BIZCOMMUNITY

Marketing in a world without third-party cookies

By Colleen Rose

23 Feb 2021

The move away from third-party cookies is gathering momentum as tech companies respond to growing consumer and regulatory concerns around personal data. Apple already ended support for third-party cookies in Safari in 2018, and Google plans to do so in its Chrome browser within the next two years. This represents a tipping point, since the two browsers have an 80% share of the market.

Image supplied

A recent class action lawsuit in the Netherlands also highlighted the risks that businesses face with Oracle and Salesforce being sued by Dutch citizens who claim their personal data was used without their consent.

While welcomed by privacy advocates, the looming demise of the third-party cookie has caused some anxiety among publishers and advertisers. For the last twenty years, third-party cookies have been a foundational part of digital advertising, allowing user behaviour to be tracked across websites, and turned into preference information which is used for targeted advertising. But what does it mean in real terms? To come to grips with the implications, it is important to first analyse what is actually changing. We are not, as it is sometimes framed, moving to a ‘cookieless world’.

First-party versus third party-cookies

The reality is that the browsers will only disallow third-party cookies - those that are set by domains other than the one the user is currently visiting. These cookies are used for purposes like ad retargeting, programmatic ad buying, cross-site tracking, sharing of data between third parties, social share buttons, customer service pop-ups and measuring cross channel campaign performance.

First-party cookies - those set by or on behalf of the website that the user is visiting - will still be allowed. Websites use these cookies to enable a convenient and seamless user experience – for example, to keep you logged in to websites and applications, track which products you have added to shopping carts, and store your website settings such as the language you selected and the values you entered in forms.
Independent Advertising Board (IAB) senior vice-president Jordan Mitchell says: “Without third-party cookies, we are only left with per-domain identifiers using first-party cookies, and it becomes impossible for third parties to set or recognise any form of shared or universal ID across domains - for any purpose.”

There are dissenting views but the impact on cross domain tracking will be significant and will require publishers to come up with creative solutions. Certainly, consent management will become increasingly important and close management of this will be key to a future response.

The impact for publishers, demand side platforms and consumers

The move away from third-party cookies affects a wide range of stakeholders in the digital ecosystem. For publishers, the concern is a potential loss of revenues. Many have already seen significant drops in programmatic ad revenue because of Safari’s anti-tracking updates and fear there is more to come when Google stops third-party cookies on its browser.

There will certainly be a significant impact in programmatic, though the exact consequences are still hard to envision. Recent studies show that when advertising is made less relevant by removing cookies, funding for publishers falls by 52% on average. This means they are less willing or able to share free content and could ultimately mean that there is less high-quality content available outside of paywalls.

Demand side platforms (DSPs) and other platforms that rely on third-party cookie syncs to identify individuals across sites will also be deeply affected. We will see a return to the time before cookie-based, behavioural data-powered advertising when marketers depended on personally identifiable information (PII) or much more explicit consent from users to extend their reach and consumer knowledge.

For consumers, less intrusive advertising, and tighter control over the use of user data by third parties might sound like a net positive. However, the move away from third-party cookies could increase the market power of already formidable companies like Facebook, Amazon and Google. They have amassed huge amounts of personal data in their walled gardens and will use this control of user preferences and user behaviours to further dominate the market.

How businesses are responding

Industry responses to the threat of cookieless marketing can be grouped into six broad categories:

1. **Rearchitect the business 1 model of the internet**

   The idea here is that consumers should own and be in control of the use of their identity and any related data. There would be an identifier that is encrypted so that it cannot be reverse engineered to identify the person. How this would play out in practice is not well defined, but it could mean that targeting decisions and ad-serving would happen on a consumer’s device. Brands and publishers would then have to offer auditable assurances that third-party vendors cannot track consumers without their explicit consent. An example of this is the IAB’s Project REARC.

2. **Privacy sandbox**

Google is proposing a secure environment for personalisation that protects user privacy. The user data shared with websites and advertisers would be minimised by anonymously aggregating user information and keeping Personally Identifiable Information (PII) on the user's device only. Google will do the conversion measurement (determining whether someone who saw an ad went on to take a desired action).

3. **Fingerprinting**

   Developers have found ways to use tiny bits of information that vary between users - such as which device they have or what fonts they have installed - to generate a unique identifier which can be used to match a user across websites. Unlike cookies, users cannot clear their fingerprint and therefore cannot control how their information is collected. Privacy regulations such as GDPR require informed consent by consumers. Since no such consent is obtained by fingerprinting companies there are sure to be moves to restrict fingerprinting.

4. **Grouping in an anonymous way**

   Users are added to a group (a cluster or a flock) that allows advertisers to target them without knowing who they specifically are. A group of different nodes - such as browsers or smartphones - could build machine learning models and upload parameters to a master model without sharing user level data. Each browser captures data on users' behaviour: websites they visit, the content of those websites and their actions.

   That data is used to build a model with parameters shared with a master model on a trusted server. In this way, each browser can be put into a cluster based on its user's browsing behaviour. This type of grouping is also known as federated learning and it means that browser manufacturers would become more significant players in the adtech ecosystem. This is more good news for Google but will be an interesting test of ambition for Apple and Microsoft.

5. **Contextual targeting**

   This refers to an ability to target users based on what they are doing on a website rather than on who they are. There have been some attempts to develop "programmatic" type of auction engines that allow publishers to sell the fact that a consumer is on their site looking at a product right now. The browser watches what users do and stores the data locally, but neither the advertiser nor the publisher learns much about them.

   A German publisher, for example, has developed a system that sends a signal to advertisers to invite them to bid to display an advert when a user visits a page. Instead of targeting a certain type of customer, advertisers will target customers reading a certain type of article or watching a video in a particular genre or topic.

6. ID resolution

This uses ID matching as a way of connecting various sources of consumer data to create a single profile. A consumer's ID across various systems (Facebook, Twitter, CRM, LinkedIn etc.) is linked to a common code. This would allow advertisers to target users based on their own first-party data or to partner with publishers in a regulation compliant way to extend their access to data. Businesses will need improved identity management to scale audiences in a post cookie world. Brands will need to update their tech stacks and strategic data partnerships to build and feature their own independent PII-based identity solutions.

To sum up, the future of marketing could be one of three scenarios:

- Consumers are fully anonymous – relying wholly on a few dominant players who control the whole user data market. The IAB says Google's move to block third party cookies means the "default future state of digital media will be 100% anonymous, non-addressable to third-party vendors that support advertising funded media and services today."
- Consumers are fully known – relying on the collection and use of first party known data.

- The way of interacting with consumers depends on the results of massive upheaval in the business model where data is owned by individuals.

What should we be thinking about?

As brands and advertisers, we can prepare for the future in a few ways:

- **Gathering first-party data**: Advertisers will need to collect more pseudo-anonymous and personal data. They will face a choice of getting more data partners or relying on market research, paying a premium and wasting a lot of impressions. It seems inevitable that larger publishers and walled gardens with large data sets will be the big winners. Brands should think about incentives they can offer to entice users and customers to share their data.

- **Manage consent**: To sustain their revenue streams and control their own destiny, publishers are looking at strategies to develop and activate their own audiences. Brands will have to look at how they make use of data sets that they have in their control to offer targeted content or advertising to their users, remembering that provable consent will be required.

- **Think about the value exchange** – How can brands make it attractive to users to share their information? What do they get in return for their consent? How do we attach a value to first party data to ensure that the cost of acquiring it does not outweigh the benefits of having it.

- **Be known as a brand that is responsible with data**. This will mean that consumers would be more willing to share data with you in whatever future scenario marketing finds itself in.

ABOUT THE AUTHOR

Colleen Rose, Consulting Director at Acceleration, a Wunderman Thompson company