consequences for publisher revenues and implications for advertising technology providers.

### **Advertisers and Marketers**

The more marketing changes, the more its fundamentals remain the same. Marketers care most about engaging current customers and using their advertising spend effectively to find their next best customers. The changing global regulatory landscape, cookie deprecation and loss of traditional identifiers used for advertising will continue to erode marketers ability to personalize, activate, grow and measure their advertising spend.

### **Publishers and Media Owners**

As advertisers pay more for identified consumers, it has a direct impact on publisher revenue. The higher the inventory of identified users or authenticated users, the higher the value of publisher inventory. One [study](#) by Mckinsey and Company estimates the risk to US publishers at USD 10 billion due to reduced personalization and activating

authenticated audience. Publishers care most about creating content and experiences that their users want and need a low effort frictionless way to grow advertising revenue.

### **Ad Technology companies**

Legacy advertising technology platforms and data providers used to facilitate personalization and audience-targeted programmatic advertising were engineered to transact on frictionless and scalable availability of traditional identifiers like 3rd party cookies and MAIDs. Without traditional identifiers, they will need to invest in new technology to sustain the services they provide to their customers.

Identity (ID) solutions have emerged as a new category of technologies that enables advertisers and publishers to create personalized consumer experiences.

- ID solutions enable universe to universe matching
- ID solutions provide real time audience activation, bidstream augmentation, campaign optimization and frequency capping capabilities
- ID solutions help with calculating reach, understanding audience insights and trends and determining attribution for campaign conversions

***Note:** While ID solutions can help achieve these outcomes, organizations should still assess each ID solution they plan to use to ensure that their particular needs are met. The rest of this document outlines ways of doing so.*

# What are Identity Solutions

An ID solution is a product or a service that can help identify a person and/or household across digital environments e.g. web browsers, mobile apps, Connected Television (CTV) or other devices with which consumers interact and consume media. The shifting identity landscape has forced a transformation of ID solutions, relying on other signals not affected by browser and platform changes and offering consumers more control around their privacy choices. ID solutions have evolved to offer future-proofed ways of user identification in the absence of 3P cookies and device IDs.

## Identity

To understand ID solutions, it is necessary to understand what is an identity or an identifier as used in digital advertising. An identifier can be made up of one or many components - each component is an attribute of the person or household or the device or their connection to the internet.

ID 1 email	someone@example.com
ID 2 Email + IP address	<a href="mailto:someone@example.com">someone@example.com</a> + 68.193.121.40
ID 3 Email+ User Agent + IP Address	<a href="mailto:someone@example.com">someone@example.com</a> + Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 + 68.193.121.40

Here is a list of commonly used components to build and identity

<ul style="list-style-type: none"> <li>• IP address</li> <li>• MAC address</li> <li>• Hashed email address (HEM)</li> <li>• Telephone number</li> <li>• Home address</li> </ul>	<ul style="list-style-type: none"> <li>• User agent string</li> <li>• IDFA (Apple)</li> <li>• IP address geo</li> <li>• IDFV (Apple)</li> <li>• AAID (Android)</li> </ul>
---	---

<ul style="list-style-type: none"><li>• First-party cookie</li><li>• Third-party cookie</li><li>• Local Storage</li><li>• Session Storage</li></ul>	<ul style="list-style-type: none"><li>• Tizen ID (Samsung devices)</li><li>• Link decoration</li><li>• Bounce tracking</li><li>• etc...</li></ul>
---	---

A component may be used directly to identify a consumer or device such as IDFA or email address. Alternatively, one or more of these components can be combined to create a compound identifier. As an example, some Identity providers may concatenate the values of identity components into a string and hashed to produce an identifier like this:

`e864d9ab9ec1622d0e6d913c0d5b9bc4cbb6a8da7b8cf92997aaec2a1e909aa5`

There are further characteristics that define the nature of an ID solution based on how the identifier is constructed or what are the components in an identifier.

## Deterministic vs Probabilistic

An ID solution is usually called deterministic or probabilistic based on the components or attributes of consumer identity (as described [here](#)). Both will help marketers achieve their objectives.

### Deterministic ID Solution

ID solutions that rely on deterministic attributes of a consumer to identify the consumer that are relatively permanent and associated with one person or household are called deterministic IDs. Some examples include email address, phone numbers, and home address. These work well for publishers and advertisers that have access and consumer consent to these user attributes. However, deterministic attributes may not be available for every consumer, so the scale may be limited. By some estimates, only about 10%-20% of “open-web” content sits behind an authentication wall (requiring email/phone numbers to be submitted).

### Probabilistic ID Solution

To expand the scale of identifying consumers beyond the limited availability of deterministic identity attributes, publishers and advertisers may choose to deploy probabilistic methods. These methods use attributes from devices a consumer uses, the attributes of the way a consumer connects to the internet or specific applications, or user agents the consumer uses in order to determine the same user across the internet.

These are usually relatively temporary attributes or attributes that change often. Some typical examples of attributes that are used for probabilistic IDs are IP address, user agent, timestamps, device details or settings. Probabilistic methods allow marketers to achieve greater scale, with potentially less precision.

## Identity Resolution

Identity resolution is not new to digital advertising. Approaches to identity resolution and the vendor landscape have been well established for quite some time, either built in house or provided by a third party (3P). Although reach, scale and precision are affected as privacy changes spread wider, these solutions are still viable. For example, during GDPR roll-out, opt-in rates began around 20% and steadily rose to 60%+ as publishers conveyed the value exchange to their audiences<sup>1</sup>.

Any identity resolution service uses the foundational elements:

### Identity resolution tools

- Consent Management & User Preference for each identified consumer
- Identity Graph or Device Graph
- 3P Identifiers

**Match keys** or values for an identifier (ID) that enable identity resolution from different sources of consumer data and some may also act as currency during data & media operations for e.g. ad request and buy side decision making.

- Browser Cookie
  - 1P Cookie (*NOTE: This only applies to publisher or owner of multiple websites on same browser*)
  - 3P Cookie (*NOTE: This match key will be ineffective in the near-future as browser vendors restrict them*)
- Mobile Device MAID
  - 1P MAID (*e.g. IDFV on iOS, Not Available for ad use cases on Android Currently. NOTE: This only applies to publisher or owner of multiple apps on the same platform or operating system*)
  - 3P MAID (*e.g. IDFA on iOS, AAID on Android*)
- Hashed Email (HEM) (*NOTE: Prevalent in AMERICAS and EU Markets*)
- Hashed Phone (HPH) (*NOTE: Prevalent in APAC Markets*)
- 3P Vendor Identifiers
  - Agency Holding Company IDs

---

<sup>1</sup> If browser or mobile operating system providers restrict the manner in which publishers can communicate the value exchange to their consumer audiences, for e.g. ATT on Apple devices, the opt-in rates can be lower.

- Martech Platform IDs
- Independent ID Solution Vendor IDs
- First Name, Last Name and Physical Address (*NOTE: This match key will be limited to within-publisher only in the near future as privacy laws transition to a more consumer-driven choice*)

**Device, HTTP Header and Environmental Data** as below but not limited to these parameters.

- User Agent
- IP Address
- Browser or OS Type & Version
- Device Type
- Environmental Signals (e.g. location data)
- Timestamp
- Installed Apps

Even when consent dips and usable digital signals fade, these elements are a necessary part of a complete media strategy required to reach consumers at scale in a privacy compliant manner and resolve the ID to one of the following granularities":

- Device or Screen (*e.g. multiple first party cookies resolved to single ID for a browser*)
- Person (*multiple signals linked together into a single ID representing an individual*)
- Household (*multiple signals get tied together into a single ID representing all devices/individuals within a single household*)

### **Privacy controls and data governance**

Each foundational element used in an ID resolution service comes with its consumer consent and preference as registered by the source of the ID element provider. Thus an ID resolution service must maintain a repository of consumer consent and preference. It is important for publishers and advertisers to understand these practices to evaluate their impact on their own privacy and data collection policies. For example, where do ID solutions derive user data from? (e.g. direct relationship, data brokers) What controls and levels of transparency do users have? How can users opt-out of these ID solutions?

In regards to data governance, security and data governance are critical elements for any identity platform. Governance is defined as policies and practices that govern who can use an ID solution and how. Strong governance ensures that only authorized entities can generate, resolve and utilize an ID. Security is defined as features of an ID solution that secure it against unauthorized use or misuse. An example of a security



feature is encryption. Some ID solutions use encryption to control access to the ID and to enforce consumer consent preferences and reduce data leakage.

Identity resolution solutions will enable all of the use cases as the industry transitions into an id-less world and users are consenting to the data value exchange:

- **Insights and Campaign Planning**
  - Universe-to-Universe Matching
  - Audience Discovery & Creation
  - Pre-campaign Insights
  - Media Mix Modeling (MMM)
- **Targeting and Activation**
  - Audience Activation
  - Bidstream Augmentation
  - Campaign Optimization
  - Fraud Detection
  - Frequency Capping
- **Reporting and Attribution**
  - Campaign Reporting
  - Reach Calculation
  - Audience Insights & Trending
  - Attribution
    - Campaign
    - Conversions
    - Multi-touch (MTA)

## ID-based Solutions

As with Identity Resolution, ID-based solutions are prevalent within the current digital media ecosystem and continue to enable viable media reach and measurement operations. Signal degradation will be an evolutionary process and with that, ID-based solutions will see lesser utility but they will be useful for direct or private marketplace environments as well as be useful for powering modeling methodologies for reaching greater scale.

Across media planning, activation and measurement, the following categories of identifiers will continue to power data and media operations across the digital advertising value chain from brand to agency to media platforms to measurement platform.

### Traditional Identifiers

- Cookies

- MAIDs
- Hashed Emails (HEM)
- Hashed Phones (HPH)
- First Name, Last Name, Address

### 3P Identifiers

- Agency Holding Company IDs
- Martech Platform Vendor IDs
- Independent ID Solution Vendor IDs

### On-device

- Publisher ID (*NOTE: IDs can be translated to Audience<sup>2</sup> and sent instead of or alongside ID depending on SSP integration approach and DSP instrumentation*)
- SDK Vendor ID (*NOTE: IDs can be translated to Audience and sent instead of or alongside ID depending on SSP integration approach and DSP instrumentation*)

One caveat with ID-based solutions is that mapping of Agency IDs, 3P Martech Platform IDs and Independent ID Solution Vendor IDs within the current OpenRTB specification is not standardized so SSPs and DSPs need to agree upon a integration approach for each type of ID they are planning to use.

For ID-based attribution, attribution vendors provide pixel-based, server-to-server (S2S) or [Data Clean Rooms](#) (DCR) data collection to provide campaign measurement services. Pixel-based data collection is starting to shift to S2S and DCR. In addition, programmatic vendors will, in some cases, provide campaign data back to marketers or their vendors with the Marketer's 3P Identifier of choice appended to the campaign performance data, usually for Multi Touch Attribution (MTA) and Mixed Media Modeling (MMM) use cases.

As of the publish date of this document, back-of-the-napkin ID-based success metrics and coverage rates look like this:

- **3P Cookie**
  - 0% for Safari and Firefox as these are no longer available
  - ~80% on other browsers, i.e. 20% opt-out
  -
- **Device-level Mobile Identifiers** (*not publisher specific*)
  - ~80% AAID coverage on Android
  - ~25% IDFA coverage on iOS due to ATT roll out

---

<sup>2</sup> An example of this is Google's Privacy Sandbox/Topics approach with Chrome

- **3P Identifiers**
  - Pre-bid adoption is ~12% (NOTE: This is not verified but generally referred to and discussed in the industry)
  - Bid Stream adoption of 3P IDs ranges from 10% on the low end to 80% on the high end
  - Distribution by Agency IDs vs. Tech Platform IDs vs. Independent Vendor IDs is not shared and considered intellectual property by vendors at this time
- **Other Success & Evaluation Metrics**
  - Number and size of publishers who have enabled identifiers on their properties
  - Average % coverage on publisher supply
  - Volume of ad-requests and programmatic bids with an ID present
  - Performance metrics: can advertisers achieve their KPIs using the ID solutions (audience reach, eCPM lift, fill-rate lift, RPM lift, CTR, CPA, etc.)

ID-based solutions will continue to enable all of the use cases to which the industry is historically accustomed to when users consent to, and feel they receive value for, this data exchange. .

- **Insights and Campaign Planning**
  - Universe-to-Universe Matching
  - Audience Discovery & Creation
  - Pre-campaign Insights
  - Media Mix Modeling (MMM)
- **Targeting and Activation**
  - Audience Activation
  - Bidstream Augmentation
  - Campaign Optimization
  - Fraud Detection
  - Frequency Capping
- **Reporting and Attribution**
  - Campaign Reporting
  - Reach Calculation
  - Audience Insights & Trending
  - Attribution
    - Campaign
    - Conversions
    - Multi-touch (MTA)

## How are Identity Solutions used

This section focuses on how different types of Identity Solutions support various buy and sell side use cases.

### 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 audience between two companies, typically buyer and seller audience 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)

### 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.
  - Campaign
  - Conversions
  - Multi-touch (MTA)

## How are Identity Solutions Enabled

ID solution providers often have both real time user ID solutions as well as identity graphs and associated services. This section describes the different ways ID solutions can be integrated and activated into the digital advertising supply chain.

Identifiers provided by ID Solutions are typically distributed by publishers and advertisers to their user base i.e. consumers who visit their websites or apps. Ad tech partners e.g. an SSP, DSP, Data Platform or measurement provider will need to be embedded in an advertiser or publisher's website or app to get access to IDs or be integrated with them server side.

### Publisher and Advertisers

Publishers and advertisers can distribute user IDs across their user base via a variety of distribution methods dependent on the solution provider and the channels they want to implement the ID solution in. Common integration methods include both client side i.e. on the web page or app and server integration options i.e. the publisher or advertiser's owned systems. These methods are used to distribute user IDs across their user base and are usually stored in local storage provided by the device or user agent. They can also be stored server side but this is currently less common. The publishers/advertiser's ad tech partners who have integrated to pages/apps are then able to retrieve the user IDs, distribute them and use them as a basis for targeting, optimization, measurement and attribution, much in the same way third party cookies have been used in the past.

### Prebid User ID Module

Publishers are able to execute a client side integration by adding their chosen ID Solution modules to their Prebid.js package. In general, the user ID module will check the necessary local privacy jurisdiction requirements via the consent string and if the appropriate consents are in place, the ID provider will be called and will respond with a user ID which will be stored to cookies or HTML5 local storage on the user's device. If there is no consent for the ID solution provider, no call will be made to the ID vendor.

Publishers are able to control which user IDs are shared with which of their bid adapters by using the bidders array, part of the User ID module configuration. The publisher's bid adapters are able to retrieve these user IDs and where they have consent to do so, use them for targeting, optimization, measurement and attribution. They can also use them to communicate user identity with their partners. This might be with DSP's in OpenRTB bid requests or server side synchronizations with data management platforms for example.

## Client Side Javascript Implementation

Publishers or advertisers that don't want to integrate using the Prebid User ID module often have the option of an alternative client side integration with an ID Solutions provider. This is common for web inventory. By implementing javascript on page, ID solution providers are able to use signals provisioned by the publisher or advertiser in the request as well as information available in the header to inform ID generation and subsequently distribute user IDs across their user base. The identifiers are generally stored in local storage or cookies and can be retrieved by ad tech vendors such as DMPs or SSPs that have access to the page via an API.

## Server Side Implementation

Publishers and advertisers can also make server side requests for a user ID for their users. This may be via a prebid server module or custom API. ID solutions may require certain signals such as user consent, IP address, user agent etc. to return a valid user ID. These user IDs can be stored both client and/or server side depending on the use case and ID Solution's policies.

## Identity Resolution / Cross device graphs

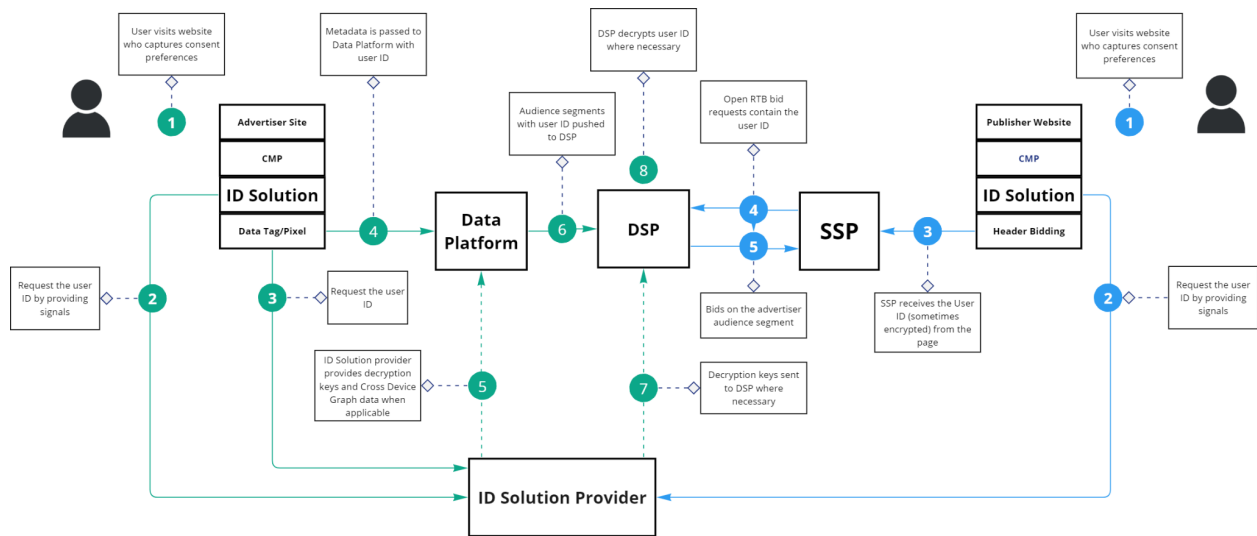
Some ID Solutions have people-based identifiers baked into their real time user IDs, others that offer browser or device based identifiers may have a separate cross device or identity graph offering. The latter may offer the delivery of a full or subset of a cross device graph file on a regular basis. This is commonly sent on a regular basis via an S3 bucket or similar. Common file formats include JSON, Parquet, CSV, and TSV. Some providers also offer real time services to access their identity graph to facilitate identity resolution.

## Ad Tech Vendors

In general, advertisers and publishers distribute real time IDs across their user base and these can be accessed by ad tech partners that have access to their pages and passed between each other through client side integrations or server side APIs. Here are two example workflows of how user IDs can be propagated and used by players in the digital ad supply chain.

## Example 1 - 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.

**Buy side User ID distribution and activation**

1. User goes on to an advertiser's web page or application
2. 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.
3. If the advertiser is working with a data platform, the data platform can call the ID provider and retrieve the user ID.
4. 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.
5. If applicable, the data provider can retrieve decryption keys from the ID provider to decrypt the ID.
6. 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.
7. The DSP can retrieve decryption keys from the ID provider if applicable.
8. 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.

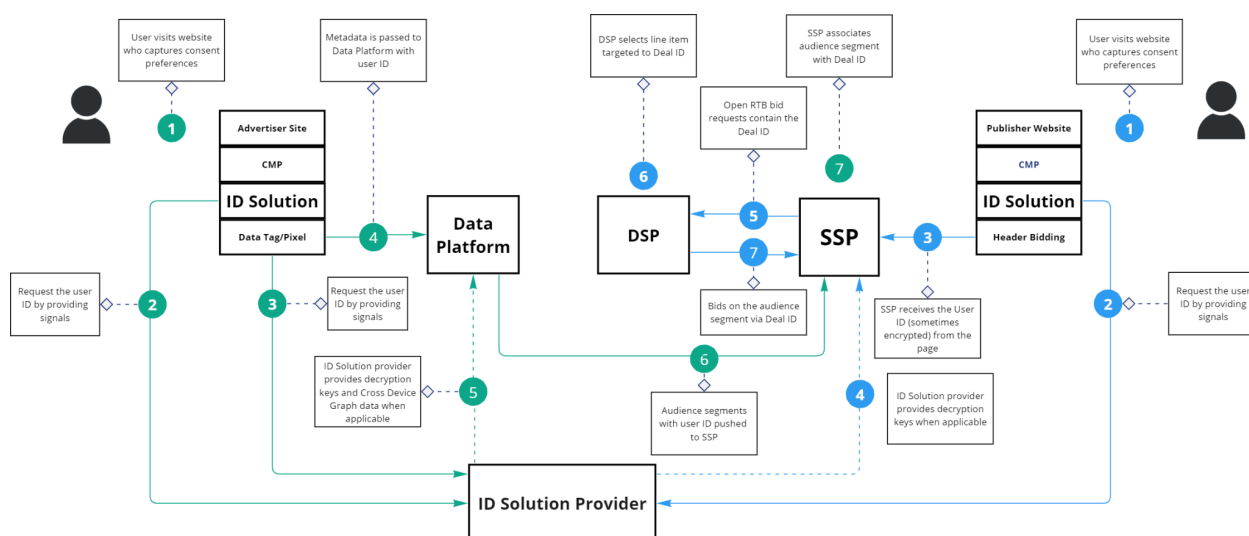


### Sell side User ID distribution

1. User goes onto a publisher's web page or application
2. 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.
3. The SSP picks up the user ID and passes it to the DSP in an OpenRTB bid request.
4. The DSP returns a bid response to the SSP.

### Example 2 - 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.



### Buy side User ID distribution and activation

1. User goes on to an advertisers web page or application
2. 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.
3. If the advertiser is working with a data platform, the data platform can call the ID provider and retrieve the user ID.
4. 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.

5. If applicable, the data provider can retrieve decryption keys from the ID provider to decrypt the ID.
6. 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.
7. The SSP/publisher associates a deal ID with the segment.

### **Sell side User ID distribution and activation**

1. User goes onto a publisher's web page or application
2. 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.
3. The SSP picks up the user ID.
4. The SSP retrieves the decryption keys from the ID provider where applicable and decrypts the user ID and assesses whether any deals are eligible.
5. SSP sends the encrypted user ID and applicable deal IDs in the OpenRTB bid request to the DSP.
6. The DSP evaluated the eligible campaigns to serve
7. The DSP returns a bid response to the SSP.

## Data Clean Rooms

Data Clean Rooms enable data to be shared between two parties in a privacy centric way. ID solutions can be used as the match key to find the overlap between the data sets for measurement and activation use cases. Most commonly the key is hashed emails but increasingly user IDs provided by ID solutions are being used to acquire more matches and better scale. Identity providers are also offering identity graphs that enable ID resolution between multiple ID and signal types (e.g., HEMs to MAIDs) in the clean room environment to maximize match rates between data sets. Learn more about Data Clean Rooms [here](#).

## Interoperability

Interoperability is an essential element for ID solutions. Most use cases in advertising, that different vendors specialize in, require interoperability across multiple IDs. For example, an advertiser uses a DSP and other channels to deliver its campaign and a measurement platform to measure the success of that campaign across that DSP and others. Both DSP and measurement platforms may use different IDs. In addition, most advertisers utilize multiple vendors with different ID solutions for various use cases, meaning that advertisers' ability to advertise in the digital ecosystem relies on those

vendors' ability to translate those IDs and transact with each other. Interoperability between IDs enables various parties in the digital ecosystem to communicate with each other and advertisers to ensure increased reach and scale for their audiences. With a highly interoperable ID solution, advertisers can deliver ad experiences across all channels.

### Challenges

Below are some of the challenges with ID Interoperability

- IDs based on diverse data sets and algorithms
- IDs with different definitions of individual and household
- IDs using probabilistic models with varying thresholds to combine multiple digital identifiers such as HEMs, MAIDs, and IPs
- Consumer privacy related methods like Apple's "hide my email" and other machine generated email tools that manipulate ability to match across contexts.

### Use Cases

Below are some of the use-case powered by ID Interoperability.

- Collaborate with data partners to enrich first-party data to understand consumer behavior better.
- Build a comprehensive view of the consumer journey and touchpoints.
- Activate audience at scale across all touchpoints and IDs.
- Maintain frequency and recency cap across multiple touchpoints.
- Understand the impact of the marketing campaigns across touchpoints.

### Solutions

Below are some of the solutions to enable ID Interoperability

- Identity Graph as typically provided by Identity Resolution services
- Real Time ID Resolution through client or server side API integration
- Cross Walks that maps identifiers from one ID solution provider to another
- Data Clean Rooms that enable private matching systems

### Consent and Privacy

*It is the responsibility of the parties that integrate and distribute ID Solutions to ensure that they have the required compliance with applicable privacy regulations (e.g. GDPR, CCPA etc.) and that they have implemented the governance tools to apply the most updated regulatory compliance to the process of sharing and distributing the ID.*

## How to Evaluate an Identity Solution

As explained in the [previous section](#), enabling and using an ID solution requires investment in integrating and provisioning throughout the supply chain and data operations. It is necessary to properly evaluate an ID solution against multiple dimensions for the intended [use case](#). This section describes some of the common factors (but not a comprehensive set of factors that can vary based on specific needs of a publisher, advertiser or platform) that may be considered when evaluating an ID Solution for deployment.

### Trajectory of availability of components

It is important to understand the trajectory or direction of availability of components used in building an ID solution so you can gauge if it is stable and future proof or not. The table below shows some of the components in three categories - growing, stable and declining availability.

Growing	Stable	Declining
<p>Publisher based identifiers that are used for publishers for other purposes but can be used for advertising use cases, for e.g.</p> <ul style="list-style-type: none"> <li>• Single context storage</li> <li>• 1P cookie</li> <li>• Local storage</li> <li>• IDfV</li> </ul> <p><i>NOTE:</i> These perform within one publisher context and do not support cross context use cases for e.g. Frequency capping and reach calculations.</p>	<p>User based identifiers that the user inputs or provides, for e.g.</p> <ul style="list-style-type: none"> <li>• Phone number</li> <li>• Home address</li> <li>• Email</li> </ul>	<p>Device/ technology based cross context identifiers, for e.g.</p> <ul style="list-style-type: none"> <li>• 3p cookie</li> <li>• IDFA</li> <li>• MAID</li> <li>• IP address</li> <li>• User agent data</li> <li>• Other device signals like user settings</li> </ul>

### Scale and 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.

Metrics you might want to consider in your decision making include:

#	Metrics Name	Metrics Equation	Comparison against
1	Publisher footprint	Count of domains, publishers, apps the ID is distributed on	What is the sell side footprint of the ID solution in the markets and channels that matter most to your business.
2	Programmatic availability	Number or % of bid requests that has the ID available	What is the real availability in the markets and channels that matter most to your business.
3	# of Households (HH)	Count (HH) Per Country	Comparison against Total country population Changes - week over week
4	# of Individuals (Ind)	Count (Ind) Per Country	Comparison against Total country population Changes - week over week
5	Buy Side Adoption	Adtech vendors, agencies and advertisers using the ID solution	Who are the buy side partners that matter most to your business and what ID solution are they using?

## 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.

- **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

- Interoperability 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 seek a vendor that has 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 monetization for publishers.

#	Metrics Name	Metric	Comparison against
1	<b>Key ID or First Party ID Types</b> (e.g., HEMs, MAIDs, Connected TV, etc.) represented in ID Solution	Number of Key IDs Types available in the ID solution	All/Most of the Key ID or First Party ID Types available in the market (e.g., HEMs, MAIDs, Connected TV, etc.)
2	<b>Scale - Key ID or First Party ID Types</b> (e.g., HEMs, MAIDs, Connected TV, etc.) represented at	% of (#HH in ID Solution with at least one Key ID per Geo/ Total HH in ID Solution per Geo)	100% - Higher the better

#	Metrics Name	Metric	Comparison against
	Household (HH) or Individual (Indv) level in the ID solution for given geo (e.g. US)	% of (#Indv in ID Solution with at least one Key ID per Geo/ Total Ind. in ID Solution per Geo)	
3	<b>Coverage or Match Rate</b> with Key IDs or First Party IDs (e.g., HEMs, MAIDs, Connected TV, etc.)	% of (# Distinct Key IDs or First Party IDs per ID Type/ Total IDs in ID solutions)	100% - Higher the better
4	<b>Persistence</b> - Household or Individual in ID Solution to Key or First Party ID (e.g., HEMs, MAIDs, Connected TV, etc.) Persistence	How often the HH or Indv in ID solution is associated with the same Key ID or First Party ID (e.g., HEMs, MAIDs, Connected TV, etc.)	Comparison with each ID solutions refresh

## Cost

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.

## Approach to Privacy

It is important to understand how your identity provider will help you comply with the evolving regulatory requirements of privacy and relegated regulations as well as how they prioritize users' rights to transparency and control. You should perform due diligence with respect to your regions of operation and your own privacy policies:

- Does the ID solution provider have a privacy policy
- What are the governance and control structures and mechanisms deployed by 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.

## 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.

## Use Cases

Each ID Solution provider approaches publisher and marketer [use cases](#) differently. It is important to understand that your use cases are solved, and what are their strengths and weaknesses. One important question to consider is if the ID solution provides cross context capabilities i.e. can you perform common use cases like activation, frequency capping, reach calculations, measurement and attribution across contexts of websites and apps owned by different publishers and developers.



## How to determine ID Solution success

Since ID solutions are a new genre of addressability solutions, it is necessary to monitor their success. This section reviews some of the use cases and their measures that advertisers and publishers can use for monitoring success of their investment in an ID solution.

### Advertisers

While ROAS and ROI remain the ultimate measure of success for advertisers, below we describe some other criteria and measures that can be monitored for monitoring success with an ID Solution.

#### Targeting and Activation

Advertisers using ID Solutions for targeting and activation purpose can use the following measures for evaluating success

- Measure increase counts for addressable audience
  - Focus on additional audience size available in cookieless browsers to set correct expectations (Safari, Firefox)
- Measure increased match rates (addressability) against target audience
  - Focus on match rates in cookieless browsers (Safari, Firefox)
- Measure the incremental reach (user/household level) that was achieved when using an Identity solution for campaign targeting.
  - Focus on de-duplicated reach across devices/browsers
  - Focus on de-duplicated reach across disparate cookies (Chrome)
  - Focus on additional reach in cookieless browsers (Safari, Firefox)
- Measure the cost per unique (user/household)
- Measure campaign costs (eCPM). Was the buy more efficient when using a cookieless solution?
  - Focus on cookieless browsers (Safari/Firefox)

#### Frequency Management and Optimization

Advertisers using ID Solutions for frequency management and/or optimization purpose can use the below criteria to assess success:

- Measure impact on user/household frequency
- Measure rate of decay or copy wear-out

#### Measurement and Attribution

Advertisers can also use measurement reporting and analytics for monitoring and measuring the success of ID Solutions

- Measure the incremental conversions captured when using an ID Solution to connect impressions/clicks to conversion events (sales or site visits).

- Measure impact on ROAS, brand lift, VCR, other KPIs
- Impact on reduction of fraud rates as determined by your verification and IVT providers

## Publishers

While an increase in overall revenue and CPM remain the ultimate criteria for publishers in evaluating any new investment in technology, here are some other measures that can be monitored to start assessing the success of their investment in ID solutions.

Publisher's 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.

- Measure the incremental improvement with auctions that include the ID Solution
  - Downstream match rates
  - Fill rates
  - Yield improvement:
    - Average Bid CPM
    - Average Winning Bid CPM
    - CPM
    - Bid Density (Valid Bids/Auctions)
    - % Bid Response Rate
- Measure impact on site load, bounce rate, or other impact on user experience
- New demand partners added due to ID solution integration