GCR Global Competition Review

Data & Antitrust Guide - First Edition

How the interplay between competition and privacy law is affecting online advertising

Data & Antitrust Guide - First Edition

In a world where data is 'the new oil', competition authorities are having to tackle fresh issues as data and antitrust converge. The first edition of the GCR *Data & Antitrust Guide* – edited by Miranda Cole and Lara White – offers a wide-ranging view of how key jurisdictions around the world are addressing new regulatory and enforcement questions and provides practical and timely guidance for those trying to navigate this fast-moving environment. The Guide draws on the wisdom and expertise of distinguished practitioners to deliver unparalleled proficiency in the field.

Generated: May 28, 2024

How the interplay between competition and privacy law is affecting online advertising

Miranda Cole, **Christoph Ritzer** and **Lara White**
Norton Rose Fulbright

Summary

INTRODUCTION

Online advertising today relies on the collection, matching and use (including sharing) of vast amounts of personal data. In some cases, this information is shared among a web of hundreds of advertising intermediaries of varying sizes. In others, the information collected remains primarily within the closed environment of a single entity (or group of entities).

The amount of personal data involved and the way it is collected, used and shared has attracted (and continues to attract) a lot of attention from privacy and competition regulators, the courts and, ultimately, consumers, including in relation to the interplay between privacy and competition laws – which are not always aligned.

In this chapter, we:

- provide a brief, high-level overview of how online advertising works;
- look at the privacy challenges relating to the online advertising ecosystem;
- look at the competition law challenges relating to online advertising; and
- explore the direct and indirect interplay between privacy and competition law in the context of online advertising.

OVERVIEW OF ONLINE ADVERTISING

The online advertising ecosystem is complex. At its core, it involves a transaction between advertisers wanting to present their advertising content to an online target audience (including users of websites, apps and social media) (the buy side) and publishers and digital platforms who have advertising space (or inventory) that they want to sell (the sell side).

At its simplest, online adverting can be split into two main channels: search advertising and display advertising.

SEARCH ADVERTISING

A search ad is displayed in search results following the use of a search engine (i.e., on the search engine results page (SERP)). Advertisers bid on keywords so that their advertisement appears when the search performed uses the keyword or term. In addition, information about the user (e.g., their location, search history and other information available to the search engine) will influence the search ads they are presented with, to ensure their relevance. These ads appear at the top of the SERP (although they are also intermingled in the search results in certain contexts, including those in respect of certain vertical searches), and are marked as 'Ad' or 'Sponsored', depending on the search engine, with information about why an advertisement is being made available to the user.[2]

DISPLAY ADVERTISING

Display ads are proactively displayed to users (i.e., visitors to a social media platform, website or app) because they fall into a category of individuals whom the advertiser wishes to target. They often take the form of banner ads, side bar ads or pop-up ads. This type of advertising is often referred to as 'outbound' or 'push' advertising because it is instigated, at least indirectly, by the advertiser, unlike search ads, which are an 'in-bound' or 'pull' form of advertising (where advertisements are displayed in response to user-initiated searches).

Display advertising falls into two broad categories:

- *Open display advertising*: Publishers sell their inventory to a wide range of advertisers through an auction process referred to as real-time bidding. This relies on a complex ad tech chain, including ad exchanges, ad servers, ad networks and data management platforms. These vendors match up the buy side and sell side and provide a range of different services, from helping publishers to generate the most revenue from their advertising space, to helping advertisers enrich the data they hold or to measure the success of campaigns.
- *The 'walled garden' model*: Large players – such as Facebook, Instagram and Google – sell their own inventory through their own ad tech stack, meaning that they own the relationships with both advertisers and the audience. They collect information about users while those users interact with their services and visit other online services or websites (using embedded tracking technology).

Display advertising relies on the collection and sharing of large amounts of data about users to try to ensure that the ads reach the most relevant audience and that individuals are presented with ads that are likely to be of most interest to them. Generally, this collection and sharing of information about a particular user occurs via third-party cookies[3] and other tracking technology[4] that is placed in a user's browser when they visit a website or app, or look at something on social media, stores information about their use of the internet (e.g., websites visited) and identifies visitors between different websites. This includes technology used by social media platforms to leverage a user's off-platform activity to advertise to them when they are on the social media platform.[5]

PRIVACY REGULATORY CHALLENGES

In many jurisdictions, the information collected via the tracking technology used in online advertising is personal data or personal information, even though a named individual cannot be identified from the relevant identifier alone. Accordingly, it must be handled in accordance with applicable privacy laws. Owing to the complexity of the online ad ecosystem, full compliance with these laws is often challenging.

Various jurisdictions have introduced rules specifically addressing the use of cookies and other tracking technologies. In Europe, for example, the ePrivacy Directive[6] (and the national laws implementing it into Member State law) requires organisations that store information on, or gain access to information from, a user's terminal equipment (which includes the use of cookies and other tracking technology referred to above) to provide users with information about the use of cookies and to collect opt-in consent from users in advance of setting them up on their browser. Providing true transparency about the use of this technology, and the collection of consent, by the large number of adtech vendors involved in the ecosystem (including about what is collected and shared and whose data is shared) has always been challenging. This was brought into sharper focus after the General Data Protection Regulation[7] (GDPR) came into effect because of its more prescriptive requirements around transparency and very specific requirements for the collection of valid consent. Most significantly, valid consent must be informed, granular and freely given and must name the party relying on it. In the context of a complex web of data sharing, this is very challenging.

This is not just a European issue. In the United States, for example, where there are many state privacy laws, the use of tracking technology (and user control of its use) is also starting to be regulated.

Leaving aside cookie-specific laws, general privacy laws also apply to the use of cookie data and other forms of personal data; for example, what logged-in users view when they access a social media platform.

Under the GDPR, any personal data collected in the context of online advertising must be processed (i.e., handled) on a valid lawful basis. Large organisations have sought to rely on lawful bases other than consent to justify the use of certain personal data for advertising purposes (e.g., that the processing for advertising purposes is necessary for the performance of the contract the user has entered into with the social media company); however, regulators and courts across Europe are tightening their view of when a lawful basis other than consent can be used for online advertising purposes. This came into focus in the Court of Justice of the European Union (CJEU) judgment in Case C-252/21 (***Meta Platforms and Others (General terms of use of a social network)***), involving Meta Platforms Ireland Limited, the operator of Facebook in the European Union (see further, below). Even consent is not without challenge, however, as questions as to whether consent has been freely given in the context of the use of large online platforms are frequently raised. The CJEU found that an alternative to consenting to the processing of data (other than not using the services) must be offered but accepted that this could be offered for an appropriate fee. Meta has since introduced a subscription option for an ad-free service for users in the European Union, European Economic Area (EEA) and Switzerland, which has already prompted calls for the European Data Protection Board to issue a binding opinion on the lawfulness of this model.

Attempts to deal with some of these privacy compliance challenges (such as the transparency and consent framework of IAB (Interactive Advertising Bureau) Europe[8] and Google's deprecation of third-party cookies) have faced criticism, and there have been calls for data protection authorities to investigate the compliance of the online advertising industry with privacy laws. Accordingly, we have seen investigations by data protection authorities, including the United Kingdom's Information Commissioner's Office (ICO), specifically focused on real-time bidding,[9] the French regulator (the National Commission for Information Technology and Liberty (CNIL)), which focused on valid cookie consent and issued some very high-profile adtech-related privacy fines,[10] and the Irish Data Protection Commission, which is responsible for regulating the EU activities of many of the world's largest technology companies.[11]

COMPETITION LAW CHALLENGES

In Europe, online advertising has been the subject of a number of investigations by competition regulators. These have addressed the accumulation of personal data for use in online advertising, and allegations of self-preferencing and other forms of exclusion.

In March 2019, the European Commission fined Google €1.49 billion for abusing its dominance in the online search advertising intermediation market. Through AdSense for Search, Google provided search ads to publishers. It had a market share above 70 per cent between 2006 and 2016 (the material time). The Commission found that the abusive conduct included exclusivity clauses (preventing competitors from placing search ads on publisher pages) and, from 2009, 'premium placement' clauses (i.e., reserving the most profitable

publisher inventory for Google) and clauses giving Google the right to approve how rival advertisements could be displayed.

In June 2021, the CNIL completed an investigation into Google's adtech business, concluding that Google abused a pan-European dominant position by favouring its proprietary display advertising intermediation services. It fined Google €220 million and made commitments by Google (to be implemented globally) mandatory.

The European Commission opened an investigation into whether Google violated EU competition law by favouring its own online display advertising technology services in the adtech supply chain in June 2021, specifically the effects of its Privacy Sandbox on third parties (see related details in the following section). The investigation is also considering whether Google's (1) publisher ad server, 'Double Click for Publishers', favoured Google's own ad exchange, AdX, in inventory auctions by informing AdX of bids in advance, and (2) advertisement buying tools placed bids mainly on AdX to make it the most attractive exchange. In June 2023, the Commission informed Google of its preliminary view that these two practices breach Article 102 of the Treaty on the Functioning of the European Union as abuses of a dominant position. In its June 2023 Statement of Objections, the Commission expressed the view that a behavioural remedy is likely to be ineffective in removing the risk that Google will continue this 'self-preferencing' conduct (or engages in new forms of according preference). The Commission describes Google's dominance on both publisher and advertiser sides, and also characterises this as an inherent conflict of interests that can only be solved by 'mandatory divestment by Google of part of its services'.[12] Recent updates suggest that the Commission is pursuing divestiture of both Double Click for Publishers and AdX. The US Department of Justice is also focusing on the break-up of Google's advertising business.

The United Kingdom's Competition and Markets Authority (CMA) is also conducting a similar investigation of Google's conduct in parts of its adtech stack. The investigation was launched in May 2022 and the information gathering and related analysis phase took place in 2024.

In December 2022, the European Commission issued a Statement of Objections alleging that Meta is abusing its dominant position and distorting competition in markets for online classified advertising by (1) tying its dominant social network (Facebook) to its online classified advertising services (Facebook Marketplace) and (2) unilaterally imposing unfair trading conditions on competing online classified advertising services on Facebook or Instagram. Meta responded in June 2023.

In the United Kingdom, the CMA launched a similar investigation in June 2021 regarding Facebook's use of data from digital advertising (and its single sign-on option, Facebook Login) to benefit Facebook Marketplace and Facebook Dating. In November 2023, the CMA accepted commitments from Meta: in essence, (1) to allow Facebook Marketplace competitors who are advertising on Meta's platforms to opt out of Meta being able to use certain advertising data to improve Marketplace; and (2) not to use advertising data to develop its own products (which compete with advertisers).

In March 2022, the European Commission opened proceedings into the 'Jedi Blue' agreement entered into by Google and Meta in September 2018. This agreement concerned header bidding services, specifically the participation of Meta's Audience Network in Google's Open Bidding programme. The Commission was concerned that the agreement enabled Google to exclude adtech services competing with its Open Bidding programme; however, the

Commission closed its investigation in December 2022 without taking action. The CMA also investigated the agreement under both Chapter I of the Competition Act 1998 (CA98) (restrictive agreements and practices) and Chapter II of the CA98 (abuse of dominance). It closed its Chapter I investigation in March 2023 and rolled the Chapter II investigation into the wider investigation of Google's conduct across parts of the adtech stack. The latter is discussed above.

Concerns about the potential anticompetitive effects of control over data enabling advertisers and publishers to assess the effectiveness of online advertising (i.e., the return on investment) were behind several provisions of the European Union's Digital Markets Act (DMA).[13] Paragraphs 9 and 10 of Article 5 of the DMA require designated gatekeepers (Google, Amazon and Meta, currently) to provide advertisers and publishers with free information (on a daily basis) concerning each advertisement placed regarding price and fees paid by advertisers, remuneration received by publishers and the metrics on which prices, fees and remuneration are calculated. Article 6(8) further requires those gatekeepers to provide advertisers and publishers (on request) with free access to the gatekeeper's performance measuring tools and the data necessary to carry out independent verification of advertising inventory.

These types of investigations are not confined to Europe (the European Commission and the CMA). For instance, in March 2021, the Competition Commission of India (CCI) opened an investigation into WhatsApp and Facebook, specifically WhatsApp's privacy policy terms (which permit data sharing with Facebook). In October 2022, India's Supreme Court held that the CCI's investigation could proceed, dismissing petitions from Meta.

INTERPLAY BETWEEN PRIVACY AND COMPETITION REGIMES

Some efforts to address the privacy challenges in the online advertising context have given rise to competition law challenges. In other instances, particularly in the context of the accumulation and use of personal data for use in online advertising, privacy and competition law have been more closely aligned.

PRIVACY – CHANGES DRIVING COMPETITION LAW CHALLENGES

Certain key players in the industry have responded to privacy regulation, and pressure from privacy activists and consumers, by changing their practices; however, as explained below, these developments help to demonstrate the difficult interplay between data protection and competition, particularly in relation to the accumulation of data and the effects of measures that reduce third-party access to consumer data. Two major developments have given rise to allegations that the companies have weaponised privacy for their own benefit.

APPLE'S APP TRANSPARENCY CHANGE

In 2021, Apple introduced app tracking transparency (ATT) and started requiring that users opt in to cross-app-tracking by app developers for advertising purposes. It did this by requiring app developers to present a pop-up to users when they download an app that prompts them either to 'allow tracking' or to 'ask app not to track'. Apple announced that it was introducing this change for privacy reasons and to give mobile users greater control over their data; however, the change mainly affects third parties and, in an age where mobile advertising accounts for a significant share of online advertising, this had a major effect on many app developers, ranging from very large players such as Facebook to very small advertisers, who relied on information collected elsewhere for their in-app advertising.

This triggered numerous complaints to competition authorities and, since introducing this change, Apple has faced investigations from competition authorities across Europe.[14] These authorities are concerned that, through ATT, Apple creates an unfair advantage for its own personalised ads, which are not subject to the same permission pop-ups.

GOOGLE'S DEPRECATION OF THIRD-PARTY COOKIES

Google first announced plans to follow Apple's lead[15] in deprecating third-party tracking cookies on 14 January 2020. Google deprecated third-party cookies in 1 per cent of Chrome browsers globally on 4 January 2024 and plans to deprecate 100 per cent of Chrome third-party cookies in Q3 2024. It describes this as 'improving people's privacy while giving businesses the tools they need to succeed online' and offers its own Google Privacy Sandbox as a privacy-preserving alternative to cross-site tracking. The Privacy Sandbox is a collection of application programming interfaces (APIs) designed to continue facilitating the presentation of 'relevant advertising' without cross-site tracking, which is facilitated by using third-party cookies. The main API from an advertising perspective is TOPICS, whereby the browser attaches a handful of recognisable, interest-based categories to a user based on its recent browsing history to enable relevant ads to be served. Unlike with third-party cookies, details of specific sites visited are not shared with the ad ecosystem. Rather, the interest group 'topics' allocated to the user are shared.

Google explained that it delayed deprecation of third-party cookies to allow more time for it to evaluate and test its Privacy Sandbox technologies, and to allow advertisers to adjust their advertising approach and test new targeted advertising technologies; however, they have also needed to address competition concerns raised by, among others, the CMA, which has scrutinised the design and impact of the Privacy Sandbox tools and, with the ICO, required Google to give certain commitments around the design and implementation of the Privacy Sandbox.[16] [17]

As noted above, in June 2021, the European Commission opened an investigation into how Google's Privacy Sandbox affects third parties – specifically whether Google violated EU competition law by favouring its own online display advertising technology services in the adtech supply chain.

The CMA also investigated Google's Privacy Sandbox (and continues to investigate other conduct in parts of Google's adtech stack). In February 2022, it accepted Google's commitments, which it continues to monitor. The commitments included an undertaking by Google not to remove third-party cookies until the CMA is satisfied that its competition concerns have been addressed. In January 2024, in its most recent quarterly update report on implementation of the commitments, the CMA set out its continuing competition concerns regarding the Privacy Sandbox, including: (1) Google may continue to benefit from user activity data while limiting competitors' access to the same data; (2) Google's ability to control the inclusion of ad tech rivals in the program could be advantageous to its own ad tech services; and (3) publishers and advertisers may be less able to effectively identify fraudulent activity. The CMA continues to work with Google to address its competition concerns and will deliver its next quarterly update at the end of July 2024.

Last, to address the CJEU's ruling that its targeted advertising could only be undertaken based on valid, freely given GDPR consent, Meta introduced a subscription-based option for an ad-free service in Switzerland and the EEA (which is commonly referred to as 'pay or okay'). This model is being scrutinised, with some data protection authorities asking the

European Data Protection Board for an opinion as to whether it is acceptable; however, as what constitutes a reasonable price by a company holding a dominant position is also a competition law issue (and a question relating to DMA compliance in the EEA), discussions about this model include data protection, competition and other authorities.

PRIVACY LAW INFRINGEMENT CAN CONSTITUTE A BREACH OF COMPETITION LAW

The above are examples of ostensible efforts by firms to address privacy concerns leading to competition law challenges. Alongside these, there have also been instances where alleged infringement of privacy laws has been the basis of competition law enforcement.

This was the case in Case C-252/21, the CJEU judgment referred to above. Although the case provided important insight regarding lawful grounds for processing under the GDPR that could and could not be relied on by Meta for online advertising, it also provided helpful clarity on the CJEU's view of the relationship between competition law and data protection law. In considering whether national competition authorities are entitled to review data processing operations for compliance with data protection law in the context of examining an alleged abuse of dominant position, the Court found that they could, provided that (1) their assessment of GDPR compliance was only to establish the abuse of a dominant position, and (2) the competition authority consulted the data protection authority and deferred to its decisions.

Similarly, Meta is facing a claim in Spain that its failure to have a valid legal basis for processing people's personal data for ads under the GDPR constitutes a breach of competition law.

In the United Kingdom, the Competition Appeals Tribunal gave the go-ahead in February 2024 for a £2 billion plus opt-out collective action against Meta to proceed to trial.[18] The claim centres on Facebook's alleged abuse of its dominant position in relation to the collection of class members' personal data. In this context, a claim for compensation under Article 82 of the United Kingdom's General Data Protection Regulation might have appeared to be a more fitting cause of action; however, the possibilities for bringing an opt-out mass claim against such alleged breaches of data protection law may be limited. In ***Lloyd v. Google LLC***[19], the Supreme Court of the United Kingdom confirmed that, for a representative action under Section 19.6 of the Civil Procedure Rules 1998 (now CPR 19.8) to succeed, it would be necessary to show that wrongful use was made of personal data in respect of each individual and that each individual suffered damage or distress as a result of that breach. A representative action, in the Court's view, was not a suitable vehicle for such individualised assessment. This high bar for data protection opt-out mass claims may have prompted the exploration of the use of competition collective proceedings.

EXPRESS REFERENCE TO INTERPLAY IN SPECIFIC LAWS

Competition laws themselves increasingly recognise how the collection, holding and use of personal data by certain companies can be anticompetitive; for example:

- In 2022, China amended its Anti-monopoly Law (AML) to specifically reference anticompetitive conduct with the use of data and algorithms.
- In Germany, the eprivacy rules were transposed into national competition law (The Act Against Unfair Competition) rather than a separate privacy law, meaning that private rights of action are available where a company considers that a competitor is infringing the eprivacy requirements. Further, if a company offers goods or services to

consumers, consumer protection organisations can request a violating company to seize and desist from such 'unfair' practices, which often goes along with requesting an organisation's lawyers' fees.

- The DMA introduces restrictions on gatekeepers regarding access to and use of user data. Specifically, Article 5(2) prohibits gatekeepers from (1) processing, for the purpose of providing online advertising services, the personal data of end users using third-party services that use the gatekeeper's core platform service, (2) combining personal data from a core platform service with personal data from any other service provided by the gatekeeper (or by a third party), (3) cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper, or (4) signing in end users to other gatekeeper services to combine personal data, without having presented end users with GDPR-level consent choices.

COOPERATION BETWEEN PRIVACY AND COMPETITION AUTHORITIES

Following a market study into online platforms and the digital advertising market in the United Kingdom, the CMA established a Digital Markets Unit to oversee a new regulatory regime to promote greater competition in digital advertising while protecting consumers. To this end, the Digital Regulation Cooperation Forum (DRCF) was formed in July 2020 to ensure greater cooperation between national regulators. The forum – consisting of the CMA, the ICO, Ofcom (the regulator of communications services), the Financial Conduct Authority and the Payment Systems Regulator – was actively engaged in the CMA's investigation into Google's proposal to replace third-party cookies with its Privacy Sandbox.

In a similar vein, the CMA and the ICO have issued joint statements expressing their view of how the two regimes are closely aligned in the context of online advertising.[20]

Some competition authorities and privacy regulators in the European Union have also adopted formal cooperation policies; for example, the French competition authority and the CNIL hold biannual meetings to take joint actions; in Spain, there is a general cooperation protocol between the National Markets and Competition Commission and the Spanish Data Protection Agency; and the Netherlands launched a cooperation platform similar to the United Kingdom's DRCF in October 2021. Germany integrates competition and privacy law with a notably different approach: its competition authority, the Bundeskartellamt, has been granted its own competencies in the area of consumer protection by law. Competition and privacy bodies in certain nations, such as Denmark, Finland, Italy and Poland, recognise the increasing need for collaboration but do so without a formal agreement in place. Belgium has struggled with this informal approach, with the Belgian Competition Authority stating in 2020 that it could not cooperate with the privacy regulator without a specific protocol in place; no such protocol has yet been enacted.

Finally, the Global Privacy Assembly has called for collaboration by authorities across the privacy, consumer protection and competition regulatory spheres. Its Digital Citizen and Consumer Working Group focuses on considering the intersections between privacy and competition. A summary of its most recent findings was published in May 2022, reflecting its overarching view that collaboration between competition agencies and privacy agencies is becoming an imperative for any jurisdiction that seeks to achieve cohesive digital regulation.

ENDOTES

[1] Miranda Cole, Christoph Ritzer and Lara White are partners at Norton Rose Fulbright LLP.

[2] Some laws, such as the EU Digital Services Act, set out minimum mandatory information with which users must be presented.

[3] Third-party cookies are set by parties other than the owner of the website being visited by the user. Examples include the cookies set by domains such as doubleclick.net for products such as Google Ad Manager.

[4] Other forms of tracking technology are also used alongside cookies for advertising purposes, including pixels and device fingerprinting.

[5] For example, the Facebook pixel, which is very commonly used technology incorporated into websites to help optimise ads, builds custom audiences on the Meta platforms and remarkets to people.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, pp. 37–47.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[8] Interactive Advertising Bureau (IAB) Europe's Transparency and Consent Framework (TCF) aims to contribute to the compliance by organisations relying on the OpenRTB Protocol (the OpenRTB Protocol is one of the most widely used protocols for real-time bidding). Since 2019, the Belgian Data Protection Authority (DPA) has received a number of complaints about conformity of the TCF. In February 2022, the Belgian DPA found that IAB Europe was a data controller, such that it could be liable for the breaches of the General Data Protection Regulation (GDPR) identified by the Belgian DPA (e.g., no legal basis for the processing, lack of transparency on the nature and scope of processing, no organisational or technical measures to ensure data protection by design and by default, no data protection officer, no data protection impact assessment). The Belgian DPA imposed a fine of €250,000 on IAB Europe, reflecting the seriousness of the infringements, and ordered corrective measures to bring the TCF into conformity with the GDPR. On appeal, the Brussels Market Court issued an interim ruling in September 2022 referring questions to the Court of Justice of the European Union (CJEU) about the concept of data controller (in light of IAB Europe's position as a standard-setting sectoral organisation) and on whether a 'TC String' (i.e., a digital signal containing user preferences) is 'personal data' under the GDPR. The CJEU answered these questions in ***IAB Europe v. Gegevensbeschermingsautoriteit*** (reference ECLI:EU:C:2024:214), confirming that the 'TC String' was personal data and that IAB Europe acted as joint controller.

[9] Information Commissioner's Office (ICO), 'Our work on adtech' (- https://ico.org.uk/about-the-ico/what-we-do/our-work-on-adtech/).

[10] These include fines for Meta, Google, Apple, TikTok and Microsoft.

[11] The Irish Data Protection Commissioner's Office adopted two decisions on 31 December 2022, in which it concluded that Meta Platforms Ireland Limited was not entitled to rely on 'contract' as the legal basis for its behavioural advertising and imposed fines of €210 million on Facebook and €180 million on Instagram. More recently, it published a decision imposing

a ban on Meta Platforms Ireland Limited for the processing of personal data for behavioural advertising purposes on the basis of contract and legitimate interest.

[12] European Commission, press release, 'Antitrust: Commission sends Statement of Objections to Google over abusive practices in online advertising technology' (14 June 2023).

[13] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[14] Including investigations by authorities in France, Germany, Italy and the United Kingdom.

[15] In 2017, Apple introduced intelligent tracking prevention, which is a privacy feature that blocks third-party cookies by default on the Safari browser.

[16] Chris Jenkins and Angela Nissyrios, 'Google's Privacy Sandbox commitments:Implementation and what comes next – Competition and Markets Authority, Competitionand Markets Authority blog (28 April 2023) (-https://competitionandmarkets.blog.gov.uk/2023/04/28/googles-privacy-sandbox-commitments-implementation-and-what-comes-next/).

[17] Constellation Research vice president and analyst Liz Miller believes the delays and impending antitrust suits against Google are unrelated, though does recognise that Google is 'caught in a riptide between those who want to protect consumer privacy and those who want to level the playing field for small and mid-sized businesses'.

[18] *Dr Liza Lovdahl Gormsen v. (1) Meta Platforms Inc (2) Meta Platforms Ireland Limited (3) Facebook UK Limited* [2024] CAT II.

[19] [2021] UKSC 50.

[20] In a joint statement in May 2021, the ICO and the Competition and Markets Authority (CMA) set out strategies to align the objectives of competition law and data protection with the primary aim of ensuring customers have a choice regarding personal data. Another statement followed in July 2022, addressing online safety and competition in digital markets, and a more detailed ICO–CMA joint paper was released in August 2023, which addressed how harmful online design practices can undermine consumer choice and control over personal information.

Miranda Cole miranda.cole@nortonrosefulbright.com
Christoph Ritzer christoph.ritzer@nortonrosefulbright.com
Lara White lara.white@nortonrosefulbright.com

https://www.nortonrosefulbright.com/en

Read more from this firm on GCR