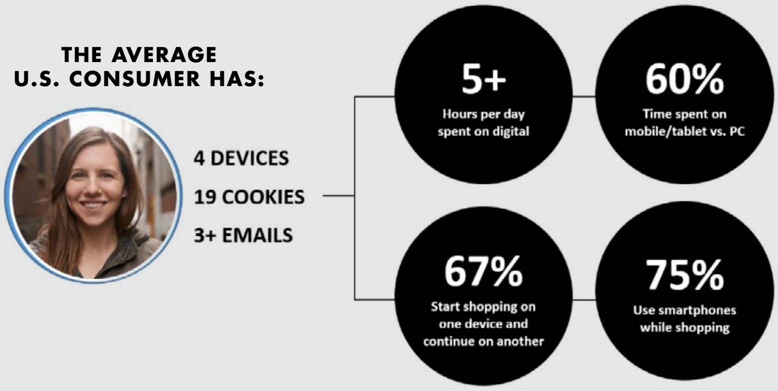
MOBILE IDENTITY GUIDE FOR MARKETERS

WHY A STRATEGIC APPROACH TO MOBILE IDENTITY MANAGEMENT MATTERS

The typical U.S. consumer has several connected devices and expects seamless ad and content experiences across those devices. Today, the challenge for marketers and publishers is how to effectively target those consumers with the right messaging, at the right time, regardless of the device they're using at any moment.

In order to effectively market to mobile audiences and capture similar reporting metrics available on desktop, advertisers must leverage a mix of tactics and solutions.



THE AVERAGE U.S. CONSUMER HAS:

4 DEVICES

19 COOKIES

3+ EMAILS

5+ Hours per day spent on digital

60% Time spent on mobile/tablet vs. PC

67% Start shopping on one device and continue on another

75% Use smartphones while shopping

Sources: Conversant, Forrester, IPSOS, ComScore

MARKETING APPLICATIONS OF MOBILE AND CROSS-DEVICE IDENTITY

The uses of mobile and cross-device identity spans the full spectrum of digital marketing activities. Identification data can be broken down into two primary categories: **TARGETING** and **MEASUREMENT**.

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

Mobile device manufacturers and operating system providers offer several identifiers for differentiating individual 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 MOBILE IDENTIFIERS

TYPES	EXAMPLES	NOTES
Hardware IDs	• Universal Device Identifier (UDID) • Media Access Control (MAC) Address	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

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

IAB.COM/MOBILEIDENTITY

ACCESS TO ADVERTISING IDS

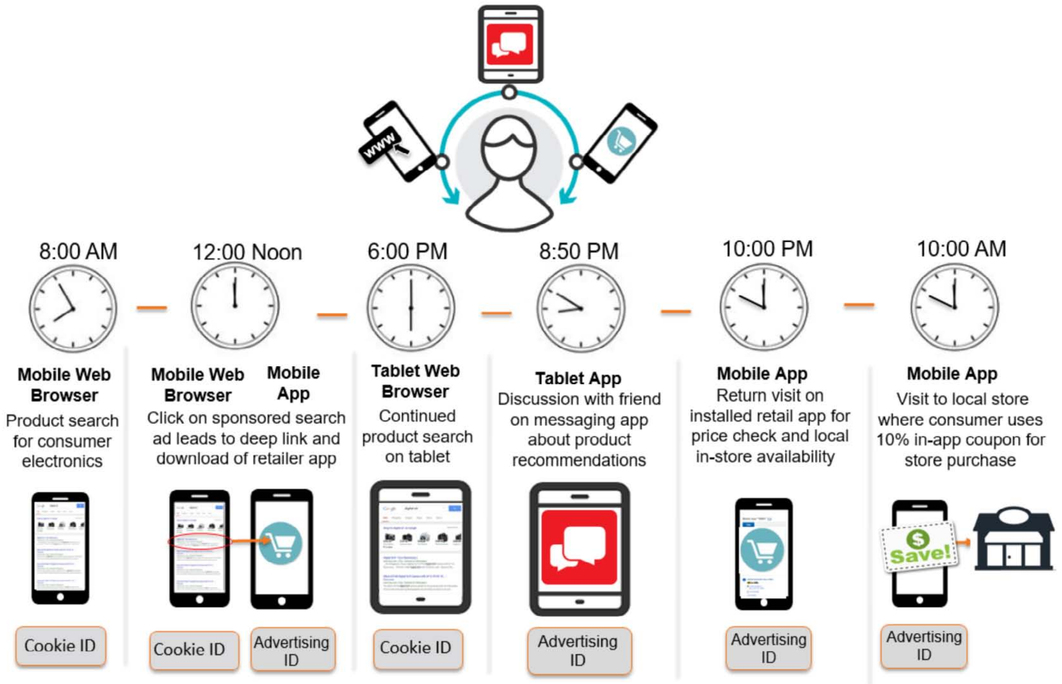
Many marketers assume that Advertising IDs gathered by publishers are openly accessible and transferable to other entities for marketing purposes. However, this isn't always the case. In RTB (real-time bidding) settings, access to these Advertising IDs is more common, but outside of that context, some publishers do not share them. In cases where the publisher has the option to share Advertising IDs with marketing partners (based, for instance, on their user agreements and business rules), there may be various contractual and operational restrictions. 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.

MYTH: 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 mobile devices, because of browser limitations and fragmented environments, cookies cannot be relied on as a source of truth for identifying a device. 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 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. For more information, please refer to **IAB Digital Simplified "Understand Mobile Cookies."**

LINKING ACROSS DATA SETS: TACTICS FOR BRIDGING WEB TO APP

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 (for example the web to app to store customer journey illustrated here). For this reason, a combination of solutions may be needed accomplish the full scope of a marketer's needs, including web-based IP addresses, cookies, app-based Advertising IDs, 1st and 3rd party data and location identifiers.


WWW
8:00 AM
Mobile Web Browser
Product search for consumer electronics
Cookie ID
12:00 Noon
Mobile Web Browser
Mobile App
Click on sponsored search ad leads to deep link and download of retailer app
Cookie ID
Advertising ID
6:00 PM
Tablet Web Browser
Continued product search on tablet
Cookie ID
8:50 PM
Tablet App
Discussion with friend on messaging app about product recommendations
Advertising ID
10:00 PM
Mobile App
Return visit on installed retail app for price check and local in-store availability
Advertising ID
10:00 AM
Mobile App
Visit to local store where consumer uses 10% in-app coupon for store purchase
$ Save!
Advertising ID

This document and **white paper** 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. 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**.