COOKIE APOCALYPSE.

THE BIG CRUMBLE

ATOMIC 212°

CONTRIBUTING EDITORS

JAMES DIXON

CHIEF DIGITAL OFFICER

RORY HEFFERNAN

GENERAL MANAGER, MELBOURNE

SASCHA BONOMALLY

HEAD OF PERFORMANCE, SYDNEY

OLIVER FIFOOT

CLIENT LEAD

COOKIE APOCALYPSE: THE BIG CRUMBLE.

A BITE-SIZED SUMMARY

Major web browsers including Apple's Safari and Google Chrome have announced significant changes to the way they process Cookies (and other identifiers), which marketers use for everything from remarketing to sales reporting. Therefore it is essential to be aware of how these changes work, how they are affecting your business currently, and how best to plan for a future without them.

CONTEXT

Looking back at the year that was 2020, it's unlikely that major changes made to the way browsers process web Cookies will be the defining subject that springs to mind. However for marketers (along with the newfound joys and struggles of Working From Home) it's the hottest topic in Adland.

Following numerous privacy-focused updates to Apple's Safari browser (the first ITP update took place back in 2017), Google has taken its first major step in a similar direction, recently announcing that its Chrome browser would not support third party Cookies from 2022.

As the browser with the largest global market share, Google's announcement made many marketers jittery, while Apple added insult to injury with the unveiling of its latest Safari update, which seemed to target Google Analytics - naming the ubiquitous web analytics service in a screenshot as an example of trackers being blocked. Since then, Apple announced iOS 14 which surfaces the IDFA (Apple's user ID function which allows advertisers to track when a device engages with their brand or app) to all phone users, warning them that they may be tracked by advertisers and giving them the option to decline. Current estimates suggest that this latest change could affect up to 80% of targeted advertising on iPhones, and this comes with the much more abrupt ETA of September/October 2020.

Both Apple and Google (along with other browsers including Mozilla) have advocated for these tighter restrictions on third party Cookies in order to support increases in user privacy, security and putting individual browsing habits back into their control. So far Apple has taken the most dramatic steps of the two giants, with Google's softer 2022 target indicative of their wider stake in the digital advertising ecosystem.

From a digital marketing perspective, there are repercussions of these developments that will affect not just Adtech and Martech companies, but also those that work with them, including agencies and brands alike, making it important for all marketers to keep abreast of the updates. At Atomic 212° we see three core areas of impact to marketers:

- Remarketing
- Audience targeting
- Analytics (i.e. measuring website visits, return visits etc)

The implications are significant to digital marketing practices. This whitepaper examines the impact and solutions being developed.

THE TOPLINE

The announcement from Google was anticipated, and generous in its timeline for adjusting to the loss of third party Cookies. We anticipate that new solutions for remarketing, targeting and measurement will be developed in the coming months to enable continuance of these important marketing activities.

The following is a list of frequently asked questions that may be used to break down some of the contextual information, while also outlining Atomic 212°'s view on the future as well as strategic media buys to prepare for this significant change.

WHAT IS A COOKIE?

A Cookie is a small file that sits on your computer, put there by the web domain's server via the website you visit. It consists of a long, unique identifier and potentially other information such as the website's domain/URL. This unique ID is both computer and browser specific. In this instance the Cookie is particularly useful for both the website owner and the user, as it enables a history of a user's browsing behaviour to be tracked. Put simply, should that person leave and return (on the same device), their settings (for example their login) are kept just as they are. Most websites you visit use Cookies in some form, whether that's to track your behaviour on the site, personalise the content you see on your return, or to show you relevant offers should you leave the website without completing a purchase.

There are two types of Cookies:

1. **Session:** Temporary file that is created and used during the user's web session.
2. **Persistent:** Permanently stored and sits on a user's computer (until they are deleted by the user, or reach their expiration date set by the website).

HOW IS A COOKIE CREATED?

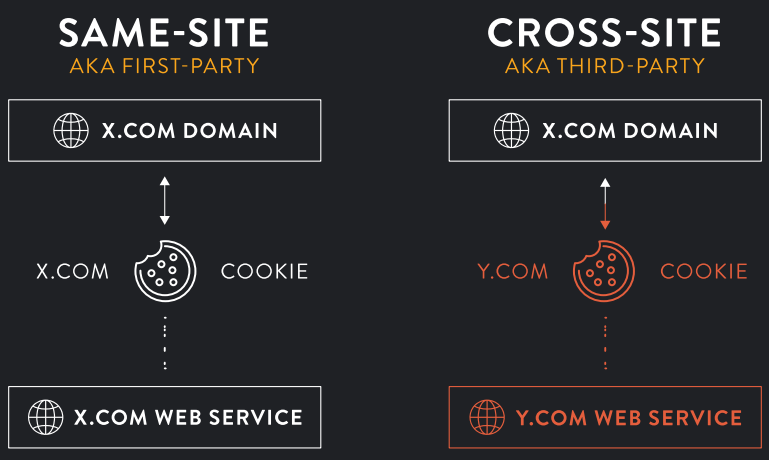
A Cookie is created when a user visits a website, usually for the first time, the website sends a message back to its server to request that a small file be placed on the user's computer via their browser.

The server sends back the file, along with the unique Cookie ID and other information for storage on the hard drive of the user's computer.

WHEN IT COMES TO PERSISTENT COOKIES WHAT TYPES ARE THERE?

There are two types of Cookies and they are labelled as:

1. **1st Party:** Created by the website and server you're visiting and contains URL information relating to the domain visited. For example, a user visits eBay for the first time, eBay's website will recognise that this is a first time user and send a request to its web server to create a Cookie file for storage. As the Cookie was generated by eBay, this is a 1st party Cookie.
2. **3rd Party:** These are generated in exactly the same way as a 1st Party Cookies but instead of the request going to the website's server it goes to a separate 3rd party server that has a different domain address. Because this server isn't part of the website domain a user visits, it is considered 3rd party. For example, upon a first time visit to eBay, eBay may deploy its ad serving Cookie owned and hosted by a technology provider (e.g. Sizmek). In this example, although the visitor visited ebay.com, the Cookie received would be communicating with a server based at sizmek.com, thus a considered 3rd party Cookie.



IF ALL COOKIES ARE THE SAME, WHY ARE THIRD PARTY COOKIES BEING BLOCKED?

Third party Cookies are on the chopping block largely due to the functionality described above. An increasing focus on user privacy and security, in the era of legislation such as GDPR, has highlighted processes and technologies that appear to transfer user data without their knowledge or consent. On top of this, Apple has cited cross-site fraud and forgery as a security risk present with the use of third party Cookies, and a key reason for their usage to be discouraged.

WHAT IS THE IDFA, AND WHY ARE APPLE CHANGING IT?

Similar to Cookies, but designed for mobile tracking, the Identifier for Advertisers (IDFA) is an anonymised device ID that Apple assigns to a user's device, enabling advertisers to track and measure user activity on mobile devices, such as online browsing behaviour or app installs. This technology is used widely across the online ecosystem, from key publishers to app measurement SDKs and martech providers.

In keeping with their increased focus on user privacy, Apple's latest iOS update will alert new and existing users when apps are attempting to track their behaviour, and whether they would like to opt-out of targeted advertising.

HOW SIGNIFICANT IS THIS TO MY DIGITAL MARKETING?

Whilst the Chrome timeline announcement is significant news, it has been in the pipeline for 2-3 years as a response to privacy requirements across the internet. The change is symptomatic of a larger issue facing marketers, particularly those that have specialised in digital. Arguably the success and growth of investment in digital channels over the past 10 years can be attributed primarily to two key factors:

- The ability to directly measure the ROI from digital advertising.
- The ability to identify, target and track prospective customers across the web (largely through retargeting).

The general trend toward user privacy, and the impending Cookie apocalypse, has rightly placed a spotlight on these practices, and left some marketers wondering "where to from here?" In the fields of measurement and targeting, we certainly believe that now is the time to take stock of your existing strategies and look to future-proof as much as possible.

IS THERE ANY UPSIDE?

Although so widely used, Cookies have never provided a perfect solution for marketers. For a start, Cookies identify browsers, not people - so most Cookie-based measurement and targeting solutions are therefore inherently flawed. Also, more and more digital media has migrated into closed environments such as Connected TV and apps, where Cookie data is of limited to no use. Cookies can also certainly go stale as people delete them or they expire. Many marketers have questioned the value of Cookie/anonymised user data beyond 7 days, where user intent becomes more questionable, and the price of inventory available to reach these users becomes more expensive.

As detailed below, many Cookie-based technologies have provided updates and workarounds in order to keep things on track, and we anticipate that new privacy-compliant targeting and measurement systems will continue to be developed and nullify most of the impact of a Cookieless world. In fact, Cookies were never intended to be used to the extent in which they currently are, so the development of more robust and privacy-compliant technologies can only be a good thing for the industry.

We also anticipate that these changes will encourage marketers to revisit how they plan and measure their activity - now is the time to get creative and we are excited to work through these challenges with our clients.

WHAT SHOULD I DO FIRST?

Now is the time to take stock of your current digital ecosystem. Look at which channels, partners and platforms are utilising Cookie-based data, and how the setup is configured. If third-party Cookies or IDFA technologies are involved, drill into how the activity is performing across different browsers, whether through the lens of audience pools, conversion tracking or any other KPI important to your business.

As the leader of the pack in terms of privacy updates, Safari will likely give you the clearest picture of what the future may look like - so pay particular attention to how your activity and audiences are behaving in this browser.

When considering your audience targeting strategy, look at how user data is being gathered and ensure it is compliant with the latest privacy practices here and abroad. Where third party data partners are in play, ask them how they will continue to gather audience information as Cookies continue to be rolled back.

Understand the short term impacts and fixes that need to be put in place (refer to the Analytics and Martech questions below), while also thinking about how to challenge what has been done in the past. Are your digital measurement models future-proof? Do they tell the whole story and show the full value of your marketing efforts? What targeting methods are in play in your advertising? Now is the time to test new approaches - insightful, audience-led targeting does not rely solely on Cookies, or any one approach.

WILL I STILL BE ABLE TO RETARGET PROSPECTS AND CUSTOMERS?

Right now, we don't know exactly what the future holds for retargeting technologies. It's safe to say that if your brand is one that users "opt-in" to by providing their email address or other identifier, then there should be no major impact to how you engage with these users. Identified, opted-in prospects will give you the broadest opportunity to reach your desired audience across a wide range of media.

However for many industries this would be of cold comfort. If your retargeting strategy relies primarily on anonymous (usually Cookie-based) information, e.g. URL visitors, then there's a very strong chance that some changes are required. Start with the Cookie audit mentioned above, then identify those audience strategies that have declined in line with Safari updates and seek out potential replacements. Ahead of 2022, the time is now to test, learn and build for the future.

WHAT ARE GOOGLE DOING?

Given Google's position within the overall ecosystem of digital advertising it seems likely that the extended timeline is to give themselves the best chance of working through the privacy wars while satisfying their enormous global community of advertisers. Already Google have released some details of potential technologies to replace Cookie functionality (likely API-based) and enable advertising functions such as retargeting, so expect more details on this to come to light over the course of the next 18 months.

Keep across the latest developments in Google's audience targeting capabilities - it is likely that they will continue to enable advertisers to deploy first-party solutions to enable retargeting across Search and Display. With Google's vast reserves of logged in behavioural data available, we don't anticipate any major impact to their proprietary audience segments such as In-Market and Affinity Segments.

WILL I STILL BE ABLE TO USE 1ST PARTY DATA TO IMPROVE MY DIGITAL ACTIVITY?

Absolutely. Now is the time to not only ensure your first party data practices are privacy compliant, but to build a data framework that is robust and future proofed. More than ever it is important to ensure your brand is the owner of your first party data, rather than relying on ad platforms. If you have a DMP or CDP in place, then you should be consulting with them on how to create persistent identities that outlive Cookies. Check how these can be deployed across key advertising channels and partners to ensure compatibility and minimise reliance on media tags and Cookies.

Consider how you can offer more value to prospective customers in order to gain a unique identifier (such as an email address) to increase your known audience pool, as anonymous retargeting is set to become more challenging. Working with your partners and publishers, look at how to best utilise their data for more robust targeting methods.

WHAT ABOUT THIRD PARTY DATA?

Beyond the information that you may have agreed to share with third parties from your own website, there are many third party data providers that provide access to data collected elsewhere. These segments are often built based on behavioural data collected from various web destinations that may indicate that an anonymous browser may fall into a desired audience, e.g. a prospective car buyer. If this data has been collected by Cookies or IDFA, then the validity of this data may now be lessened.

Other providers build segments based on data they access through partnerships - one such data provider accesses the shopping habits present in the data of one of the country's largest supermarket loyalty programs, thereby providing valuable insights to FMCG brands that would struggle to build a 1-to-1 data connection with the end consumer themselves.

These segments are usually sold on a CPM, applied to programmatic buying and often washed against a brand's own database in order to gain further segmentation, for example between prospective and repeat customers.

If third party data is part of your marketing ecosystem, have conversations with your providers about how the data is gathered - if based on anonymous third party Cookies, then it is likely that these segments will become less useful. Some data providers would not rely on third party Cookies at all. A rigorous test, learn and measure approach is ultimately the best way to ensure you are getting the most from your data partners.

DOES IT AFFECT FACEBOOK MARKETING?

The Facebook pixel that is used for website tracking within the Facebook ecosystem is currently viewed by browsers as 1st-party, due to updates made on Facebook's end - so there are no urgent actions for advertisers using the pixel. This enables Facebook to continue to track website activity and use that information within Facebook to either include that user in a category or directly as part of retargeting - largely within their closed, authenticated ecosystem.

This samesite attribute within the Cookie is essentially a workaround for now, so again it is worth reviewing how best to pass your data back to Facebook in a way that minimises risk of Cookie loss, as we anticipate further updates over the coming 18-24 months.
Pressure on Facebook data accuracy may also come from user privacy settings. Facebook currently allows users to opt-out of being tracked on websites (enabling retargeting and profiling), however this option is not as visible as similar settings on Apple devices and therefore has a lower adoption rate.

DOES IT AFFECT WEBSITE ANALYTICS (SUCH AS GOOGLE ANALYTICS)?

Analytics platforms generally set a first party Cookie by default. So in terms of third party Cookie deletion, we don't anticipate any major issues.

However, from a Safari perspective, where first-party Cookies have been restricted to a 24 hour expiry, there's likely already an impact on how performance is being attributed within that browser. For example, you may see a decline in return users, and a higher attribution rate toward true "last touch" channels in Safari, e.g. Brand Search and Direct, as the Cookie window has been gradually decreasing in Safari. The following section on Marketing Platforms addresses how to check and potentially fix this issue.

Understanding the nuances of your Safari traffic will help determine a future-proof measurement approach. Again we see opportunities for marketers to question the status quo and improve their digital program, as these browser and tech privacy updates may further highlight flaws with reporting and measurement models such as Last Click analytics.

At Atomic 212° we have developed agile media measurement models that do not rely on Cookie-based attribution, in order to quantify the true impact of all media channels.

IF I AM CHOOSING OR USING AN INTEGRATED MARTECH PLATFORM SUCH AS GOOGLE, ADOBE OR SALESFORCE, DOES THIS IMPACT ME?

Generally speaking, web analytics platforms tend to use 1st party Cookies by default. Each martech stack will have tech that uses 1st or 3rd party Cookies so you will need to evaluate each product individually. In consultation with each provider, try to get an understanding of how the products are implemented - where there are first or third party Cookies in use, see if there are alternative implementation methods to factor in both Safari ITP first party expiry and third party Cookie blocking.

The major providers have provided implementation options for their first party Cookies to minimise the impact of Safari's ITP 2.2 last year, usually setting something called a CNAME record within your website's Domain Name Settings (DNS).

CNAME records essentially allow a provider such as Adobe or Google Analytics to appear and function as if they were native to your website/domain. Both the Google and Adobe Marketing clouds advocate for the use of CNAME records to future proof their stacks against ITP and other Cookie-focussed privacy updates.

If you are currently using an Analytics, DMP, or Personalisation platform - it's essential to find out if your implementation has been updated to account for these changes.

FINAL THOUGHTS

There's never been a more exciting and challenging time to work with digital media and analytics. The advances being made, be it in the way browsers handle Cookies, or how brands adapting their data practices to ensure they are privacy-compliant, are in the best interest of consumers and the industry at large.

Ensuring your business and people are actively engaging with, not running from, these challenges will not only safeguard your marketing program but also open up new opportunities and approaches to marketing and measurement.

The changes discussed in this paper are largely technological, but are indicative of the beginning of an exciting new chapter in the marketing playbook. We think we'll all come out of this as better marketers.

ATOMIC 212°

ATOMIC 212° SYDNEY
9/23 Hickson Road
Sydney, NSW, 2000

ATOMIC 212° MELBOURNE
31 Ross Street
South Melbourne, VIC, 3205

ATOMIC 212° DARWIN
19 Smith Street Mall
Darwin, NT, 0800

W. www.atomic212.com.au
E. reception@atomic212.com.au
P. 02 9247 8388