Regulatory Scrutiny of Cookie-less Adtech Continues to be one of Google's Topics

Emily Morgan
Solicitor, Wedlake Bell LLP

Alexander Dittel
Partner in Technology, Wedlake Bell LLP

Advertisement control; Competition law; Cookies; Online intermediaries; Online services; Privacy

After over 20 years of ever-more-targeted online advertising, the dawn of "privacy-first advertising" is almost palpable. What was started by legal events such as the introduction of the EU's General Data Protection Regulation (GDPR)[1] and California's CCPA in 2018, the Planet49 case against pre-ticked consent boxes,[2] the many redrafts of the EU's proposed ePrivacy Regulation, and regulatory pressure including the Information Commissioner's Office's 2019 report into real-time bidding,[3] ultimately translated into real-world actions by the industry itself.

Apple's attack on third-party cookies, the rise in privacy-enhancing browser features, and Google's announcement of the "death of third-party cookies" in early 2021, has kept marketing teams on their toes for the last two years. Privacy advocates and regulators have been gradually increasing the heat. With the recent Belgian enforcement action regarding IAB Europe's Transparency and Consent Framework relied on by so many for their "compliant" cookie consent solution, it seems that the path of change has moved beyond the point of no return.

Third-party cookies and beyond

Cookies are small text files of data (which might include personal or non-personal data) that are used by a website or app to store information. Whilst first-party cookies generally serve less invasive purposes such as remembering language preferences and items in online baskets, the use of third-party cookies by marketers has been criticised for allowing advertisers to harvest vast amounts of information about the individual's web behaviour for economic gain. The shady surveillance-for-hire industry is said to rely on the same tools for unlawful tracking of individuals on the instruction of well-paying customers regardless of motive.

However, for digital marketing professionals and businesses generally, third-party cookies are a long-established fundamental asset for creating data-driven value. By collecting and sharing web behaviour data among multiple organisations, knowledge of individual's preferences and interests can be used to customise advertising to improve the relevance of ads and improve user experience.

This has created an ecosystem where advertisers, on the one hand, get to reach their near-ideal audiences, and publishers, on the other hand, get rewarded for offering up their properties to host ads consumed by their users. Most notably, the free press relies significantly on its advertising revenues which help fund journalism.

However, with a recent increased drive against "dark patterns" designed to encourage user consent to, arguably, circumvent existing rules, the consent mechanism had to become clearer and offer an easy way to "reject all". Increasingly more consumers are actively choosing to disable third-party cookies, thanks to the transparency rules reinforced by data protection authorities in Europe.

Privacy advocates and a recent spike in claims for compensation have played an essential role in calling out breaches of the rules and investigating complaints, despite the arguably limited harm to individuals. In response, we see more paywalls and mandatory user registrations to access content which was once one click away. The trade-off between privacy and free content is real.

So, what is next for digital advertising?

Is profiling the main issue?

Recently, other types of tracking have proliferated to compensate for the upcoming end to third-party cookies such as fingerprinting, i.e. pulling together mostly device data which makes up an individual's unique "digital fingerprint" and combining this with other personal data to recognise, track, and profile individuals. However, this type of activity is still subject to the Privacy and Electronic Communications Regulations (PECR)[4] and the GDPR, meaning that companies cannot avoid compliance although tracking is less visible to individuals.

However, the complexities of adtech are not easily explained to consumers. In its opinion late last year, the ICO reiterates that neither the legitimate interest balancing test nor a compatibility assessment would enable such processing to be fair and lawful without consent, because of the nature, scope, context and purposes of these processing activities including

[1] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 [2016] OJ L119/1.
[2] *Bundesverband der Verbraucherzentralen und Verbbraucherverbande v Planet49* (C-673/17) EU:E:2019:801; [2020] 1 W.L.R. 2248.
[3] "ICO Update report into adtech and real time bidding" 20 June 2019 at *https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf* [accessed 19 April 2022].
[4] Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

predicting actions and informing decisions, and the risks they pose to rights and freedoms. The Belgian fine of IAB Europe suggests that even consent is insufficient given the inherent lack of transparency.

It seems that some processing will simply be irreconcilable with data protection. According to the ICO, even if data is collected passively, or where the processing involves observed, derived, or inferred personal data, this is still processing of personal data which can, in some circumstances, raise more significant risks of harm where individuals are entirely unaware that it takes place. This includes processing of device information and data matching, combination, and enrichment within the extensive data supply chain.

The ICO's bar is clear, with a focus on prevention of harm. It is recognised that extensive profiling for advertising could give rise to lack of autonomy, loss of control, information asymmetry, manipulation and influence, misuse, lack of confidentiality, chilling effects, reduction in trust and confidence, or impeded exercise of rights. Somewhat late to the table, in March 2022, the UK Government launched its "Online Advertising Programme consultation" which will attempt to clarify the level of harm to consumers from online advertising. If the UK pursues the harm-based approach to enforcement and regulation, this may set us apart from Europe which seems to focus on technical breach of the law.

Google's Topics

Google's Privacy Sandbox initiative attempts to offer a solution for the cookie-less future. The initial "Federated Learning of Cohorts" or FLoC offering was discontinued over privacy concerns. FLoC would put people in interest cohorts, based on their browsing history. The solution relied on machine learning which would run on the user's device to categorise each user. However, it transpired that FLoC data could be combined with personally identifiable information and allow third parties to discriminate against particular groups of people.

Building on the privacy-enhancing use of machine learning and on-device only processing, Topics will assign five topics such as gardening or cooking to an individual each week, based on the websites visited. A sixth wildcard topic is assigned to dilute the possibility of identification. Websites will be able to declare their topics from a list of 350+ topics failing which, it will be determined by the Topics algorithm. Topics will remain assigned for three weeks.

When an individual visits a publisher site, advertisers will only see three topics per individual in respect of the individual's last three weeks of browsing. This includes one topic randomly selected from the five for each week. Different sites will see different topics, and only one new topic can be learned per week. This will allow advertisers to personalise advertising based on the topics. However, they will not see any topics which do not match their audience criteria.

Google's Topics almost reaches into that space between targeted and contextual advertising, where the content viewed rather than the user profile is important. According to the ICO, as a general rule, contextual-based advertising allows most readily for compliance with the data protection principles. Whilst Google Topics will still attach topics to specific individuals, it removes the complex and intrusive profiling based on inferred data which is currently subject to much criticism. Topics will likely result in less targeting, given the lack of granular profiling.

Possible issues

There is a risk that ads may not be relevant by the time they are presented, because by week 3 the user may no longer be interested in his or her week 1 topic. This could cause a data accuracy issue.

To enhance tracking-prevention, a "week" will begin at different times for different sites and so will allocated topics. This is a data minimisation measure by making it difficult for advertisers to cross-correlate the same individual and build a profile.

Topics will be deleted after three weeks. However, there is a risk that such publishers may share data to build larger profiles, which may lead to intrusive profiling.

As a form of web-behaviour tracking which could be considered invasive, Google Topics will have to offer a high degree of transparency about how the tracking works and how it can be controlled, or face the risk of penalties. For example, one of the shortcomings identified by the Belgian authority in its fine against IAB Europe was that its Transparency and Consent Framework allegedly does not offer sufficient transparency about the complex data processing in the advertising ecosystem.

Google has confirmed that no topics will be presented to advertisers if a user opts out, clears their browser history, or if they are using Chrome in incognito mode. However, this is still placing the ultimate responsibility to take action in the hands of the user, which cannot arguably be a "privacy-first" approach. In order to show compliance with the data protection by design and by default principle, as required by the GDPR art.25, default settings should be set to benefit and protect the users' interests rather than those of the service provider. Perhaps Google could address this by requiring not just advertisers but also users to opt-in. It appears that as Google Topics relies on the browsing history and writing and reading data on the device, it will likely trigger the consent requirement under ePrivacy rules.

Google plans to rely on an external party to set up a list of excluded topics which cannot be presented to advertisers, thus further supporting the data minimisation aim and limiting the processing of special category data or data that individuals would consider private. However, it should be taken into account that some users may wish to see ads that are relevant to their sexual orientation or political views.

The competition concern

The Competition and Markets Authority (CMA) is concerned about the dominance of the likes of Google and Facebook in online advertising. As they hold massive amounts of data by aggregating information across their ecosystems of interconnected consumer services, they create significantly better-informed targeting and personalisation. This means they face little competition from smaller adtech players with less detailed profiling methods.

Currently, third-party cookies are relied on by most of the adtech industry. Due to its market share, Google has the power to significantly affect the industry's direction by stopping its own reliance on third-party cookies. Google's and Facebook's "walled gardens" comprising granular first-party data are well-poised to absorb the shock this will cause, something that cannot be said about many smaller adtech players. These parties will struggle to develop an alternative without knowing where the majority of the industry will end up. Google is in a unique position where it can set rules in Chrome, which is used by well over half of internet users. Google's Topics will not be just a new service by Google. It will dictate the future opportunities for the industry as a whole.

Unsurprisingly, the CMA and ICO demanded certain commitments from Google, in the hope of relinquishing some control and allowing the rest of the industry to have some influence in the new proposals. According to Google, the Privacy Sandbox will protect consumers and support a competitive ad-funded web, and not favour Google. The changes in Chrome will apply globally, Google's Topics will be developed with regulatory input and Google will not sunset third-party cookies without notifying the CMA and allowing time to address competition law concerns. Google will not be allowed to share personal data within its ecosystem where users have not consented to its collection for advertising purposes.

The CMA suggested that increased competition can be achieved by greater sharing of non-personal data between businesses and increased interoperability between services. This initiative is simultaneously being pursued by the EU, with the recently proposed draft Data Act. Google is also being scrutinised in the US, being faced with multiple competition lawsuits accusing the tech giant of preventing competitors from using advertising space.

What this means in practice?

It is hoped that the regulatory scrutiny will lead to more transparency about the proposals for a cookie-less future. Businesses may be able to plan better as a result.

The industry will inevitably be led by their initial solution offering, but this is not to say that rivals may emerge with better alternatives which provide increased autonomy and control within the advertising process.

Organisations should undertake an audit of their current use of third-party cookies in advertising and keep an open mind when planning for what comes next. The use of new technologies might trigger the requirement for a data protection impact assessment.

The ICO has made it clear that certain data protection standards must be followed in order to prevent overpowering individual rights and freedoms when monetising data. Preserving the intrusive profiling and status quo by new means will not cut it. While the ICO has not issued any penalty in the past, its position is sufficiently clear. The current adtech offering is intrusive, unfair and gives rise to numerous risks to the individual. Once new solutions are available allowing industries to move forward, there will be no excuse for continuing with outdated technology.