2013

Mobile Cookies 101

Understanding the Limitations of Cookie-Based Tracking for Mobile Advertising

December 2013

Published by IAB Australia's Mobile Advertising Council based on IAB US' Mobile Cookies 101, published in November 2013

Acknowledgements

This document was developed by the US Mobile Ad Operations Working Group, part of the IAB's Mobile Marketing Center of Excellence and adapted for the Australian market by IAB Australia's Mobile Advertising Council.

About IAB Australian's Mobile Advertising Council:

The IAB Mobile Advertising Council was established in 2011, since then, its remit has been to:

- Evaluate the needs of the Australian mobile advertising industry
- Establish a program of work for mobile advertising
- Produce, fund and promote mobile research studies
- Produce and promote mobile standards and guidelines

The IAB Mobile Advertising Council meets on a monthly basis and has industry wide representation of mobile experts from across publishers and media agencies. The council provides a broad, collective voice in addressing the key issues and challenges faced by the industry.

Member companies of the Mobile Advertising Council include:

Big Mobile
Carsales
Fairfax Media
Google
Ikon Communications
inMobi
MCN
Mediacom
mi9
Network TEN
News Corporation
Pandora
REA
SBS
Telstra
Yahoo7!

IAB Australia member companies are able to nominate a representative for this council on the IAB Australia website

IAB contact:

Gai Le Roy, Director of Research gai.leroy@iabaustralia.com.au

About the IAB US' Mobile Ad Operations Working Group:
The Mobile Ad Operations Working Group is dedicated to improving the operational efficiency of mobile advertising. The group meets regularly to talk through the challenges of mobile ad operations as well as initiates projects via sub-groups with the goal of improving the understanding and work process of mobile ad operations.

Representatives from the following companies participated actively in creating Cookies on Mobile 101:

24/7 Media
AdMobius
AOL
BlueCava
Datalogix
Fiksu
Jumptap
Millennial Media
Mojiva
The New York Times Company
Pandora
The Weather Channel

IAB acknowledges Dan Grigorovici of AdMobius and Toni Cruthirds of the New York Times Company, who chaired the effort to create this document, and Sabrina Alimi, now at FreeWheel, who managed this project during her IAB tenure.

About the IAB US' Mobile Marketing Center of Excellence:
The IAB's Mobile Marketing Center of Excellence, an independently funded and staffed unit within the IAB is charged with driving the growth of the mobile marketing, advertising, and media marketplace. The Mobile Center devotes resources to marketplace and consumer research, mobile advertising case studies, executive training and education, supply chain standardization, creative showcases, and best practice identification in the burgeoning field of mobile media and marketing. Our agenda focuses on building profitable revenue growth for companies engaged in mobile marketing, communications, and advertising and helping publishers, marketers, and agency professionals understand and leverage interactive tools and technologies in order to reach and influence the consumer. More information can be found at: http://www.iab.net/mobile

Table of Contents

Executive Summary

The rapid growth of the mobile marketplace motivates advertisers to run campaigns across mobile devices such as smartphones and tablets to reach their audiences who have integrated these devices into their everyday lives. Cookie tracking has become the status quo for measuring digital advertising campaigns on websites viewed via desktop browsers. Many features that allow advertisers and agencies to optimise their campaigns—such as frequency capping and re-targeting—are based on information provided by cookie tracking. Similar targeting and optimisation is needed for mobile campaigns as well, but the limitations of cookie tracking on mobile devices make it challenging.

While web browsing on mobile browsers allows for cookie tracking abilities similar to what exists in desktop browsers, user activity on mobile devices is more fragmented and often takes place outside the browser in multiple native applications ("apps"). This division of activity and the inability to share cookies across apps makes cookie tracking insufficient on mobile devices. For this reason, many wrongly assume that "cookies don't work on mobile." This document details the limitations of using cookies in different mobile environments and the impact this has on common advertiser requests.

Intended Audience

This paper was written for advertisers, agencies, and marketers who are familiar with common practices in digital advertising on desktop browsers—specifically cookie tracking and optimisation—but who need a better understanding of how these work on smartphones and tablets. While there is a need for campaign optimisation and tracking on mobile devices, the common cookie method introduces limitations that ad buyers need to understand.

1. Overview

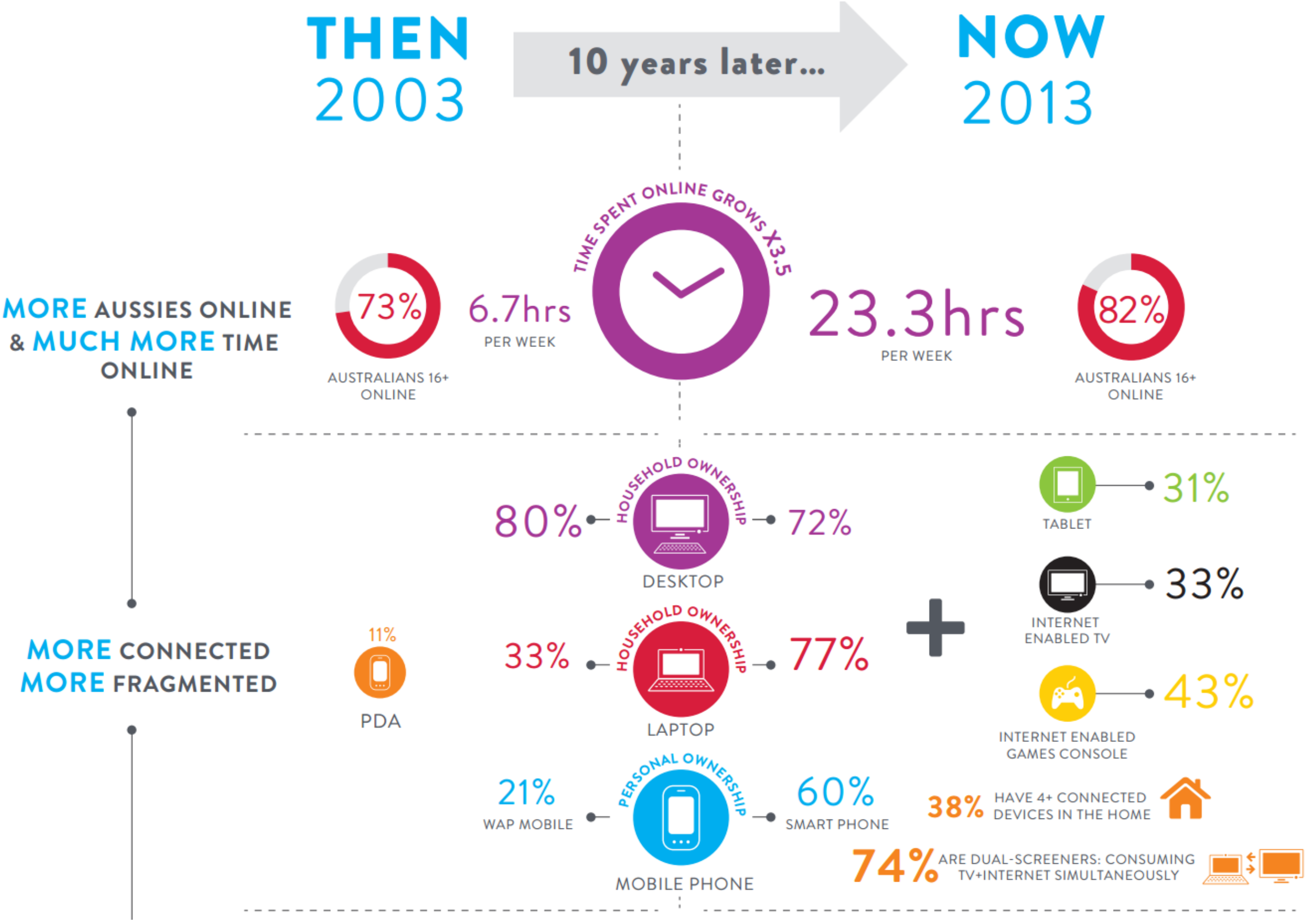
“Cookies don’t work on mobile” is a common assumption in the digital advertising ecosystem. However, this statement isn’t completely accurate which has caused much confusion in the marketplace. There are many differences and limitations in the way cookies function on mobile devices, such as smartphones and tablets versus desktop browsers. These restrictions make it challenging to utilise many of the optimisation strategies that have become commonly employed in digital advertising.

A cookie is a small text file that is stored on users’ web browsers typically to store a unique identifier that can be used in different ways to enhance the users experience such as enabling custom settings and keeping users logged in. Used by most content publishers in the digital advertising marketplace, cookies often store additional information such as what ads were recently seen and the publisher websites they were displayed on. While it is not technically prevented, it has become industry best practice to not store any personal identifiable information (PII) such as name or address via cookies.

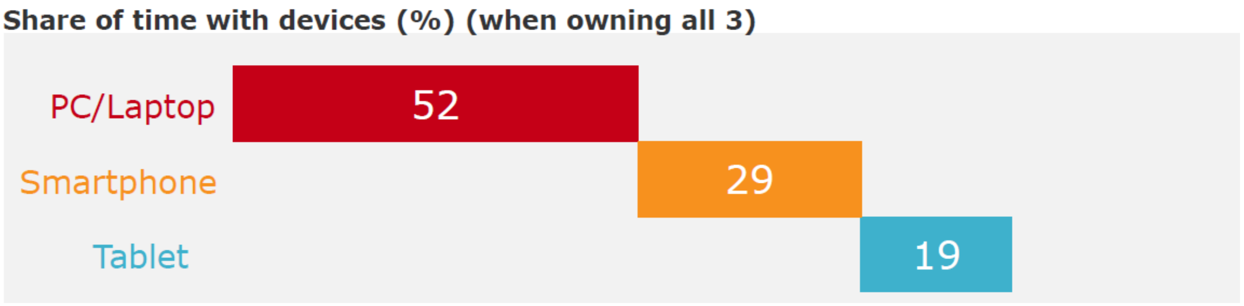
This combination of information stored within a cookie and tracking activity over time is useful to those managing advertising campaigns as it provides information that can be used to optimise desired audience and track effectiveness of spend with things such as frequency capping, audience targeting, and conversion tracking.

With consumers’ time spent browsing the Internet spreading across multiple devices, it brings up questions about effective campaign optimization on mobile platforms, particularly smartphones and tablets. Campaign managers need the same tracking and optimization functionality that they have for desktop-based campaigns across all devices. While using cookies is the common way to do this on desktop, it is not as effective on mobile due to the limitations of cookie functionality that vary by device and environment as well as the fragmentation of user’s activity between apps and mobile web. Other tracking methods have been developed to overcome these challenges, but cookie tracking alone on mobile is of limited utility.

CHANGING DEVICE OWNERSHIP IN AUSTRALIA[1]



DEVICE OWNERSHIP CHANGING MEDIA CONSUMPTION[2]

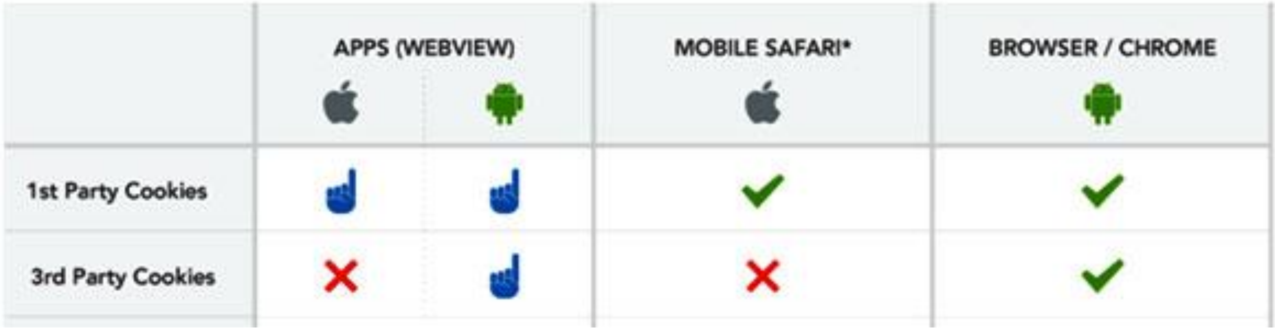


[1] Nielsen's Australian Connected Consumer Report 2013

[2] IAB TNS Australian Mobile Advertising Landscape 2013

2. Cookie Functionality in Mobile Environments

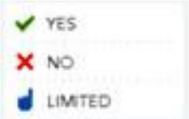
Most digital advertising campaigns executed on desktop devices are delivered through a browser. However, on mobile devices the user experience is more fragmented. Users browse the web via mobile browsers, but also install an array of applications (“apps”) that may also include advertisements. Cookie tracking abilities differ across environments, and it is important to understand how. In the discussion that follows, “First-Party Cookie” refers to a cookie whose domain is the same as the domain of the visited website. Example: cookie domain is news.com placed by http://www.news.com.



	APPS (WEBVIEW)		MOBILE SAFARI*	BROWSER / CHROME
		🤖		🤖
1st Party Cookies	☝	☝	✓	✓
3rd Party Cookies	✗	☝	✗	✓

“Third-party Cookie” refers to a cookie whose domain is different from the visited website. (Example: cookie domain is advertisinginfo.com placed on http://www.news.com).

*Installed browsers can behave differently. E.g., Chrome on iOS will support third-party cookies. Please note that this grid summarizes common experiences for Android and iOS only.



✓ YES
✗ NO
☝ LIMITED

2.1. Mobile Web

Mobile web refers to accessing a website through a mobile device's web browser whether that is a mobile optimised site, a responsive design site, or a desktop designed site. Cookie settings for mobile websites, just like websites viewed in a desktop browser, are dependent on the browser settings. Similar to desktop browsers, different mobile browsers will handle first- and third-party cookies differently. This acceptance affects what type of advertising features are available to the marketer.

For most browsers, there are three levels of cookies settings:

1. Allow all cookies
2. Allow cookies to be set only from sites you have visited (first-parties)
3. Block all cookies

Default Mobile Browser Settings

Mobile Browser	Default Setting	Note:
Opera	Allow all cookies	Option to adjust their settings to one of the more restrictive options
Chrome	Allow all cookies	Option to adjust their settings to one of the more restrictive options
Safari	Allow cookies only from sites you have visited (first-parties)	Blocks third-party cookies by default and has done so for the past decade. Users have the option to change this setting to allow third-party cookies to be set.
Firefox	Allow all cookies	In February 2013, changes were released to test branches of the desktop version of Firefox, changing the default browser settings from allowing all cookies to only allowing cookies from sites that a user has visited. This has yet to be released to the production browser.

Most advertising measurement happens through third-party vendors such as ad servers and ad networks. When third-party cookies are not accepted, these vendors cannot set a cookie, which is necessary to track the conversion. However, if a user clicks on an ad that redirects through the third-party vendor, the third-party becomes a first-party during that interaction and can set a cookie. Once a cookie is set, normal tracking will ensue.

2.2. Mobile Applications — The Sandbox

Within mobile apps, webviews are used to display online content such as a website or an ad. Cookies can be stored within a webview similar to the way they are stored in a browser setting. The webview (and, therefore the cookies stored in it) is unique per application. In the same way that Chrome and Firefox browsers do not share cookies on a device, mobile apps cannot share cookie information with each other or with the device's mobile web browser. Each app has its own private space on the device, 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 data within the application itself, but it is restricted from grabbing 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.

Apple explains why application sandboxes are important: "[The] App sandbox provides a last line of defense against the theft, corruption, or deletion of user data if an attacker successfully exploits security holes in your app or the frameworks it is linked against." (Apple, "About App Sandbox," Mac Developer Library, https://developer.apple.com)

3. Other Tracking Solutions in Mobile

The limitations of cookie tracking on mobile devices have led to the creation of many alternative methods of tracking to achieve results similar to advertising campaigns executed on the desktop. The approaches vary in methodology, implementation, and scale. The four most common solutions that are emerging in today's marketplace include ID-Based tracking, Statistical ID, HTML5 Cookies, and Universal Login.

Client/Device Generated Identifier

This method involves capturing a unique device identifier (ID) set and/or made available by the operating system. Examples include: Apple's Identifier for Advertisers (IDFA), Google's Android_ID, Universal Device ID (UDID) and Mac Address. UDID and Mac Address have been phased out due to the consumer's inability to control or manage privacy preferences and are no longer available in Apple's iOS7. In addition, there have been initiatives focused on developing an Open Device Identification Number (or ODIN), which prescribes platform-specific approaches for generating reusable device identifiers.

Statistical ID

This method involves a server-side algorithm for inferring the uniqueness of a user based on the values of a combination of standard attributes passed by every device. The list of available attributes contains but is not limited to, device type, operating system, user-agent, fonts, and IP address. This list may also vary by ad context (e.g. app vs. web) and some vendors may have access to different attributes than others. In addition, those attributes change over time due to regular device updates. Since statistical IDs are more profile-focused as opposed to identifying a unique user, there is an error rate because multiple devices may fall under the same profiles.

HTML5 Cookie Tracking

This method involves storing a cookie-like file in HTML5 local storage on the device. Similar to a cookie, when the user clicks on an ad, the identifier can be stored on the device and then be retrieved at the point of conversion. It is important to note that this file can only be set or retrieved when the browser is open and running. When tracking is needed in the app environment, the user experience is disrupted as the browser is launched to store the identifier.

Universal Login Tracking

This method requires consumers to log into different experiences using a preexisting login rather than create a unique one for that experience. Companies like Google, Facebook, Microsoft, and Twitter allow consumers to use their logins across other sites and applications. This type of tracking is limited to specific vendors, but enables companies with this type of universal login to gather data across applications and devices.

Each of these methods has different strengths and weaknesses, depending on what you are trying to measure and accomplish with your digital advertising campaign. No matter which one is being used, it is important to understand its limitations and the integrations needed to ensure the solution fits your needs.

4. Answers to Common Questions about Mobile Cookies

While the potential for mobile advertising is enormous, it is challenged by the lack of tools available to meet advertisers' needs for targeting their desired audience and tracking the effectiveness of their spend, which is powered in the desktop environment by the use of cookies. The most commonly used digital advertising capabilities for improving campaign performance such as campaign conversion tracking, targeting user segments, and frequency capping to avoid ad fatigue can be executed on mobile via the use of alternate tracking methods mentioned above.

4.1. Conversion Tracking

Conversion Tracking refers to the ability to track events that occur post impression (view-through) or click. Conversions normally occur after a user has visited an advertiser's site and can include actions such as filling out a form, making a purchase, or downloading an app, file, or coupon.

1. **Can you track click-based conversions on mobile devices?**

For mobile web, standard cookie tracking can be used to track click conversions assuming the ad impression and conversion happen within the same mobile web browser and a cookie has been set. Due to the mobile cookie limitations and complexity as noted in 2.1 above, conversion times are shorter in mobile browsers. Alternate tracking methods such as the referral string supported in the Google Play Store or statistical IDs are needed to enable tracking between mobile web and other environments such as an app store where a user has decided to install a new app.

Because mobile apps are "sandboxed," other tracking methods such as the use of Apple's IDFA and Google's Android_ID are typically used to enable cross-app conversion tracking. SDKs that are integrated into the applications to deliver ads are also used to collect these IDs. When a click/tap on an in-app ad takes a user to a landing page in a mobile browser, the IDs need to be passed via the landing page URL.

2. **Can you track view-through conversion on mobile devices?**

When an impression and conversion without a tap occurs in a mobile web browser where the tracking cookie has been set, view-through tracking is possible, but is not as reliable or accurate as on desktop due to the frequent turnover of cookies in mobile.

Since apps deliver ads via a webview with no navigational control, it is highly unlikely that a user converts within the same instance of a webview without tapping through via an ad.
If a user sees an ad in an application and then converts later without immediately clicking/tapping in a mobile browser, it cannot be easily tied back to the app impression because IDs such as Apple's IDFA and Google's Android_ID are not accessible in mobile browsers. However, conversions such as app downloads and app installations can be tied back with the use of IDs such as Apple's IDFA and Google's Android_ID.

4.2. Mobile Targeting

Targeting refers to the ability to serve ads based on particular parameters such as type of device, demographic characteristic, location, or browsing history. There are many targeting techniques that have become very popular in digital advertising and new ones that have gained traction due to new features available on mobile devices. Many of these targeting strategies don't require the use of cookie tracking and as a result are just as successful with mobile campaigns.

1. **Can you re-target on mobile?**

Re-targeting refers to the ability to target users based on sites they've visited previously for increased frequency or sequential messaging. Site re-targeting can be executed between mobile sites visited in a mobile browser when third-party cookies are available. Retargeting across applications is not possible with the use of cookies because they can't be shared across mobile apps, but other tracking solutions make this type of targeting possible. Users often float between the two worlds of apps and mobile web. The lack of common identifiers between mobile apps and mobile web make re-targeting across these environments very difficult, if not impossible, without specialised techniques.

2. **Can you do audience/user-based targeting on mobile?**

Audience or user-based targeting, which is the ability to show an ad specifically to visitors based on their shared behavioral, demographic, geographic, and/or technographic attributes, on desktop is typically done via cookie tracking and matching to additional demographic information. The limitations of cookies in and across mobile environments make this challenging with the use of cookies alone, but other tracking methods enable this type of targeting. The most direct method is to tie a device directly to real-world, offline data (e.g. purchase-based or public-record data) using anonymized email or postal addresses and device IDs. Another method is to collect opt-in data directly from consumers (e.g. age, gender, zip code) usually through registration. A third method is to infer information about a user based on usage behavior (e.g. types of apps used most frequently, time of day, websites visited), which is commonly used to reach users based on their interests.

3. **Can I geo-target (location-based targeting)?**

Geo- or location-based targeting is one of the most sought after targeting techniques on mobile devices because users physically take the devices with them everywhere they go. There are many ways to obtain location from a mobile device, which vary in geographical precision and opt-in requirements. Within an ad request call for mobile devices, location can be revealed as latitudinal/longitudinal coordinates via the device's GPS, which is more precise and accurate than using IP address. This can be used to target based on current location, such as geo-fencing (e.g. targeting all users within a radius around a particular retail chain) or geo-aware (all devices within a particular state, postcode, suburb). Some companies overlay additional context about the location to target things such as a device in a shopping mall vs. concert venue vs. park. None of these methods of location targeting require the use of cookies. Another strategy is to observe a device's location over time to build an audience profile (e.g. device moves around the country, often on weekdays = business traveler); this type of targeting will often be positioned as user-based targeting and, as a result, needs the use of a unique identify as noted above.

4. Can I target by mobile device and OS?

Within an ad request call, a good deal of information is provided about the device itself which can be used for ad targeting. This includes the device operating system (e.g. iOS or Android), device type (e.g. tablet or phone), the model, the mobile carrier, and whether the device is connected via WiFi or through a carrier network. This type of targeting does not rely on the use of cookies.

5. Can I target based on content?

Many ad networks and large publishers allow marketers to run ads on select sites or applications. Often blocks of inventory will be grouped together as channels based on context (e.g. news, music, cooking) or inferred demographics (e.g. properties that skew heavily towards middle-aged women). This type of targeting functions similarly on mobile as it does on PCs because all it takes is categorisation of content and does not rely on the use of cookies.

4.3. Frequency Capping and Unique Reach

Advertisers commonly desire frequency capping, or restricting the number of times (frequency) the visitor is shown a particular ad. On the PC web, frequency capping is most commonly achieved by storing visits in cookies; however, with the limitations of the use of cookies on mobile devices, other mechanisms must be used to achieve the same effect. The challenge is to avoid unknowingly reaching duplicate users, which is even problematic on PCs as different ad networks do not share cookies.

1. **How is unique reach determined on mobile devices?**

Within mobile browsers, unique reach can be determined by the use of cookies the same way it is done on desktop browsers as long as a cookie has been set. However, the accuracy over time is limited due to the frequent turnover of cookies in mobile browsers.

Mobile applications are sandbox environments so cookies cannot be shared across them and, as a result, unique users cannot be identified across applications with the use of cookie tracking alone. Device IDs such as Apple's IDFA and Google's Android_ID can be used to determine the different applications that are installed on the same device and, as a result, are the same user. In programmatic environments, determining unique reach is still a challenge because the original IDs are typically obscured when being passed to different parties. For instance, a publisher may give an SSP/exchange access to traffic, but will obfuscate/encrypt an IDFA/Android ID before passing it to the SSP; the SSP, unaware it's been obfuscated, will further encrypt it before passing it to a DSP/buyer, who finally also encrypts it before delivery.

Determining the same user across both apps and mobile browsers is additionally challenging. Tracking methods such as statistical IDs try to solve this challenge, but come with limitations.

2. **How is unique reach determined across mobile devices and computers?**

Determining unique reach is even more complicated in this scenario unless a user is registered with a publisher that maintains (and the user employs) logins for their PC and mobile sites/apps. Outside of this, only limited technologies that rely on pattern matching exist to determine cross-PC-mobile usage.

3. How does frequency capping work on mobile devices?

Mobile web frequency capping within mobile browsers functions similarly to desktop browsers as long as cookies have been set, but is not as reliable or accurate as on the desktop due to the frequent turnover of cookies in mobile.

To frequency cap across applications, an identifier such as Apple's IDFA and Google's Android_ID or a statistical ID is necessary to determine that the same user is accessing multiple applications. The obfuscation of ID's in the supply chain makes frequency capping across different networks challenging.

Frequency capping across mobile apps and mobile web and/or PC websites can be done using probabilistic method, but it is challenging to achieve accuracy. It may be best to run these campaigns separately with separate frequency caps.

5. Conclusion

Mobile advertising is essential for brands and advertisers to reach the millions of users who have deeply integrated the use of smartphones and tablets into their everyday lives; however, the use of cookies to track and optimise mobile campaigns (as it is done in the desktop environment) is not sufficient. Cookie tracking can work in siloed situations on mobile devices, but other tracking methods have been developed to successfully track ad campaigns across environments. It is not exactly accurate that "cookies don't work on mobile." More precisely, cookies don't work across mobile environments, which is necessary to meet the needs for tracking and optimizing digital campaigns. Asking vendors and partners tough questions about conversion tracking, mobile targeting, and frequency capping will help ensure buyers understand and can trust the data they get back from their campaigns.

6. Mobile Terminology

Mobile Environments

Android Operating System: A mobile-based operating system developed by Google.
iOS Operating System: A mobile-based operating system developed by Apple to run exclusively on iPhone, iPad, and iPod devices.
Mobile Web: A website that is viewed through a device's web browser
Mobile App: An application that is designed to run on various mobile devices, such as smartphones and tablets
WebView: A browser view within an app that can display web content
WebKit: A browser layout engine that is used by a WebView to render web content
Software Developer's Kit (SDK): A pre-packaged piece of code that developers can incorporate into their work in order to avoid having to develop it from scratch

Metrics

Impressions: The count of ads that are served to a user
View Throughs: A measure of the number of conversions within a number of days (often 30 days) after a user viewed an ad, but did not click
Click Throughs: A measure of the number of clicks on an ad
Conversions: A measure of users who click through and complete a specific action on a website, such as a purchase, a newsletter signup, an app download, etc.

Cookies

Cookie: A small text file deployed to a browser by a visited website or advertisement that can contain information such as login settings, user preferences, geographic, and demographic information
First-Party Cookie: A cookie whose domain is the same as the domain of the visited website. Example: cookie domain is news.com placed by http://www.news.com
Third-party Cookie: A cookie whose domain is different to that of the visited website. (Example: cookie domain is advertisinginfo.com placed on http://www.news.com