Deloitte.

How the cookie crumbled: Marketing in a cookie-less world

1. What's happening? A summary

In January 2020, Google announced its plans '*to phase out support for third-party cookies in Chrome… within two years*'. In two years' time, all major browsers (Google Chrome, Firefox, Safari) will have blocked the use of third-party cookies. This may alter the landscape for digital advertising which currently relies extensively on third-party cookie data for personalisation. Businesses need to prepare and adapt to changes in personalisation solutions. However there is no need to panic.

- Personalisation will still be possible with other currently available solutions (such as first-party data, location and time-based messaging, and contextual targeting) across all the main digital channels (display, video, social, search).
- Audience data will be available as first-party (advertiser-owned) and second-party (tech or publisher-owned) cookie data, and will likely be supplemented by clean, fully GDPR-compliant, and transparent non-cookie-based third-party data.
- Investment in audience data technologies (such as DMPs and CDPs) will not be wasted, as there will still be multiple sources of audience data (even if first-party) that benefit from consolidation.
- Advertisers are expected to benefit from greater customer confidence over time in consuming online content and purchasing online safely.

So, do not worry. In our view, this decision is best for customers and brands. Here we outline our key thoughts on the topic.

2. Cookies: Key concepts

What are cookies?

Cookies are small pieces of code that are placed in your browser when you visit a website. They usually contain at least two pieces of information – a site name and unique user ID – but they may also capture other details such as website configuration (e.g. language preferences), login details, or products added to a basket.

What are first- and third-party cookies?

First-party cookies are cookies that are owned, stored and dropped by the website domain that the user visits. These cookies are used by the website owner to collect analytical data, remember preferences and provide personalised experiences. First-party cookies will not be blocked or phased out by Google.

Third-party cookies are created and stored by organisations other than the one that the user is visiting. These cookies are dropped by the website you visit but are not necessarily stored or owned by the website or its parent company. They are used for cross-site ad tracking, wider audience profiling and targeting, and wider personalisation in advertising (especially when prospecting for new users). Third-party cookies will be blocked or phased out by Google on its Chrome browser from 2020 to 2022, and have already been blocked by default within other browsers such as Safari and Firefox.

How are cookies used?

Cookies are used to collect user data, which can be on both an aggregate and anonymised level, such as clicks on page, pages viewed, engagement elements, and also on a PII (personal identifiable information) level, such as device IDs, names, addresses, passwords and credit card numbers.

All types of cookies are intended to provide a targeted and/or personalised experience to anyone using the internet, or to gather user behaviour for aggregated insights into user behaviour. These are applied to various decision-making processes, including those around user experience and even product design.

First-party cookies are used to understand the behaviour of visitors to a business website, remember their preferences and personalise the overall user experience with the brand.

First-party cookies can also be used to remember for example the contents of your basket on a website, the articles you last read or the progress of a video you are watching. This data can be utilised for personalisation of the website content and also for targeted messaging through paid advertising.

First-party data, collected by first-party cookies, can be shared with or sold to other organisations as third-party data.

Organisations can benefit from aggregated data collected by third-party cookies whenever their first-party data is non-applicable or insufficient. For example, a telecom brand may be interested in targeting individuals moving to a new home, but not be able to collect relevant user data using their first-party cookies, so that behaviours cannot be tracked from their own website. In such circumstances purchasing third-party data may be very useful for prospecting new users within a target audience.

However, not all third-party audience data is generated by third-party cookies. Organisations may gather granular user data using first-party cookies within their websites (e.g. through a detailed personality and behavioural questionnaire, or tracked consumption of news articles in different subjects), then aggregate the data within audiences and offer it for sale to marketers for targeting and personalisation.

In addition, content publishing organisations can make their owned data (collected through their first-party cookies) available directly to marketers that purchase advertising space on their website. This is second-party data from the perspective of the marketers.

What are the benefits of cookies?

Both first- and third-party cookies enable a person's experience on the internet to be personalised with interesting and engaging content. Cookies ensure that when you revisit a website, you don't have to alter the language settings, your basket is still there, and any preferences you have shown are still in place. They also allow businesses to target users through paid advertising channels with products and messages that are particularly relevant to their individual interests.

Third-party cookies are also used by businesses to build an in-depth understanding of consumers and to target them better with advertising, as well as understanding the performance in general of their advertising activities.

3. Third-party cookie data: What are the pros and cons?

Pros

Third-party cookies allow ads to be 'hyper-targeted' or personalised for individuals even when they have not yet engaged with the advertiser, providing a more engaging and relevant user experience across the internet, and encouraging discovery of targeted products or services. Data technology companies aggregate user data through third-party cookies, and these are widely available at market rates.

Cons

Data privacy is an issue. Users have no visibility about which companies are processing their data, beyond those that own the websites they visit. The GDPR includes cookie consent mechanisms, but once users have consented, they have little or no visibility about which organisations are directly collecting their data. From a user perspective, this can lead to hyper-targeted and persistent messages by unknown – and sometimes perhaps disreputable – organisations, which can be seen as invasive rather than helpful and interesting.

4. What will happen now? The main implications from the change

For consumers

The ban on third-party cookies will give consumers more control over the data they share with companies online. Consumers will be better able to manage and understand which companies capture their behavioural data, since they must give explicit consent for it to be collected: this should avoid cases of 'hidden' data collection. The downside is that personalisation of a web experience (outside a specific brand's owned website) could become less common, with more irrelevant or 'boring' ads being shown. However consumers who have visited the website of a specific brand are still likely to be targeted with personalised messaging from that brand (or other brands owned by its parenting company).

For internet users in general

The universal block on third-party cookies will lead to greater rigour in data privacy for all internet usage. Other browsers including Firefox, Internet Explorer and Safari have already announced or implemented a ban on third-party cookies.. This will give internet users much greater clarity, confidence and assurance when using the internet, especially about who they are giving their data to and what those companies are doing with it.

For advertisers

As an immediate effect after the implementation of the ban, most third-party audiences (those whose data is collected via third-party cookies) will diminish in size due to cookie expiry, until they are no longer sufficiently scalable for most media buying activities. This means that advertisers will need to develop new strategies for prospecting and rely more heavily on other tactics. Advertising data processing and selling organisations will need to develop new ways to collect and aggregate audience data that do not require third-party cookies.

For publishers

Large digital publishers typically generate a large proportion of their revenue by partnering with third-party data providers who collect data via their pages. With the third-party cookie ban, this will no longer be possible, possibly resulting in a large loss of revenue for digital publishers in the short term and requiring them to develop new strategies for revenue generation from the large audience data they produce.

For demand side platforms (DSPs) and ad tech providers in general

Many DSP vendors will need to revise their strategy for the marketability of their products, which typically emphasise the availability or differentiated use of third-party data for targeting, in response to the threat from media giants such as Google and Facebook, which offer their first-party audiences free-of-charge for targeting within their media buying platforms.

The appeal of DSPs should not be diminished drastically. Most of them enable granular targeting and campaign management through other parameters (e.g. site whitelists, content categories, keywords, location, time-of-day and day-of-week, device and browser, and first-party audiences), as well as the vast access to inventory through partnering ad exchanges for display and video advertising.

Other ad tech or ad buying solution providers, such as social platforms, will need to adapt their standard tactics on collecting user data on advertisers' websites for performance tracking and targeting. Until now these have been implemented through the insertion of cookies on websites. It is unclear at this point what will be the implication of the third-party cookie bans for 'cookie piggybacking' or other indirect ways of appropriating or transferring first-party cookie data usually practised for ad serving.

Short-term implications

In the short-term there will be minimal impact on digital marketing, as Google has set a two-year timeline for phasing out the use of third-party cookies on the Chrome browser. Targeting and personalisation through third-party data on both owned media (on-website) and paid media (advertising on other websites and channels) may continue for the time being. However data privacy and transparency have been brought into focus, and there will be more visibility for consumers about who collects their data and how it is used. There is a need for the entire digital community at all levels to find solutions that allow the same (or similar) levels of personalisation and targeting that third-party cookies have been providing, whilst also addressing concerns and the new mandatory practices around privacy, transparency and data ethics.

"The downside is that personalisation of a web experience (outside a specific brand's owned website) could become less common, with more irrelevant or 'boring' ads being shown."

5. How to manage the change? Our recommendations.

There is no need to panic. The changes are not due to be implemented until 2022, and Google has yet to provide details about what will change. There are other examples of technologies that were discontinued with little to no impact on advertising performance, such as Flash, and the market evolved and adapted adequately to avoid disruption. In the meantime, there are a number of practical things you can do:

01 **First and foremost, amplify your owned data: improve first-party data collection.** A precise, careful and thorough implementation of data capturing mechanisms will ensure robust data is available as granular input for targeting and personalisation of users who have already engaged with your brand. But bear in mind that starting early is key, as you may need time for data to build up sufficient data volumes.

02 **Implement best-in-class cookie consent management solutions,** if you haven't already done so, to ensure that your first-party data is fully compliant with regulations and future-proof. Also, clearly communicate to your customers how you process and protect their data, to increase trust.

03 **Explore second-party data from tech leaders.** Google and Facebook, for example, offer aggregated but granular audience data collected across their respective platforms (including Google Search, YouTube and all websites within the Google Display Network, and Facebook and Instagram) through their respective media buying platforms (Google Ads and Display & Video 360, and Facebook Ads Manager), completely free of additional charge (unlike third-party data).

04 **Explore second-party data from publishers.** The main publishers typically offer display, video and native buys overlaying their owned data, when contracting directly or through programmatic private auctions.

05 **Apply 'unusual' personalisation tactics.** Campaigns applying deep personalisation through clever geo-targeting and time-parting (often called 'moment marketing') typically generate high engagement and even lead to advertising awards, but are still not widely used in the industry!

06 **Stay tuned for clean third-party audiences.** Not all third-party audiences rely on cookie data. Some of them are already available for targeting, such as VisualDNA, which aggregates its audiences in a transparent manner based on direct personality quizzes. More of these non-cookie-based third-party audiences should emerge within the next two years after the third-party cookie ban.

07 **Use the opportunity to rethink your marketing tech ecosystem.** Take the chance to re-strategise your data and tech ownership, so you can obtain the most control, visibility and usability of your own data. First-party data is now more important than ever, and owning all your data will act as a safeguard in the event that you need to change agencies or tools, which could otherwise result in loss of data.

08 **Enjoy higher expected returns from the elevated customer experience,** based on greater customer trust, coupled with cleverly personalised messages to reach them when they are most likely to do business with you!

So times are changing, but one person's problem is another's opportunity. There is time to adjust to the changes and the benefits from the increase in consumer trust they will generate. With our deep understanding of consumers and the data, technology and vendor landscape, Deloitte Digital will be leading clients through this transition, helping to optimise current activity, introduce new systems and processes and elevate the customer experience.