MOBILE IDENTITY
GUIDE FOR MARKETERS

A BEST PRACTICES PRIMER FOR MOBILE & CROSS-DEVICE MARKETING

This document was written primarily for marketers who wish to better understand current approaches for identifying users on mobile and other devices for marketing. It was developed by the Mobile Identity Working Group, part of the IAB's Mobile Marketing Center of Excellence

Representatives from the following companies participated actively in creating *Mobile Identity for Marketers:* 4Info, Adobe, Cadreon, Celtra, comScore, Conversant, Drawbridge, Flashtalking, Foursquare, Google, GumGum, Jumpstart Automotive Media, Jun Group, Kochava, Lonely Planet, Medialets, Nielsen, NinthDecimal, OpenX, Screen6, Sizmek, TapAd, The Weather Company, Yieldmo.

ABOUT THE IAB'S MOBILE MARKETING CENTER OF EXCELLENCE

The IAB Mobile Marketing Center of Excellence focuses on driving the growth of mobile marketing, advertising, and media. Under the guidance of a Mobile Board of Directors, we pursue initiatives including the improvement of mobile creative, creating a reliable and accountable measurement regime, smoothing supply chain problems, advocating for the industry in Washington DC, and educating buyers and sellers of advertising alike as to how mobile and cross-screen consumer behavior is evolving and impacting the mobile ecosystem.

OVERVIEW: WHY A STRATEGIC APPROACH TO MOBILE IDENTITY MANAGEMENT MATTERS

A day in the life of the typical US consumer is increasingly complicated in terms of how media and advertising are consumed. Indeed, according to **Forrester**, the average US adult juggles more than four connected devices. Three-quarters use a smartphone and more than half use a tablet. As the connected devices we use proliferate, we're also consuming more digital media, with a growing expectation for seamless ad and content experiences between our smartphones, tablets, laptop and desktop computers, connected TVs and the various web and app experiences we traverse. At the same time, given the limited effectiveness of cookies on mobile–the challenge for marketers and publishers to effectively reach consumers with the right message at the right time–regardless of their device they're using–is growing as well.

Sources: Conversant, Forrester, IPSOS, ComScore

In addition to the use of first party data, advertisers are increasingly relying on user-level device identity as a foundation of their marketing activities to effectively connect with and manage relationships with multi-screen consumers. Having a consistent consumer identity for marketing activities across a consumer's multiple mobile devices is intrinsically more difficult than having one on desktop devices. Indeed, as a "fairly mature" 23 year old1, desktop advertising has benefitted from having the cookie as its primary identifier to support measurement and interest-based ad delivery. By contrast, mobile brings with it two distinct environments (app and mobile web), a completely different set of consumer behaviors and hundreds of thousands of different device / OS / screen size combinations. In addition, desktop measurement and tracking solutions (like cookies) don't work across the board in mobile. Perhaps for all these reasons, cross-channel audience identification and cross-channel measurement were cited as two of the three most important focus areas by digital marketers and media practitioners in a recent **IAB / Winterberry study.**

In order to capture similar metrics, reporting and ROI that's available on desktop, advertisers on mobile must leverage a mix of tactics and solutions. Even though it does take time to understand how to "get it right" on mobile, there is an extraordinary upside for marketers who put in the effort. As consumer time spent on mobile continues to grow, personalization of advertising and content at scale becomes more tangible, not only in single mobile device settings, but in multiple connected device environments as well. By accurately identifying individual users and establishing profiles of their behaviors, advertisers can create and manage consistent models of user identity needed to:

- Track ad exposure (enabling personalized, creative sequential messaging and management of reach and frequency)
- Attribute online and offline conversions, including store visitations (to impressions served through mobile and cross-device media)
- Match mobile devices (e.g.; smartphones and tablets) to computers (e.g.: desktops and laptops) enabling targeting and retargeting (especially important in the context of online retailing, where nearly three quarters of shopping carts are **abandoned**)
- Link devices to physical locations and offline activity
- Connect with consumers as they move from in-app to mobile web experiences and to and from various social media platforms
- Analyze viewability (to understand the amount of time consumers are actually spending with a brand before converting online or in store)

HOW IDENTITY IS USED

1. TARGETING

The broadest, most simplistic form of targeting begins with understanding and identifying the population or audience segments to which you are marketing. With mobile and cross-screen identity measurement capabilities available today, marketers can rapidly model, scale and test a variety of segments and response outcomes that support secondary, tertiary, quaternary and greater orders of relational values for more effective targeting.

Once the target audience is identified, a core use case for identity management and targeting is frequency management (limiting or optimizing the number of times a visitor is shown a specific ad.) Frequency capping is important not only for the management of efficient ad spend to the above mentioned segments, but also to avoid creative burnout and negative consumer sentiment that can arise from ad over-exposure. In terms of managing frequency caps in programmatic contexts, it's important to note that, depending on the volume of programmatic activity and the match rates between the various vendors in the ecosystem, it may be difficult to guarantee that the frequency targets are met. For this reason, marketers should pay close attention to frequency reporting in programmatic (especially when targets or segments are particularly granular).

Another application of mobile identity is retargeting; for instance, showing an ad to a consumer who uses two or more different devices after they've visited a particular site or app. This "reach the single user of multiple devices" scenario is possible through the use of a diverse set of identifiers for each device. The initial challenge

has been linking the various IDs to real people as they switch from device to device and content property to content property. However, innovation by and competition between companies offering identity linkage services have driven the mobile and cross-device marketing sector to be more effective at delivering relevant audiences.

Beyond audience-based targeting, creative sequencing and more sophisticated dynamic creative strategies can also benefit from improved user identification. Having the ability to layer data such as device type, OS (operating system), device version, geography, daypart and dozens if not hundreds of additional values allows marketers to test and confirm campaign strategies to their liking (in channel-specific or Omni-channel environments). Once validated, marketers can then apply common profile modeling techniques such as audience amplification—finding other Unique Identifiers of the same exact person across the same as well as other devices—to expand their campaign delivery and reach.

These and other tactics that leverage identity management principles may be used across all inventory types, providing marketers and agencies with greater flexibility since the creative determination and campaign optimization is no longer tied directly to the media strategy.

2. MEASUREMENT

At its core, mobile identity management improves the most basic building blocks of measurement. Any metrics based on or derived from unique users will be affected. And it's not only critical for ad impression-based metrics, but for site and in-app conversion metrics as well.

User-based reporting can provide marketers with the ability to identify, segment and analyze unique users and gain insights into campaign reach, as well as content consumption habits and purchase behaviors of customers and prospects. Additionally, many third-party providers offer the ability to accurately determine LTV (lifetime value) and ROI and give app marketers real-time, device-level insight of revenue including downloads, subscription fees, in-app purchases and ad revenue. Lastly, with the ever increasing issue of ad fraud and questions surrounding publisher or agency transparency, implementing an unbiased third-party measurement tool will ensure that advertisers maintain full visibility and control over campaign performance. End users of reports that include this information should understand the benefits and limitations of the underlying technology, the methodologies used as well as the circumstances under which various types of identifiers are (and are not) available. Marketers should also be aware that limitations such as a lack of shared, common identifiers between media buying platforms and third party measurement platforms, can result in challenges with deduplicating IDs across screens and devices, impacting report consistency as well as planning and buying.

Beyond the common metrics such as reach, frequency and conversions, mobile and cross-device identity plays a critical role in deeper engagement analytics and attribution by filling in gaps along the path to conversion to which marketers may not have previously been aware.

User identity scoring can also be applied to predictive variables based on the measurement of impression frequency and distribution by network to give marketers a more complete understanding of the networks and publishers driving the highest impact (or influence) in a campaign. The goal of this measurement exercise is to identify when networks are running ads at an increased frequency due to the lack of new, previously unreached users.

3. SUMMARY: MARKETING APPLICATIONS OF MOBILE AND CROSS-DEVICE IDENTITY

TARGETING

- **FREQUENCY CAPPING –** limiting impressions delivered to users across their mobile and other devices
- **TARGETED ADVERTISING –** serving ads specifically to people based on their behavior
- **RE-TARGETING –** serving ads specifically to people who have already visited a website or app, or are a contact within a database
- **AUDIENCE EXTENSION –** leveraging technology that allows publishers (and their marketing clients) to identify and reach audiences beyond the publisher's owned and operated properties
- **DYNAMIC CONTENT PERSONALIZATION –** dynamically changing content and messaging based on criteria such as user behavior, demographic information and interests to create a more personalized, relevant experience

MEASUREMENT

- **REPORTING –** enables marketers to identify, segment and analyze users, and gain highly granular insights into their behavior, habits, content and offer response patterns. Key metrics can include those related to impression delivery (reach and frequency) as well as ad engagement and conversions.
- **ATTRIBUTION –** the process of identifying a set of user actions ("events") across multiple screens and touch points that contribute in some manner to a desired outcome, and then assigning value to each of these events
- **PREDICTIVE MODELING –** using statistics to predict future behavior

WAYS OF IDENTIFYING USERS ON MOBILE

Mobile device manufacturers and operating system providers offer several identifiers for differentiating device owners, some of which can be used for consumer advertising and marketing purposes and some that can't. These identifiers can be grouped into two categories; hardware-based and software-based.

TYPES OF IDS

HARDWARE-BASED IDENTIFIERS (AKA PERSISTENT DEVICE IDS)

Hardware Based Identifiers are associated with physical components on the mobile device, are non-privacy supporting and should not to be used for marketing purposes because consumers cannot turn them off or opt-out of sharing. For this reason, in **2012**, Apple, and in **2013**, Google disabled access to these persistent IDs in order to protect consumer privacy. A description of these persistent IDs is below:

HARDWARE IDS	DESCRIPTION	WHAT THEY LOOK LIKE	NOTES
Universal Device Identifier (UDID)	The manufacturer's persistent and unique ID for the actual mobile device	2b6f0cc904d137be2e1730235f5664094b831186	Non-privacy supporting
Media Access Control (MAC) Address	The manufacturer's persistent and unique ID for each network interface card on the mobile device	B8:53:AC:B1:12:87	Non-privacy supporting. Most phones have two MAC addresses which equate to one for each antenna – the Wi-Fi antennae & the cell network antennae

SOFTWARE-BASED ADVERTISING IDENTIFIERS can be disabled and/or reset by the consumer. The major operating system manufacturers have their own implementations for generating and controlling Advertising Identifiers. The most prevalent Advertising Identifiers today offering the scale needed for marketing purposes are the following:

SOFTWARE BASED ADVERTISING IDS	DESCRIPTION	WHAT THEY LOOK LIKE	NOTES
IDFA	Apple's Identifier for Advertising on the iOS operating system	AEBE52E7-03EE-455A-B3C4-E57283966239	Privacy-supporting (may be disabled / reset by user). Used for advertising purposes
AAID	Google's Android Advertising ID	97987BCA-AE59-4C7D-94BA-EE4F19AB8C21	Privacy-supporting (may be disabled / reset by user). Used for advertising purposes

There are additional software developers in the space offering unique probabilistic IDs produced through statistical modeling to identify individual devices or environments. These tools, addressed later in the document, are designed to take multiple disparate data points (screen size, processor, OS, etc.) from the same devices in mobile web and app environments and produce a unique ID completely independent of cookies.

NOTE: In some marketing circles, the term "Device ID" is considered synonymous with "Advertising ID". Marketers and publishers should be aware that use of the term Device ID may raise concerns that they are using non-privacy supporting hardware based IDs for marketing purposes. While persistent hardware IDs are available for use by app developers for use cases not related to advertising, marketers and publishers with apps should be aware that using a persistent ID other than the user-resettable advertising ID (or mis-using an Advertising ID) may result in an app developer policy violation notice from **Apple** or **Android** and potential removal from the app stores. IAB encourages marketers and publishers to use privacy supporting identity management practices. See the Privacy section in the Appendix for more information, resources and best practices.

COOKIE-BASED APPROACHES

As mentioned in IAB's earlier white paper **Cookies on Mobile 101**, there is a commonly held belief that "Cookies don't work on mobile". A more nuanced and accurate version of this statement would be "cookies don't work on mobile the way we expect, based on desktop."

On desktop, cookies generally work well in terms of identity management. For instance when a user clicks an ad or a link on a website on their desktop browser, a cookie is typically placed on that user's computer that can be used for follow-on marketing. On mobile devices, because of browser limitations and fragmented environments, cookies cannot be relied on sole means for identifying a device. A number of other tracking methods have been developed to overcome these challenges, because the reality is, cookie tracking on mobile alone is of limited utility unless paired with tactics such as synching with offline data or combining with additional tracking pixels. When thinking about mobile cookie availability and its relative usefulness, it is helpful to divide the mobile world into browsers/websites and mobile apps.

A. COOKIES IN MOBILE WEB BROWSER ENVIRONMENTS

Most mobile web browsers accept first-party cookies (e.g., a cookie whose domain is the same as the domain of the visited website). For example, a cookie whose domain is news.com may be placed by http://www.news.com. Different mobile browsers behave differently when it comes to accepting third-party cookies (that is, cookies whose domain is different from the visited website) For example a cookie whose domain is advertisinginfo.com, placed on the site **http://www.news.com**. While third party cookies are supported in Android devices for all the various marketing use cases described earlier, on iOS they are not (the default setting on Apple's Safari browser has third party cookies disabled). The variation on this rule comes into play when a consumer clicks on or engages with an ad and then is redirected to a 3rd party's web site. At that point—assuming the advertiser is also the publisher—the 3rd party site becomes a 1st party since the consumer has now visited its web site on its own domain (and that former third party, now first party, is able to set cookie in the user's mobile browser). In terms of most ad tech platforms (DSPs, Ad Servers etc.), cookies remain 3rd party as they are typically not set on an individual (first party) domain.

There are time limitations that apply to cookies as well. Mobile cookies can be short-lived (session-based) or persistent. Session-based cookies (assuming the user has configured their browser to allow cookies) are temporarily set in the user's mobile browser while they are visiting a website, but are then deleted when the user leaves the site (or when the user shuts down their mobile browser or turns off their device). Persistent cookies however (again, assuming the user has configured their browser to allow first and third party cookies) can stay within the user's browser until the cookie expires (as defined by the web site developer or mobile app developer, or until the user deletes their cookies (through the process described in the appendix). A cookie without a defined expiration date is a session cookie.

B. COOKIES IN MOBILE APP ENVIRONMENTS

As highlighted in "Cookies on Mobile 101", mobile apps handle cookies somewhat differently than mobile browsers. Apps use a technology called a "webview" which lets people briefly access online content such as websites without leaving the app. Cookies generated through a webview can be stored on the device in an app-specific space commonly referred to as a "sandbox" environment.

This sandboxed environment limits the application's ability to access data from other apps. The application can still store and access cookies and other data within the application itself, but it is restricted from accessing information from any other app on the device. Because of this, advertisers cannot follow a user from app to app based on a cookie in the same way that they can track behavior within a browser window. Therefore, for any given webview session, the cookies stored in it are unique to the application that launched it. Going back to the previous example of the news.com web site, if the same mobile user/device were to visit the site via two different browsers (ex: Chrome and Safari) two different cookies would be generated even though the user visited the same site.

Apple further describes the purpose of the **app sandbox** as follows: "By limiting access to sensitive resources on a per-app basis, app sandbox provides a last line of defense against theft, corruption, or deletion of user data, or the hijacking of system hardware."

Ultimately, while cookies on mobile do exist, and may be used by advertisers, their persistence and acceptance can vary. Marketers should pay careful attention to the distinctions between the two operating systems and web vs app content environments as they can have positive or negative implications depending on the audience the marketer is trying to reach. The larger implications this fragmented environment has on issues of crossdevice identity resolution will be addressed in future IAB initiatives. For more information on how to get involved, contact: **committees@iab.com**.

C. ENCRYPTION AND HASHING OF IDENTIFIERS

Some publishers encrypt or hash their Advertising ID's before sharing externally with 3rd parties. Encryption is a practice of encoding this information with a mathematical algorithm so only authorized parties can interpret the ID. In the mobile ecosystem, the most common forms of Advertising ID encryption are:

· SHA1 (Secure Hash Algorithm 1) (https://en.wikipedia.org/wiki/SHA-1)
· MD5 (https://en.wikipedia.org/wiki/MD5)

SHA1 and MD5 refers to the math algorithm used to hash the Advertising Identifier. Here are examples to convey the encryption concept:

APPLE IDENTIFIER FOR ADVERTISING (IDFA) ENCRYPTION EXAMPLES	
RAW Version	AEBE52E7-03EE-455A-B3C4-E57283966239
SHA1 Version	A7FE134E3C8E805D2FB72151146AB7841F275C36
MD5 Version	E69A1078552E13F2734C22322708BD95

GOOGLE ADVERTISING ID ENCRYPTION EXAMPLES	
RAW Version	97987BCA-AE59-4C7D-94BA-EE4F19AB8C21
SHA1 Version	D42B4890298FC4821A52C11F24E2A8AC06FA10B0
MD5 Version	BA06C008973B8A1BFF6E087C6149227F

ACCESS TO ADVERTISING IDS

Many marketers assume that Apple's IDFA, Google's Advertising ID and **Microsoft Mobile OS Advertising IDs**, gathered by publishers are openly accessible and transferable to other entities for marketing purposes. However, this isn't always the case. In RTB (real-time bidding) settings, access to these Advertising IDs is more common, but outside of that context, some publishers do not share them. In cases where the publisher has the option to share their Advertising IDs with marketing partners (based for instance on their user agreements and business rules), there may be various contractual and operational restrictions required. For this reason, marketers should become familiar with how, and in what format Advertiser IDs are shared, which may be on a case-by-case basis, often with specific data usage contracts and restrictions, before a mobile or cross-screen campaign is run.

IDENTIFYING USERS ACROSS SCREENS[1]

Early measurement systems revolved around desktop browser functionality where, at the time, media consumption largely took place on personal or family computers. Cookies were the primary markers to determine when a person was exposed to paid messaging and if a person engaged with the ad unit in a specific way, as well as the events that took place along the path to conversion within a specific campaign.

As media consumption began to fragment across mobile, tablet, OTT TV, auto and IoT platforms, the lack of cookie support within these devices forced industry participants to find new techniques for identifying when the same user sees campaign messaging across different devices and channels. The resulting approach—known as user level device mapping—attempts to assemble an individual consumer's device graph, largely based on the likelihood that seemingly disparate devices are being used by the same individual. Device graphs are now seen as a necessary foundation for a holistic view of message delivery within a modern, omni-channel digital media campaign.

Device graphs are generally built and maintained by third party analytics organizations that rely on two distinct approaches: probabilistic methods and deterministic methods. Challenges with both approaches include accuracy testing against a consistent baseline, and controlling for errors. For example, the approaches cannot control for when other individuals—friends, family, etc.—are using a person's device.

DETERMINISTIC APPROACHES[2]

The deterministic method relies on personally identifiable information (PII) to make device matches when a person uses the same persistent identifier—namely an email addresses, a phone number, mailing address or credit card information—when logging into an app or website or when making a purchase. When a user logs in or makes a purchase at any point across multiple devices, deterministic data providers can associate those cookies or device IDs in a device graph and use that information to identify or target the same user across multiple screens with great confidence. Because of the ability to authenticate across devices, deterministic approaches are thought of as the most accurate way to determine user-level device graphs. However, one downside is the perceived lack of scale across devices, as there are hard limits to the amount of registration data that companies have, contingent upon growing user bases. There may also be differing levels of precision or validity among the available identifiers used for Deterministic solutions. Given these and other issues, some deterministic data partners may also leverage probabilistic device inferences to augment their PII.

[1] See IAB 2016 IAB Digital Attribution Primer Section 2.3

[2] See 2016 IAB Digital Attribution Primer Section 2.3.1

PROBABILISTIC APPROACHES TO IDENTITY[3]

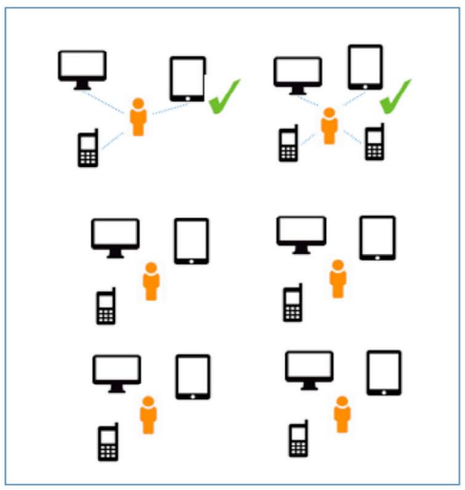
By drawing on aggregation techniques, probabilistic approaches may incorporate thousands of anonymous data points—things like device type, operating system, and location data associated with bid requests, time of day, and a host of others—to identify statistically significant correlations between devices. Signals may be also be drawn from known multi-user identifiers like IP addresses or from geographic regions. By using IP to Geo technology—which can establish a ZIP code or other geographical coordinates from an IP address—the incorporation of additional aggregate signals is possible.

Based on the various available signals, probabilistic techniques attempt to determine the devices that are likely being used by the same person. Once this determination is made, that provider would likely assign a particular organization ID to the device. For example, if a smartphone, desktop computer and a laptop connect to the same networks or Wi-Fi hotspots at the same time and in the same places every weekday, one can develop a degree of confidence that all three devices belong to a specific person.

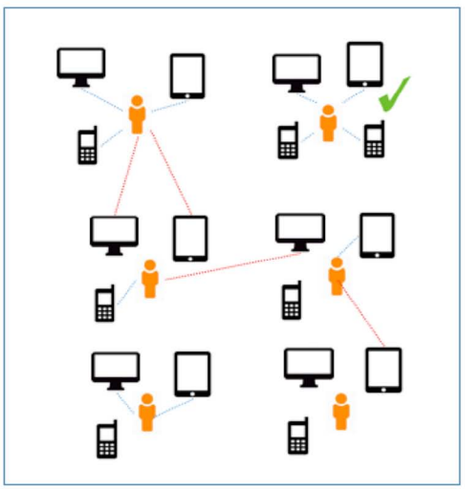
Probabilistic approaches are generally considered to be less accurate than deterministic approaches when associating device pairings, as they are largely based on inferred and/or modelled data. One benefit is that these solutions have greater flexibility to scale across devices, meaning that device mappings can potentially incorporate more overall consumer devices than deterministic partners.

A. The importance of precision (aka accuracy) and recall (aka reach or scale) in probabilistic identity matching

Comparisons of mobile and cross-device matching solutions often start by comparing device graphs. When evaluating device graphs, it is important to consider both Precision and Recall metrics. Precision is the percentage of correctly identified matches among all matches identified within the device graph. A high precision graph only guarantees that a high percentage of the matches that have been identified within the graph are correct. It provides no indication of how many devices may not be matched at all. Recall, often interchangeably called either scale or reach, helps address this. Recall is the percentage of matches correctly identified from all possible correct matches. Probabilistic methods of matching aim to strike a balance between these two metrics, since one can be increased at the expense of the other.



HIGH PRECISION GRAPH
(Of the devices matched all are correct, but it leaves many devices unmatched)



HIGH RECALL GRAPH
(A lot more devices are matched, but not all matches are correct)

Source: Drawbridge

A higher precision graph will be great for retargeting, since the likelihood of the retargeting messages reaching the wrong individual will be low. However, precision at the expense of recall, will seriously limit how many individuals can be retargeted. Similarly, if the marketer is hoping to reach the individual on as many of their devices as possible, then a higher recall number will be beneficial. However, higher recalls at the expense of precision, will lead to the marketing message reaching a lot of individuals who are not the intended audience for the message. Hence it is important for the marketer to be clear about their marketing goals, while determining the ideal tradeoff between these two metrics.

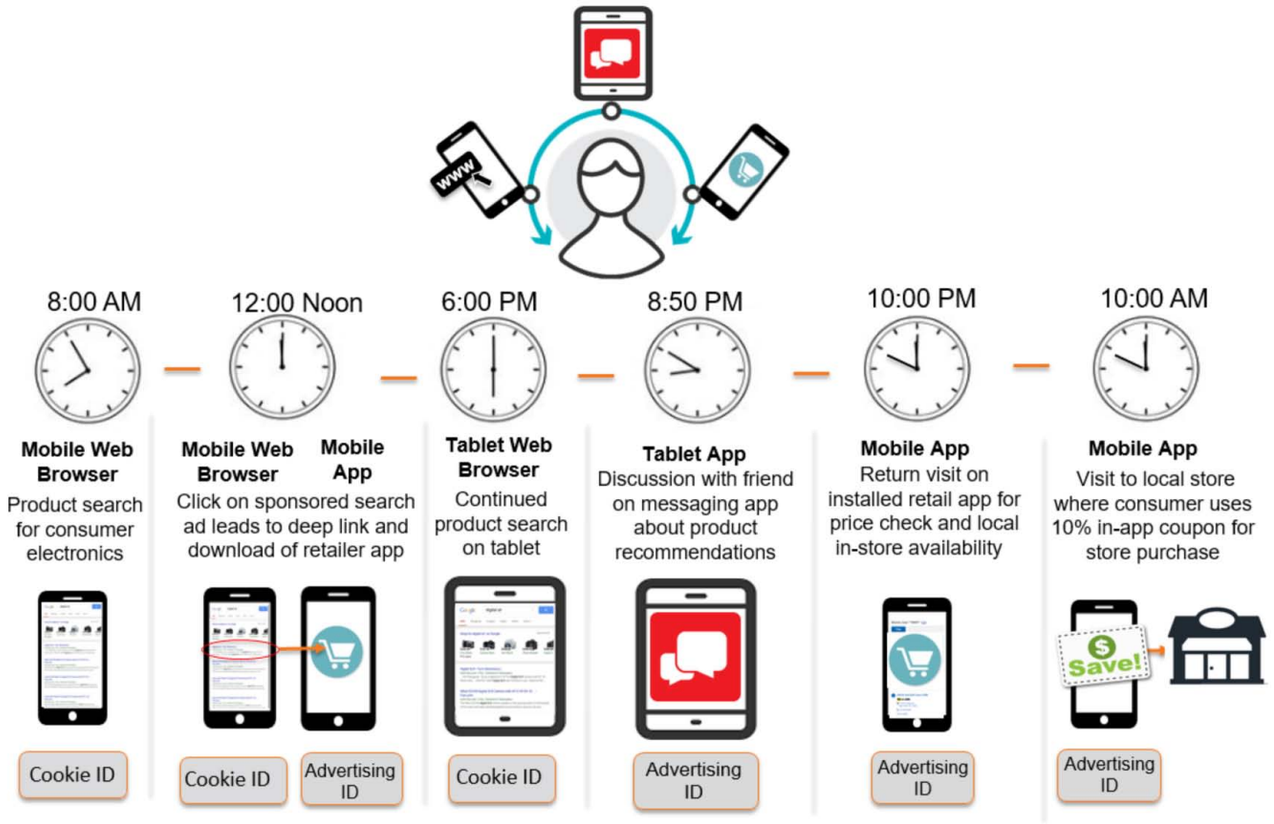
For more information on the trade-offs between precision and scale, and the difference between the often confused terms of Accuracy and Precision, see Appendix.

LINKING ACROSS DATA SETS: TACTICS FOR BRIDGING WEB TO APP

As mentioned earlier, the growth in number of devices used by consumers creates a fragmented media landscape and adds complexity to the process of mobile and cross platform marketing. Continually shifting content consumption behavior also adds a layer of complexity.

For example, a consumer may start their day conducting a product search from within their mobile browser. From that search they may be deep linked into a retailer's app installed on their device. When the consumer arrives home that night they may continue their product search, perhaps on a tablet, where they ask a friend via messaging app for additional recommendations. Finally at the end of the day, having chosen a particular product, the consumer searches the retailer's app for local availability and in-store pick up the next today.

MULTI-SCREEN, WEB TO APP TO STORE CUSTOMER JOURNEY



These varied web-to-app, app-to-web content experiences characterize a day in the life of the mobile consumer. They also offer a glimpse of future consumer retail experiences characterized by mobile-centric shopping, leading to online ordering with merchandise personalization and pickup at a physical location. As more purchases are made using multiple channels, attribution of sales by device becomes critical–increasing the need for device matching and multi-touch attribution.

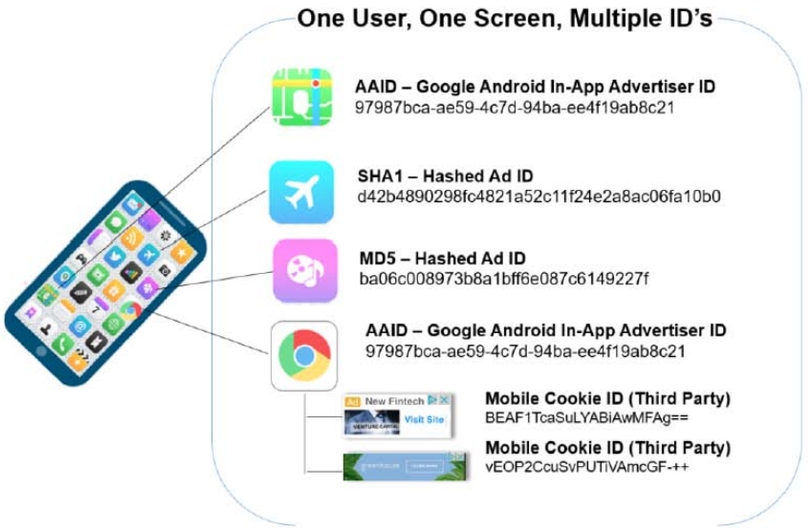
Today, there is no easy, one-stop-shop solution that marketers can leverage to address any and every mobile intra or inter-device matching and marketing scenario and it may take a combination of solutions to accomplish the full scope of a marketer's needs. Depending on the methodologies of the various vendors, there might also be some discrepancies when it comes to bringing everything together in a holistic view of the customer. All this to say, there are a number of solutions[1] (see below) available for the various needs of the market which may rely on a combination of web-based IP addresses, cookies, app-based Advertising IDs, 1st and 3rd party data and location identifiers. It's best for marketers to be clear on their objectives and to ask a lot of questions during the vendor evaluation process (for guidance on the questions to ask, see pg 17 in the conclusion).

[1] Vendors in the mobile and cross-device identity measurement and mapping space include: mobile app deep linking providers, cross-platform data onboarding firms, deterministic and probabilistic audience and device graph solutions providers, data enrichment firms and mobile and cross-device ad tech firms.

ATTRIBUTION AND IDENTITY: COMPARING APPLES TO APPLES

When considering reach metrics in the context of mobile targeting and attribution, marketers should be sure to specify with their 3rd party vendor partners how they're counting audiences, especially for cross-device campaigns. Are they counting screens (i.e.: unique devices) or **unique users**? (an unduplicated person* exposed to advertising messages during a reporting period). The diagram below illustrates why the differentiation of screens versus unique users should matter to marketers.

A CONSUMER WITH A SINGLE DEVICE CAN HAVE MULTIPLE ID'S



The example report here shows how a "screen centric" methodology can result in the over-counting of audience reach. Reach measurement providers should not conflate or confuse machine-based measurement (that measure unique devices) with people-based measurement (that measure unique users). Vendors should have a robust methodology in place to identify and deduplicate unique devices and/or users for their reach reporting and be able to filter invalid or fraudulent user IDs.

	Day 1	Day 2	Day 3	Day 4
Raw Advertiser ID	1	0	1	0
ID hashed with SHA1	0	0	1	1
ID hashed with MD5	1	0	1	0
Total Visits: screen-centric	2	0	3	1
Total Visits: user centric	1	0	1	1

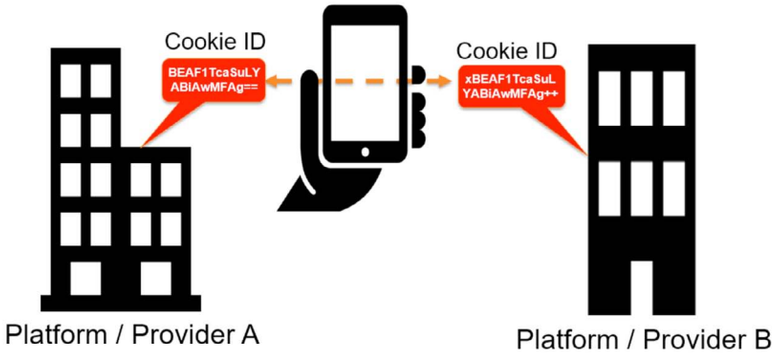
Duplication risk in screen-centric methodologies

ANSWERS TO COMMON QUESTIONS

WHAT DOES THE IDENTITY MATCH DEPLOYMENT PROCESS LOOK LIKE?

Matching processes may vary depending on the particular Cross-Device Identity Vendor. Some vendors offer device graphs based on master data sets, which leverage a "cookie-synch" between the vendor and the marketer-licensee (a process by which the companies exchange their own unique cookie IDs to jointly identify a user's browser).

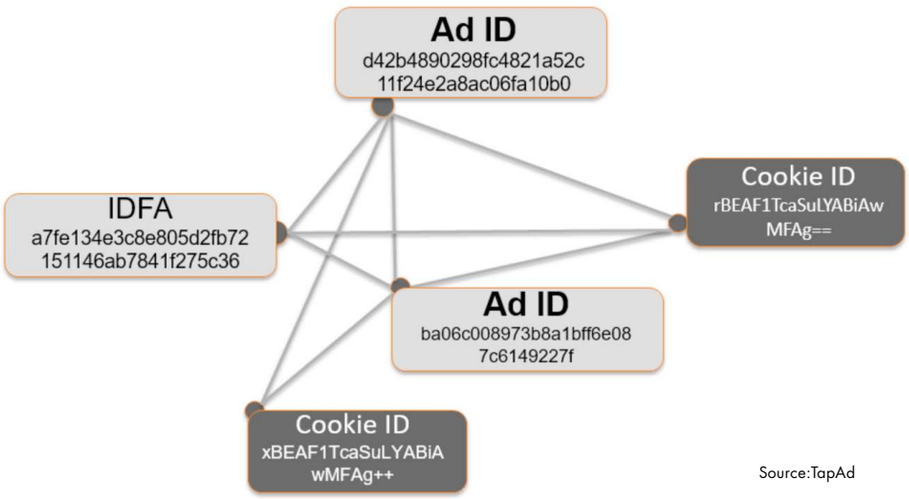
As highlighted earlier, cookies are domain-specific. Those created by one third-party cannot be read by another third-party unless a cookie joining, or synchronization process is used.



The cookie synch process involves the creation of a match table used to map the IDs of one platform to IDs for that same user, on another platform. This cookie ID mapping and matching can occur for instance between a cross-device marketing partner as well as various other data providers and platforms.

Other vendors do not co-mingle data. For these solutions, there is no initial cookie synch or pixel-based implementation.

Advertising IDs gathered through mobile in-app contexts (for example, Apple's IDFA or Android Advertising IDs), in hashed or plain-text versions, can also be linked with cookie IDs in the identity match deployment process.



Source:TapAd

Alternately, device graphs can also be provided within a common cookie space, where a match table of cookie or advertising IDs is stored, such as that of a DMP (Data Management Platform), SSP (Supply Side Platform) / DSP (Demand Side Platform) or ad server. Once a cookie space has been identified and mapped, a cross-device vendor can provide a graph in the form of Clusters (sets of n device identifiers mapped to the same user) and bridges. A cluster (example above) is a group of IDs connected together, representing a single entity.

Clusters are combined in a Device Graph-building process that yields data, referencing connections between IDs, based on anonymous and/or login data. Device graphs are periodically updated and transferred to the licensee via File Transfer Protocol (FTP) or S3 (Amazon's Simple Storage Service).

HOW IS LOCATION DATA USED IN THE CONTEXT OF MOBILE AND CROSS-DEVICE IDENTITY?

Data gathered from opt-in users through their location enabled apps, is a key source of matching identifiers. Showing an ad to a consumer on either their mobile or desktop device and then identifying the consumer when they visit a store with their mobile device, can inform both attribution and purchase intent (and through integration with credit card data, verify actual purchase). The matched identity can be used for retargeting across devices and for better targeting of ads using the advertiser's first or third party data.

HOW DO THE VARIOUS TYPES OF IDS EFFECT MY REACH CALCULATIONS?

Often, reach calculation (unique device counts) leverages cookie IDs or other non- people connected IDs. When a cross device ID is enabled you may have access to a more accurate count of humans rather calculation than devices or cookies, depending on whether or not your system of record for reach can leverage these people-based IDs. Verify with whichever provider you use for reach calculation, as to whether they can count reach against alternate or third party connected IDs.

SHOULD I BLACKLIST ASSOCIATED DEVICES FROM A USER TO LIMIT OVERLAP?

Rather than blacklisting devices, frequency capping can be approached holistically at the user level by maintaining a count of campaign frequency across all their devices, rather than on a device-by-device basis.

HOW OFTEN ARE USERS EXPOSED TO MEDIA ON MOBILE DEVICES? WHAT DEVICES AND PLATFORMS ARE THEY USING?

SMARTPHONE OS PLATFORMS: According to comScore's 2017 mobile platform rankings, the top platforms (in a 3 Month Average, for the period ending Jan 2017) shows Android at the top of the list with 53.2% of subscriber share, followed by Apple at 44.6%. Microsoft Mobile garnered 1.6% and Blackberry had a 0.6 % share of smartphone subscribers.

TOP PLATFORMS - SHARE OF U.S SMARTPHONE SUBSCRIBERS AGE 13+

3 Month Avg. Ending Feb. 2017 vs. 3 Month Avg. Ending Nov. 2016

#	PLATFORM	NOV-2016	FEB-2017	POINT CHANGE
1	Android	54.80%	53.30%	-1.5
2	Apple iOS	42.70%	44.60%	1.9
3	Microsoft	1.80%	1.50%	-0.3
4	BlackBerry	0.60%	0.60%	0

Source: comScore **MobiLens**

TOP SMARTPHONE DEVICE MANUFACTURERS: in terms of device penetration, Apple ranked as the top manufacturer with 44.6 percent of U.S. smartphone subscribers (up 1.9 percentage points from Nov 2016). Samsung ranked second with 28.3 percent market share (down 1.2 percent), followed by LG with 10 percent, Motorola with 4.3 percent and HTC with 2.2 percent.

#	DEVICE MANUFACTURER	NOV-2016	FEB-2017	POINT CHANGE
1	Apple	42.70%	44.60%	1.9
2	Samsung	29.50%	28.30%	-1.2
3	LG	9.90%	10.00%	0.1
4	Motorola	4.40%	4.30%	-0.1
5	HTC	2.50%	2.20%	-0.3

Source: Source: comScore **MobiLens**, Total U.S. Smartphone Subscribers Age 13+

#	TOP 15 APPS	% REACH
1	Facebook	78.70%
2	Facebook Messenger	68.40%
3	YouTube	68.20%
4	Google Search	62.40%
5	Google Maps	55.80%
6	Google Play	49.90%
7	Gmail	46.50%
8	Snapchat	45.60%
9	Instagram	45.10%
10	Pandora Radio	38.80%
11	Google Calendar	36.60%
12	Amazon Mobile	28.30%
13	Apple Maps	28.00%
14	Apple News	27.60%
15	Apple Music*	27.60%

Source: comScore **MobiLens**, Total U.S. Smartphone Mobile Media Users, Age 18+ (iOS and Android Platforms)

TOP 15 SMARTPHONE APPS: In terms of the top smartphone apps, reach-wise on both iOS and Android, Facebook ranked as the top individual app.

CONCLUSION

As the march towards mobile continues, the opportunities for marketers to leverage consumer's increased connectivity are increasing, along with the challenges that come with reaching them in an increasingly fragmented media environment. Given the varied persistence and acceptance of mobile cookies from device to device and across web and app environments, marketers must become adept at drawing on a range of identity management and matching solutions, in order to view, understand and reach their mobile consumer more consistently and holistically across their devices.

When it comes to developing an Identity Management Vendor RFP, it's important that marketers ask the right questions to make sure the vendor (or combination of vendors) fits with the marketing objectives. While this buyer's guide is designed to offer a high level overview of mobile identity management, the list of questions below should serve as a starting point in the vendor evaluation process.

SAMPLE MARKETER QUESTIONS TO ASK WHEN EVALUATING DATA LINKAGE / MATCHING SERVICES

- What is the vendor's process for creating matches between devices, cookies and IDs?
- What is the pricing model for their service? (ex; flat rate, CPM rate, matched user rate, data processing fee)
- What is the onboarding process and is the advertiser required to contribute data?
- Does the vendor filter invalid traffic (IVT) or work with upstream data providers who use MRC accredited filtration methods[1] as part of their service or solution?
- Are the vendor's processes privacy-supporting (and if so, in which geographies)?
- How does the vendor measure performance for their solution?

For additional guidance related to vendor selection for cross device and multi-touch attribution and measurement solutions, please see **IAB's Multi Touch Attribution Guide**.

[1] See MRC Invalid Traffic Detection and Filtration Guidelines Addendum

KEY TAKEAWAYS

Personalized messaging requires a person-level insights
In order to deliver truly personalized and relevant messaging, marketers should not only work with cross-device identity vendors, but also with attribution providers and internal data teams to help them not just connect and match devices with unique, people based IDs, but also to gain an understanding of the consumer behind the device.

Identity management requires profile management
The quality of a consumer profile depends on continually updated data. To improve the relevance of your messaging be sure to press vendors on the recency and freshness of their data. The process of identifying a consumer across their devices requires tying those devices back to a common profile.

Respect and support consumer privacy
The use of consumer's mobile and cross device data requires transparency and choice. Marketers should work with their own legal counsel to ensure that they are in compliance with all laws and self-regulatory programs including privacy policies that disclose how data is collected, used and shared.

In the appendix we have provided links to additional resources on managing mobile identity in privacy supporting ways. IAB will continue to work on industry-wide options for streamlining mobile and cross-device identity management and we welcome you to join the discussion. If you're an IAB member and would like to participate in IAB's working groups, please email: **committees@iab.com**.

GLOSSARY OF KEY TERMS

ADVERTISING ID
Advertising ID is a user resettable ID assigned by the device or operating environment for advertising purposes (e.g. targeting, frequency capping) Examples include Apple's IDFA and Android's AAID.

COOKIE ID
A cookie is a small text file and associated alphanumeric identifier generated by a website or a website partner (advertisers, data management platforms, etc.). Cookies are stored on a visitor's browser upon arrival at a particular destination, and Cookie IDs are passed along with ad requests. They are most frequently used to determine desktop or laptop associations. Cookies can generally be read only by the assigning service (i.e. websites can't read cookies from other websites)

- **First Party Cookie** – Cookies which are assigned in and by the domain of the website shown in the browser's address bar.
- **Third Party Cookie** – Cookies which are assigned in and by a domain different from the website shown in the browser's address bar. These cookies originate from parties who serve content into the webpage you're visiting (e.g. advertisers, plugins and other content providers).

CROSS-PLATFORM DIGITAL ADVERTISING
Advertising served across a range of places where consumers might be exposed to digital advertising, including: Desktop/PC media platforms, Mobile (phones & tablets), OTT/Connected TV, Digital Out of Home (DOOH), Digital Audio, Gaming Platforms (source: IAB Sales Certification)

CROSS-SCREEN MEASUREMENT
Tracking and measurement of metrics across a variety of devices such as Mobile, Tablet, Desktop, Connected TV

DEEP LINKING
A method typically used as a targeting tactic by mobile app marketers by which a URL links to and opens a specified page or location within a mobile app, rather than simply launching the app. There are two types of URL schemes that can be leveraged when deep linking. An http/https based scheme (Universal Links and App Links are the standards for iOS and Android respectively) and a custom scheme (myapp://), the latter being less flexible/ secure and considered a legacy scheme.

DEFERRED DEEP LINKING
Related to the process of App Deep Linking and used when the consumer does not have the app downloaded in advance, Deferred Deep Linking first directs the user to the appropriate app store page for app installation, and then upon opening the app, the user is automatically redirected to the specified page, location in the app, a specific web landing page or even an interstitial as intended in the initial engagement.

DEVICE GRAPH / DEVICE MAP
A database of unique devices that can be tied together, without links to specific individuals or households. Device graphs are assembled by associating primary device currencies such as Advertising IDs, Statistical IDs, Cookie IDs, and/or WAN IP addresses. Using publicly available signals, mapping providers need first to be able to consistently identify the same device against these currencies to develop a confidence threshold. The second step is to make an association with other known devices, a process that is often proprietary and used as a primary differentiator by device graphing providers. In addition to device mapping, these currencies can also be used for targeting, segmentation, and/or online-to-offline tracking.

DEVICE RECOGNITION
Device Recognition is an audience identification analysis using statistical algorithms based on the values of a combination of standard attributes made available by the device. This analysis is largely dependent upon device information passed in HTTP headers of ad requests, namely: device type, operating system, user-agent, fonts, and IP address. Some attributes can change over time due to device changes or updates. Device Recognition can be used for attribution, frequency capping, and retargeting, among other applications.

FILTRATION OF INVALID TRAFFIC
Filtration of invalid site and app activity is critical for accurate and consistent counting of users. Examples of invalid traffic can include: General Invalid Traffic (ex: bots, spiders and crawlers, and data center traffic determined to be consistent source of non-human traffic) as well as Sophisticated Invalid Traffic (ex: hijacked devices, hijacked sessions within hijacked devices, hijacked ad tags, invalid proxy traffic etc.) For more information, see **MRC Invalid Traffic Detection and Filtration Guidelines Addendum**.

FREQUENCY CAPPING
The process of restricting the number of times a set of creative or content is delivered to a consumer.

HARDWARE BASED DEVICE ID
A device-generated identifier set and/or made available by the device's operating system. Users usually cannot control or change a device-generated identifier. Examples include device specific MAC address and UDID.

HASHING (AND SALTING) IDS
Security enhancement processes used in the storage and management of databased IDs

IDENTITY MAPPING
Practice of establishing (deterministically or probabilistically), linking, and storing consumer identifiers (e.g., cookies, Advertising IDs, statistical IDs, IP addresses)

MATCH RATE
Match rate is the percentage of unique records in a data set that can be matched to an identifier in a marketing solution provider's database.

STATISTICAL ID
An identifier derived and assigned by an algorithm to determine a device or user based on the values or a combination of standard attributes made available by the device. This analysis is largely dependent upon device information passed in HTTP headers of ad requests, namely device type, operating system, user-agent, fonts, and IP address. Some attributes can change over time due to device changes or updates.

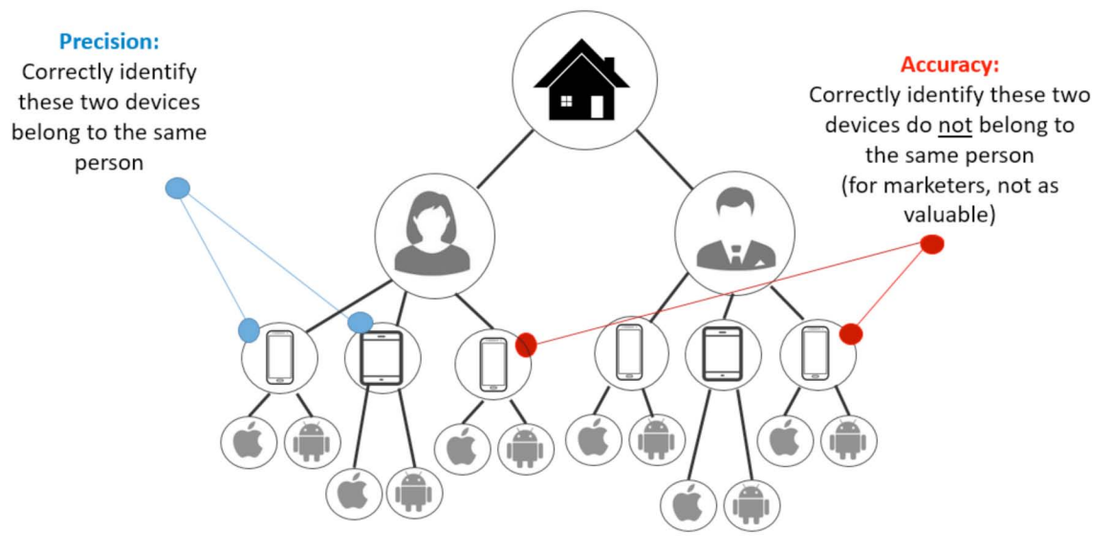
UNIQUE USER
A person using an application and exposed to advertising messages, as determined through registration, user self-identification or some form of heuristic. A Unique User is an unduplicated person using an application and exposed to advertising messages during a reporting period. For the requirements for reporting a Unique User metric, refer to the IAB Audience Reach Measurement Guidelines, available at **www.iab.com**

USER AGENT
Text sent as part of the HTTP protocol that identifies aspects of the software accessing the internet and the web-enabled device on which it is running. This information typically includes the application name, its version, the host operating system, and the user-preferred language. See IAB Networks & Exchanges Quality Assurance **Guidelines**

WEBVIEW
A View within an app that displays web pages. In the **Android** operating system, the WebKit rendering engine is used to display web pages.

ADDITIONAL NOTES ON ACCURACY VERSUS PRECISION

Another way to look at the challenge (and confusion) surrounding Accuracy versus Precision is to look at it in the context of the marketer's goal of correctly or "precisely" identifying two devices that belong to the same person (shown by the blue arrows below) versus the lower value process of "accurately" identifying two devices that don't belong to the same person (shown by the red arrows below)



Source: Drawbridge

In colloquial (non-mathematical) contexts, accuracy and precision are often used interchangeably (and misused in the process). The difference is especially important when working with analytics data. In a nutshell, accurate measurements return correct values and precise measurements return consistent values.

In the context of identity management solutions, accuracy means knowing to a certain percentage that this device may (or may not be) that person. Whereas precision calculates—to a percentage—that this is the person to whom the device is matched. What marketers ultimately care about is predictions of correct device matches. They don't care very much about the non-match predictions. But the reality is there will be many more non-matches than correct matches (which can skew accuracy scores, making them look better than they really are. So when someone says: "This match is 99% accurate", it actually means "I'm 99% sure I may (or may not) know what this device is, or who this person is." Whereas precision means, "I know 99% that this is the person I'm talking to." Ideally you want to get results that are not only correct, but are consistently correct.

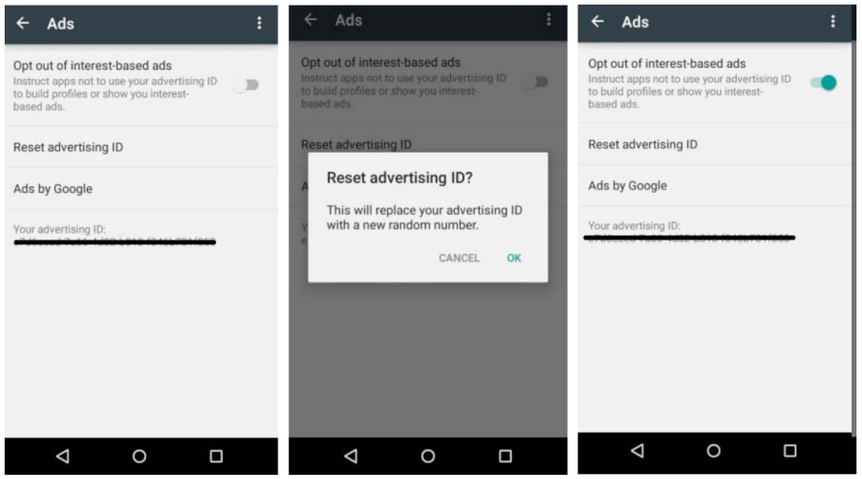
MARKETER'S COMMON TERM	DATA PARTNER / VENDOR TERM	WHAT MARKETERS CARE ABOUT
Accuracy	Precision	Percentage of correctly identified matches among all matches identified within the device graph
Reach (aka scale)	Recall	Percentage of matches correctly identified from all possible correct matches

MECHANISMS FOR CONSUMER OPT-OUT OF ADVERTISING IDS

GOOGLE ANDROID ADVERTISING ID OPT-OUT: App developers and associated marketing services providers can–assuming the consumer has not opted out of receiving targeted advertising via the platform settings—leverage Google Android's unique Advertising ID for advertising purposes. There is an Android advertising ID API that enables app developers to access the ID stored on the user's devices.

These IDs can be reset by consumers through the following steps:

- Open Google Settings on the Android device by tapping menu
- Tap on Google Settings and then Services
- Tap on the Ads menu under Services
- Tap on "reset advertising ID" (the user's current advertising ID will appear on this page)



- A reset confirmation prompt is then displayed.
- Click "OK" to reset and the new Advertiser ID will be appear.

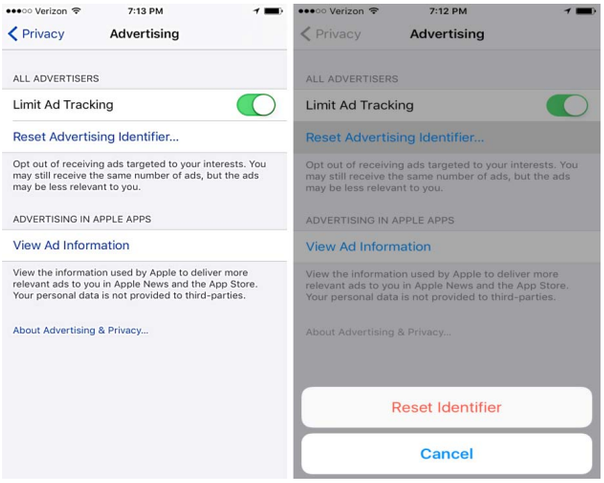
Once the new Advertiser is assigned, advertisers are not permitted to link prior consumer behavior to the device (assuming marketers used the prior advertising ID to target ads). Consumers may also opt-out of interest-based ads via a link on the same menu.

Google policy prohibits app developers and associated marketing companies from using the advertising ID for interest tracking and targeting purposes following an opt-out. Only non-interest based ads may be shown to users who have opted out in interest based ads. Google guidelines state that app developers must respect user's personalized ad flag preferences and may not link the Advertising ID to personal identifiable information or persistent device IDs (such as the previously mentioned hardware-based IMEI or Mac address) without explicit user consent. As Google states in their developer guidelines:"You must abide by a user's 'Opt out of interest-based advertising' or 'Opt out of Ads Personalization' setting. If a user has enabled this setting, you may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising. Allowed activities include contextual advertising, frequency capping, conversion tracking, reporting and security and fraud detection. Visit the Android Developer Policy Center for more detail on **usage of the Android Advertising ID.**

APPLE IOS ADVERTISING PREFERENCES AND OPT-OUT PROCESS

Apple's iOS also enables consumers to opt out of interest-based ads served within mobile apps by selecting the "Limit Ad Tracking setting". The **process** is as follows:

- Choose "Settings" from the iOS home screen
- Select Privacy
- Select Advertising
- Select "Limit Ad Tracking"



NOTE: In iOS 10 and later, when the consumer has selected "limit ad tracking", the **value** of the IDFA advertising identifier is set to: 00000000-0000-0000-0000-000000000000).

OPT-OUT PROCESS FOR IOS SAFARI MOBILE BROWSERS

Apple smart phone owners may also opt out of ad tracking on Safari through the following steps:

- Select "Settings" from the home screen
- Locate the Safari browser app icon
- Select "Do Not Track"

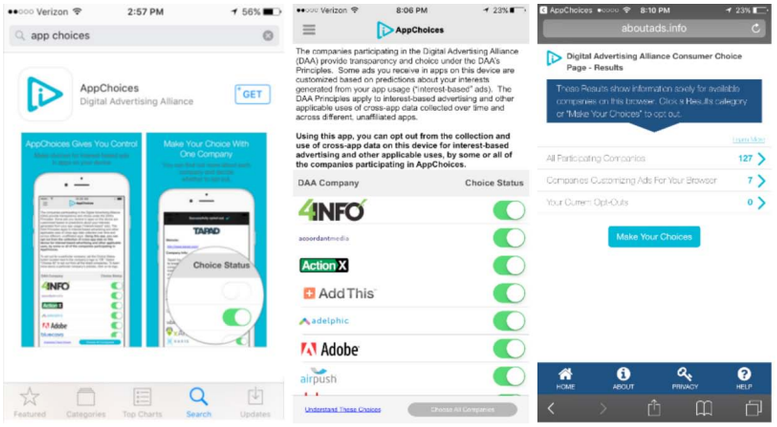
NOTE: Apple iOS does not allow the use of cookies for 3rd party advertising serving purposes. However browser cookies may be used by websites to store information about user visits and shopping cart preferences and to serve more relevant content and offers. Consumers have the option with their Safari browser privacy settings to **clear their browsing history** and cookies and, while using the browser, to **enable private browsing**.

OTHER OPT-OUT MECHANISMS

The DAA (**Digital Advertising Alliance**) is an industry body focused on giving consumers more control and better understanding of interest-based ads that are served based on online behavior. IAB and many other organizations are members of DAA. Their AdChoices privacy management solution (for web and mobile web) and App Choices service (for in app advertising) are visible to consumers in the form of icons displayed in or around ad creative. When the consumer clicks the icon they're presented with information about the data providers and ad servers that are used to select and serve ads and they can opt out from receiving interest based ads in the future. Consumers can download the DAA AppChoices app on iOS and Android devices to opt out of interest-based ads from a particular company, or they can "select all companies" with a click.

AppChoices
Control for in-app advertising

The Digital Advertising Alliance (DAA) enforcement of its guidance on the Application of the DAA Principles of Transparency and Control to Data Used Across Devices (DAA cross-device guidance) began on February 1, 2017 and is independently enforced by the Council of Better Business Bureaus (CBBB) and the DMA, which provide ongoing independent oversight of the DAA Principles.



The guidance available **here** from the Digital Advertising Alliance explains how self-regulatory principles apply to browser and app-based choices made by consumers, and to data collected on the user's device for use elsewhere. The DAA cross-device guidance applies to all companies engaged in data collection and use. Whether a company is directly collecting multi-site data or cross-app data or transferring data to a non-affiliates, all parties (collectors and transferees) must provide data use disclosure and links to mechanisms like **DAA**'s **AdChoices** or **App Choices**. The consumer's opt-in and opt-out choices apply to future data collection, use and transfer of data for marketing purposes.

IAB supports these guidelines and mechanisms that enable a consistent self-regulatory framework. Consumers increasingly own and use multiple connected devices per day and purchase new ones every couple of years. This creates difficulties for both the marketers seeking to reach and understand their consumers across devices in order to deliver more relevant advertising, and for the industry to provide those consumers with choice related to interest-based advertising. This is why it's important that the industry continue to self-regulate by implementing and complying with these industry guidelines so that marketing innovation can continue to flourish. Companies with questions regarding their compliance obligations and the guidelines enforcement process can contact the DMA at **ethics@the-dma.org**.

PRIVACY RESOURCES RELATED TO THE USE OF MOBILE LOCATION DATA

From: IAB **Mobile Location Data Guide for Publishers**

OBTAINING USER PERMISSIONS FOR IN-APP LOCATION DATA

Brands which publish mobile apps should obtain the end user's permission, and to provide notices describing how their app products and services use and share location data and what the consumer's choices are. User's permission may be obtained via a simple opt-in message by which the user indicates that they understand their location information is being collected by the publisher.

OBTAINING USER PERMISSIONS FOR LOCATION DATA IN MOBILE WEB

The process of confirming permission to collect mobile location data on mobile web is different from that of mobile apps. With mobile web, assuming the user's device-level and browser-specific location access settings are turned on—users will be prompted when visiting a web site requesting current location data–with a message saying "web site [URL] would like to use your current location". At that point, the user can choose "Don't Allow" or "OK". This request must display the website hostname, and the option for the consumer to accept or deny permission.

While there are nuances depending on the platform, typically, iOS and Android apps that request user location must also get the user's permission via a pop-up. This might happen the first time the app is open, but other times this might occur when a user attempts a function that utilizes location services. Usually, once a user grants an app permission to use their device's location data, it retains the setting moving forward unless the user changes the permission in the location services setting within the device settings. A user is highly likely to grant permission for an app that has clear benefit or justification for accessing the device's location. Again, the brand or publisher should clearly state in their privacy policy why they are collecting this information and how it may be shared.