

Mobile Identity for Marketers

ESPC 2017 Annual Meeting October 24, 2017 WilmerHale 1875 Pennsylvania Ave., NW Washington, DC

IAB EMPOWERS THE MEDIA AND MARKETING INDUSTRIES TO THRIVE IN THE DIGITAL ECONOMY.

iab.

We Are Digital Media's Biggest Tent

650+ LEADING MEDIA COMPANIES RESPONSIBLE FOR SELLING 86% OF U.S. DIGITAL ADVERTISING





IAB and Our Partners





What IAB Does and How We Do It





IAB Data & Ad Effectiveness



All in service of ensuring and assessing...

Data & Ad Effectiveness Charter:

Fulfill data's central role in planning, activating, and measuring effective advertising (for consumers, publishers, and marketers) by raising awareness, publishing and driving adoption of guidelines and best practices, and informing tools and standards.



IAB Data & Ad Effectiveness – Scope

		Consumers	Marketers	Publishers
Data (Center of Excellence)	Data Benchmarks & Activation		\checkmark	\checkmark
	Identity & Audience Data	\checkmark	\checkmark	\checkmark
Ad Effectiveness	Consumer Experience: Relevance/Targeting & Personalization	\checkmark	\checkmark	
	Consumer Experience: Privacy/Controls	\checkmark		
	Measurement & Attribution		\checkmark	\checkmark
	Buying Automation		\checkmark	\checkmark
	Selling Automation			\checkmark
	Publisher Monetization/Design Insights	\checkmark		\checkmark



Identity Management – Why it Matters





Mobile Identity Whitepaper Objective



Mobile Identity 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 dentify 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: Adobe. Cadreon. Centrs. comSorsor. Conversant, Drawhridge, Flashalking, Foursquare, Google, GumGum, Jumpstart Automotive Media, Jun Group, Kochava, Lonely Planet, Medialiets, Nielsen, NinthDeoimal, OpenX, Stornek, TapAd, The Weather Company, Vieldmo

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 <u>Forrester</u>, the average US addult juggles more than four connected devices. Three-quarters use a smartphone and more than half use a tablet. As the connected devices we use poliferate, 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.



White paper and 1-sheet focused primarily on mobile (secondarily on cross-screen):

- Different approaches and solutions for identifying users on mobile & cross-screen
- How mobile differs from desktop
- Answers to buyers most frequently questions
- Addresses privacy best practices

Primary Audience Marketers, Advertisers and Agencies

Secondary audience: publishers

Released at IAB Mobile Symposium



Building on Earlier Documents



2013 Paper highlighted limitations in cookies function on mobile devices. References client/device generated ID's and Statistical ID.

IAB.com search "Cookies 101"



Released in August of this year, includes chapter on device graph as a foundation for a holistic view of message delivery and definitions of deterministic / probabilistic methods

IAB.com search "Attribution Primer"



Privacy and Tracking in a Post-Cookie World

A whitepaper defining stakeholder guiding principles and evaluating approaches for alternative models of state management, data transparency and privacy controls for consumers, publishers, and trusted third parties.

JANUARY 2014

2014 paper explored potential alternatives to cookies. Examined needs of consumers, publishers, advertisers and solution classes: server issued (cookies), device-inferred (algorithm driven IDs), client generated (browser, app, OS generated), network inserted (3rd party servers between user device and publisher servers), and cloud synchronized (centralized service that all parties would potentially agree to work with)



Cross-channel audience identification & measurement cited as key focus areas by marketers and media practitioners

"Which use cases do you expect will most occupy your time, attention and resources during 2017?"





Marketing Begins with Identity Mapping and Matching

The practice of establishing (deterministically or probabilistically), linking, and storing consumer identifiers (e.g., cookies, device IDs, statistical IDs, IP addresses)

Essential to:

- Data hygiene
- Accurate audience segmentation (targeting/addressability)
- Consumer experience / personalization
- Delivery measurement
- Multi-touch attribution
- **Publisher liquidity / yield** (especially mobile)

And increasingly critical with the rise of mobile and cross-device media consumption...





How Identity is Used

Marketing applications of mobile and cross-device identity

TARGETING

- 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
- FREQUENCY CAPPING limiting impressions delivered to users across devices
- AUDIENCE EXTENSION reach audiences beyond a publisher's owned and operated properties
- DYNAMIC CONTENT PERSONALIZATION tailoring messages based on criteria such as behavior, interests and demographics

MEASUREMENT

- REPORTING identify, segment and analyze users, gain insights into behavior, habits, content and offer response patterns. Metrics can include impression delivery (reach and frequency) as well as ad engagement and conversions
- ATTRIBUTION identifying a set of user actions ("events") across multiple screens and touchpoints that contribute 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 | Ad ID vs Cookies

Device / Ad IDs

TYPES Hardware IDs	 EXAMPLES Universal Device Identifier (UDID) Media Access Control (MAC) Address 	NOTES Non-privacy supporting
Software-based Advertising IDs	 Google Android Advertising ID (AAID) Apple iOS Advertising ID (IDFA) Microsoft Mobile OS Advertising ID 	Privacy-supporting (may be disabled / reset by user). Used for advertising purposes

Cookies



"Cookies Don't Work on Mobile"



Cookies on mobile work (to an extent)

- Their persistence and acceptance can vary
- NEW: in iOS 11 Safari now blocks passing of cookies to 3rd parties determined to be "trackers"

Cookies in Mobile Browser: 3rd party cookies supported in Android (not iOS, where default Safari setting has 3rd party cookies disabled)

Cookies in Mobile App: cookies handled via "webview" (enables access to content/sites without leaving app), stored in appspecific space called "sandbox" <u>Result</u>: advertisers cannot follow users from app to app with cookies like they can on browser.



Safari Cookie Blocking | Update

With the release of iOS 11 in September came an updated version of the Safari browser with a feature called **Intelligent Tracking Prevention** (ITP). Enabled by default, ITP blocks certain cookies from websites

Before ITP: Safari desktop & mobile browsers blocked 3rd party cookies by default (1st party cookies were traditionally safe from automatic blocking/removal, as they retain user sessions/login status, shopping cart info, website settings etc.)

<u>With ITP</u>: Apple removes possibility of 1st party user event establishing a more persistent cookie readable in 3rd party contexts.

- 1) Safari determines algorithmically whether a web domain has the ability to track a user across sites
- 2) When a domain is flagged as being able to track a user across sites, 2 new rules are applied to cookies from that domain:
 - 24 hours after most recent 1st party interaction with the domain, cookie payload for that domain becomes unavailable in a third-party context
 - 30 days after most recent 1st party interaction with the domain, cookie payload for that domain is purged



Implications of ITP for Advertising

Eliminates method of establishing consistent, cookie-based identity for use by 3rd party ad systems (ultimately depreciates value of cookies in match tables). Other implications:

- Publishers with (a) frequent first-party engagements with users and (b) their own advertising ecosystems will be less affected than smaller publishers (who are more reliant on 3rd party tracking)
- Publishers with significant off-property ("network") business will be significantly affected
- Industry efforts to create standard ID (using cookies) may be further challenged as will industry wide opt-out
- Minimal impact on short-term conversion tracking (cookie remains available for 24 hours after it's been set during click), and web analytics (whose systems generally depend on 1st party cookies set by JavaScript)



Short-term Solutions to Mitigate ITP Impact on Reach, Targeting, Measurement (within browser-based and in-app webview Safari environments)

Focus on establishing a first-party assets (continually refresh that 1st party asset vs relying on 3rd-party data synch)

Buyers:

- Develop first-party data strategy by leveraging first-party cookies in combination with ID matching to protect and activate data assets.
- Advertisers can serve 1st party cookies from their own sites, warehouse in a 1st party location (onboard data from external sources to enrich)
- Apply non-cookie-based technologies for user identification and impression valuation (Probabilistic and statistical approaches are the most common)

Publishers:

- Build data assets against first-party cookies and store in ways that retain first-party relationships with users (warehousing done via white label DMP, or bespoke/custom DMP).
- Consistently use same ID matching service as buyers and DMP partners (allows buyers to decision on publisher first-party data by mapping that data to the identity vendor's user ID for un-fragmented activation).
 <u>Note:</u> not all identity vendors develop their own ID, should factor into partner selection in this scenario



Other Ways of Identifying Users Across Screens

Access to Advertising IDs - not a given

Marketers assume Ad IDs gathered by publishers openly accessible / transferable (not always the case, more so in RTB settings)

Device graphs

Rely on two distinct approaches: probabilistic and deterministic methods Challenges with both approaches include accuracy testing and controlling for errors (ex: friends, family, using same device)

Deterministic Approaches:

Relies on PII (ex: email, ph #, mailing address, credit card info) to identify / target same user across screens

- User logs in or makes a purchase, deterministic providers associate those device IDs or cookies in a device graph
- Because of ability to authenticate across devices, deterministic approaches are thought of as most accurate
- Downside is perceived lack of scale across devices (hard limits to the amount of reg data that companies have)
- Because of this, some deterministic providers may also leverage probabilistic device inferences

Probabilistic Approaches

Incorporates thousands of anonymous data points (device type, OS, location data etc.) to identify statistical correlations between devices.

- Signals may be also be drawn from multi-user identifiers like IP addresses or geographic regions.
- Based on these signals, probabilistic techniques attempt to determine devices likely used by the same person.
- Once determination is made, provider assigns particular statistical ID to the device.



Precision (accuracy) and Recall (reach or scale) in Probabilistic Approaches

High Precision Graph



Of the devices matched, all are correct (but leaves many devices unmatched)

High Recall Graph



A lot more devices are matched (but not all matches are correct)



Linking Across Data Sets | Tactics for Bridging Web to App



Combination of web-based IP addresses, cookies, app-based Ad IDs, 1st and 3rd party data and location identifiers

Screens vs Users | How Audiences are Counted Matters

A consumer with a single device can have multiple ID's



One User, One Screen, Multiple ID's

AAID – Google Android In-App Advertiser ID 97987bca-ae59-4c7d-94ba-ee4f19ab8c21

SHA1 – Hashed Ad ID d42b4890298fc4821a52c11f24e2a8ac06fa10b0

ba06c008973b8a1bff6e087c6149227f

AAID – Google Android In-App Advertiser ID 97987bca-ae59-4c7d-94ba-ee4f19ab8c21



Mobile Cookie ID (Third Party) BEAF1TcaSuLYABiAwMFAg==

Mobile Cookie ID (Third Party) vEOP2CcuSvPUTiVAmcGF-++

TIP: Confirm the process by which your vendor is matching IDs to users

Source: Conversant



Example Identity Match Processes

- Since cookies are domain-specific, those created by one 3rd-party cannot be read by another unless matching process used
- "Cookie synch" used by companies to jointly identify user's browser



22

- Match table created to map IDs of one platform to IDs for that same user, on another.
- Ad IDs gathered through mobile in-app can also be linked with cookie IDs



- **ID clusters** combined in **device graph**-building process
- Result is data that creates connections between IDs based on anonymous and/or login data

NOTE: Post Safari ITP techniques going forward will likely be based on:

- (1) a short-interval sync leveraging 1st-party assets available within 24 hours;
- (2) passively executed sync using HTTP header fields (user agent, referrer, etc.), on-page script, or other probabilistic approaches
- (3) an actively requested sync through user-provided data such as email address or via an explicit authentication



Marketer Considerations for Data Linkage / Matching Vendors

- Discuss service pricing model (ex; flat rate, CPM rate, matched user rate)
- Determine data onboarding process/costs (how client segments / data handled to ensure compliance)
- Question vendor processes for matching devices, cookies and IDs
- How does the vendor measure performance for their solution?



Privacy Resources

- Apple iOS Advertising Preferences and Opt-Out process
- Other Opt-Out Mechanisms
 - DAA (Digital Advertising Alliance) AdChoices and App Choices
- User Permissions for Location Data In-App and mobile web
- GDPR: IAB working group forming to help educate





Other IAB Identity Initiatives

Identity Standards Working Group Examining Identity solutions and key quality components:

- Reliability (persistence) of underlying data currencies used
- Processes to associate nodes to graph
- Graph maintenance over time
- Consumer privacy considerations





IAB Members Contact: committees@iab.com



Thank You

