THE ADTECH CHALLENGE
THRIVING IN AN E-COMMERCE WORLD

Jo Farmer, Mark Hersey and Helen Hart of Lewis Silkin LLP explain the privacy and other legal challenges that advertisers face in navigating the online advertising industry and, in particular, the use of adtech.

The e-commerce industry is big business, accounting for revenue of around £700 billion in 2019, and it is set to grow further (*www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/ecommerceandictactivity/2019*). With the COVID-19 pandemic forcing people to stay at home more and closing physical premises, it is no surprise that consumers are increasingly shopping online. Recent growth has been staggering, with the retail industry seeing internet sales over the last decade increasing from around 8% of the total share to approximately 25% by August 2021, peaking at over 35% around Christmas in 2020 (*www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi*).

For retailers, capturing a share of this market has therefore never been more important and, just as consumers are flocking to digital channels to make purchases, internet-related advertising spend is growing at a fast pace (*see feature article "Challenges in the consumer sector: transformative technology", www.practicallaw.com/w-020-3706*).

This article:

- Explores the privacy and other legal challenges that adtech services pose to the online advertising industry.
- Looks at some key proposed reforms.
- Examines the potential difficulties caused by some recent industry initiatives.
- Explains how advertisers can best position themselves to take advantage of online advertising opportunities and thrive.

THE INTERNET AND ADVERTISING

When Facebook's CEO, Mark Zuckerberg, gave testimony before the US Senate in April 2018 to address revelations that Cambridge Analytica had used personal data for political advertising, many were surprised by Senator Hatch questioning how Facebook could sustain a business model in which users do not pay for the service (*www.youtube.com/watch?v=n2H8wx1aBiQ*). While not obvious to some, it is commonly understood that a free internet is funded by adverts.

More knowledgeable users may also understand that adverts are sometimes personalised based on, among other things, browsing history and user profiles, even if those users do not understand the underlying processes that drive the delivery of adverts.

Adtech

Adtech is, as the name suggests, advertising technology, often in the form of a software-as-a-service product, provided by third-party vendors that publishers (that is, the operators of websites, apps or any other digital property) and advertisers and their media agencies can use to trade online advertising space. Key examples of the vendors and their technologies include:

- Demand-side platforms (DSPs), which are used by advertisers to bid on advertising space.
- Supply-side platforms (SSPs), which are used by publishers to supply advertising space.
- Ad exchanges, which are online marketplaces that connect publishers and advertisers, through DSPs and SSPs, to agree a price for the purchase of advertising space.
- Data management platforms, which collect, segment and analyse user data from a variety of sources and can be used by advertisers, in conjunction with a DSP, to make decisions about the purchase of advertising space.

Programmatic advertising

Programmatic advertising is the use of adtech to buy or sell advertising space in an automated manner, as opposed to through traditional processes of booking media, such as through insertion deals. Real-time bidding (RTB) is an example of programmatic advertising (*see box "Real-time bidding"*). All programmatic advertising involves the use of adtech. However, not all uses of adtech are programmatic in nature; it is possible, for example, for a publisher and an advertiser to directly agree the purchase price of advertising space without automation, but for the transaction to then be executed using adtech.

These services and technologies are highly valuable to advertisers because they provide greater control in respect of the context within which an advert will be displayed and the frequency of delivery, achieve greater relevance in targeting adverts to audiences that are most likely to find them of interest, and target new audiences that otherwise would be difficult to reach. The upshot is a reduction in wasted advertising expenditure and a higher number of conversions; that is, any desired action by the end user in response to the advert, such as clicking on the advert, viewing a video or making a purchase.

For publishers, adtech and programmatic advertising enable exposure to more advertisers, which means higher demand, and therefore price, for advertising space, including non-premium advertising space that may otherwise go unsold. In a nutshell, publishers can obtain higher advertising revenue when using these technologies by achieving a better cost per thousand impressions; that is, the amount that an advertiser pays for each 1,000 views of its advert.

Programmatic advertising also has potential benefits for the end user. In March 2019, a survey by the Information Commissioner's Office (ICO) found that the majority of end users prefer to see adverts that are more likely to be relevant to them and most find it acceptable that websites display adverts in exchange for free content (*https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf*). However, the survey also revealed a lack of awareness of how adtech works and, after respondents had been provided with an explanation, levels of acceptance decreased.

KEY LEGAL CHALLENGES

Advertisers must overcome a number of legal challenges in order to benefit from online advertising opportunities.

Privacy

The adtech ecosystem relies on the collection, dissemination and use of significant amounts of personal data by multiple providers of adtech services (*see "Adtech" above*). The personal data can be as generic as the country in which the end user is based or as specific as their IP address, but can include information about their website browsing history, which can potentially reveal sensitive data, for example, about a person's health, political views or sexual preferences. In addition, much of the personal data is collected through the use of cookies and other similar technologies. From a privacy perspective, this engages the requirements of two key regimes:

- The UK General Data Protection Regulation (UK GDPR), which is the retained EU law version of the General Data Protection Regulation (*679/2016/EU*), and the Data Protection Act 2018 comprise the UK's principal legislative framework that regulates the general use by controllers of personal data. The UK's data protection regime is principles based and, among other things, requires controllers to ensure that their processing of personal data is fair, lawful and transparent (*see feature article "GDPR enforcement: a changed landscape", www.practicallaw.com/w-030-5470*). In the adtech context, the lawful basis for processing is typically based on consent or legitimate interest.
- The Privacy and Electronic Communications Regulations 2003 (*SI 2003/2426*) (2003 Regulations) are the UK's principal piece of e-privacy legislation and set out specific rules in respect of electronic communications, whether or not the communication involves the use of personal data.

Of particular relevance as regards adtech is the requirement to obtain consent, subject

Real-time bidding

One of the most common forms of delivering online advertising is through real-time bidding (RTB), where publishers sell online advertising space, through an auction, to the advertiser that is willing to pay the highest price. The price is determined by a variety of information that might be available to the advertiser, including information about the end user and context relating to the advertising opportunity, such as the site on which, and the time of day at which, the advert will appear. This auction process is automated and takes a matter of milliseconds while the webpage loads.

While RTB is in the spotlight, as seen by the Information Commissioner's Office investigation into RTB, there are many other ways to deliver online adverts that fall under the adtech and programmatic advertising umbrellas (*https://ico.org.uk/about-the-ico/what-we-do/our-work-on-adtech/#blogs; see News brief "ICO's cookie recipe: consent is the missing ingredient", www.practicallaw.com/w-021-3574*).

to certain exemptions, and provide clear and comprehensive information to end users when information on their device is stored or accessed. This requirement is colloquially known as the cookie law despite the 2003 Regulations not mentioning or being constrained to the use of cookies or any other particular type of technology. However, for ease of reference, this article will refer to "using cookies" to mean any storage of, or access to, information on a user device.

Taken together, these two regimes require all controllers within the adtech ecosystem to be transparent; that is:

- To be clear, open and honest with people about how and why their personal data will be used.
- To obtain consent for the initial collection and subsequent use of data for online advertising purposes, subject to some nuanced but imperfect arguments that an organisation's legitimate interests can sometimes provide a valid basis for processing despite the initial collection of the personal data relying on the use of cookies.

Although there are many other privacy issues to consider, such as security of processing, transparency and consent lie at the heart of the privacy challenges faced by the adtech ecosystem.

Transparency and consent

To achieve the benefits that adtech can offer, personal data is shared among many vendors that provide adtech (*see "Adtech" above*). These vendors will often be considered to be controllers of the personal data due to the discretion that they exercise in determining how and why the personal data is processed. This dissemination of personal data has led some to describe the adtech ecosystem as perpetuating the biggest data breach in history and the RTB system, in particular, as a data protection "wild west" (*https://brave.com/rtb-updates/*).

However, on a more practical level, achieving transparency is logistically difficult due to the number of vendors that receive personal data, not least because the majority of these vendors sit between the publisher on the supply side and the advertiser on the demand side, and do not have a direct relationship with the end user. These vendors therefore have limited opportunities to present their privacy policy, which is the medium for achieving transparency, to the end user. In addition, the underlying processing activities are complex, making it challenging to explain the activities in a way that is readily understood by the average end user.

For similar reasons, it can also be difficult for vendors to obtain effective consent for the use of cookies and the processing of personal data. To be valid, the UK GDPR requires consent to be a freely given, specific and informed exercise of choice; that is, it should be opt-in based. The requirement for consent to be informed demonstrates that transparency and consent are interrelated, although separate, concepts. Therefore, a lack of transparency will be fatal to effective consent.

In addition, the requirement for consent to be specific means that it must be granted to each controller by name and granular choice should be provided in respect of the different purposes and types of processing activity. In adtech, there are many different underlying processing activities, for example, building a user profile and measuring advert effectiveness, which can undermine efforts to achieve granular consent.

Advertisers may not be able to absolve themselves of responsibility for ensuring compliance with transparency and consent requirements simply by ensuring that they do not receive any of the underlying personal data. This is an area that is subject to debate, but the European Court of Justice has held that having access to personal data is not a prerequisite to controllership and that an entity can be a controller of personal data where it requests or takes part, by defining parameters, in the processing of personal data (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH C-210/16*).

Regulatory enforcement

Much remains to be seen as to the approach that the ICO will take to enforcing transparency and consent requirements, and as to the potential impact of any legal challenges. However, getting it wrong has the potential to be costly. The ICO has the power to issue fines for non-compliance of up to the greater of 4% of total global annual turnover or £17.5 million. Privacy and trust are inextricably linked, and regulatory action can have serious consequences for an organisation's reputation.

While it is likely that fines on this scale are likely to be reserved for the most serious breaches, and although most of the processing activities that drive the adtech industry are carried out by intermediaries that connect advertisers to publishers, publishers and advertisers cannot afford to be complacent. The ICO and other regulators frequently signal a willingness to find joint controllership and joint, but not necessarily equal, responsibility for the use of personal data, particularly where allowing third parties to collect personal data or where a commercial benefit to processing activities is derived.

Any regulatory action is likely to necessitate remedial action, which may come at significant operational cost and may hinder the ability to rely on, and reduce the value of, existing data sets (*see feature articles "Data use: protecting a critical resource", www.practicallaw.com/w-012-5424 and "Data assets: protecting and driving value in a digital age", www.practicallaw.com/w-019-8276*).

Contractual claims

In addition, the potential for third-party claims should not be underestimated. To overcome the transparency and consent problem, organisations that have no direct relationship with the end user will frequently impose contractual obligations on their counterparties that discharge these obligations on their behalf. While the ICO has indicated that it is likely to give short shrift should an organisation seek to rely on this as a defence, that would not prevent the organisation from pursuing an action against its contractual counterparty for a failure to comply with contractual obligations.

Other challenges

There are other, non-privacy related, risks that advertisers face when buying advertising space through the use of adtech, in particular, relating to viewability and brand safety (*see boxes "Viewability" and "Brand safety"*).

PROPOSED REFORMS

A raft of regulatory and legislative change is proposed at an EU and UK level that is intended to improve safety and competition in the digital market, and shape how the adtech industry operates.

EU digital services package

In December 2020, the European Commission (the Commission) published its proposals for two legislative initiatives, a Digital Services

Act (DSA) and Digital Markets Act (DMA), to upgrade rules governing digital services in the EU (*https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; see feature article "Regulating digital services in the EU: a paradigm-shifting legislative framework, www.practicallaw.com/w-030-6172*).

The DSA aims to create a safer digital space in which the fundamental rights of all users of digital services are protected. For online advertising, the proposals include new transparency rules to give users meaningful information about the adverts that they see online, including real-time information on why they have been targeted with a specific advert.

The DMA aims to ensure fair competition within EU digital markets and proposes to establish rules that will apply to large online platforms, known as gatekeepers. The Commission considers that the conditions under which gatekeepers provide online advertising services to businesses lack transparency. This is partly due to the complexity of programmatic advertising, which leads to higher costs and a lack of information about the conditions of the advertising services that have been bought and undermines the ability to switch to alternative service providers. The proposals in the DMA will therefore require gatekeepers to provide advertisers and publishers with more information about the price paid for the various advertising services that are provided within the advertising chain.

UK digital markets study

The Competition and Markets Authority (CMA) is also concerned about competition within digital markets and, in July 2020, completed its market study into online platforms and the digital advertising market in the UK (*www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study*). The CMA identified a number of competition concerns within digital advertising that, among other issues, lead to consumers giving up more data than they would like and increase prices for goods and services across the economy.

In order to address this, the CMA established a Digital Markets Unit (DMU) that will oversee a new regulatory code for digital firms that hold a dominant market position, to promote greater competition and protect consumers (*www.gov.uk/government/collections/digital-markets-unit*). The new code will require platforms that are funded by digital advertising to be more transparent about their services and how they use personal data, and to provide users with choice in respect of their receipt of personalised advertising. The DMU is expected to work alongside other regulators, including the ICO. To this end, in May 2021, the CMA and the ICO issued a joint statement whereby they committed to work together to achieve an ecosystem where users have choice over the service they prefer and a clear understanding of how their data will be used to inform that decision (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf*).

Online safety in the UK

The government's ambition is to make the UK the safest place in the world to be online while defending freedom of expression. It plans to introduce legislation to achieve this, principally to tackle illegal activity taking place online and prevent children from being exposed to inappropriate material (*www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response*). However, the proposed legislation will also address other types of online harm, including misinformation, and it is expected that some types of advertising will fall within the scope of the online harms regulatory framework (*see News brief "The Online Safety Bill: will it do more harm than good?", www.practicallaw.com/w-031-4818*).

Online advertising programmes

The government's Online Advertising Programme is considering how the online advertising market is regulated in the UK and, at the end of 2021, it will consult on the use of personal data in the targeting of online advertising and ensuring transparency and accountability with respect to the content and placement of online advertising (*www.gov.uk/guidance/digital-regulation-overview-of-government-activity*).

OTHER INDUSTRY CHALLENGES

The growing pressure on the adtech industry to use personal data responsibly has led to some industry initiatives that have hampered, or have the potential to hamper, the ability of advertisers to target users.

App tracking

In April 2021, Apple rolled out iOS 14.5 and, with it, a requirement for iOS apps to request user permission through Apple's AppTrackingTransparency framework if the app owner would like to track users. This requirement is commonly misunderstood to apply only to the use of a device's Identifier for Advertisers (IDFA) for advertising purposes but, crucially, Apple's definition of tracking applies to a wider range of scenarios.

According to Apple, tracking refers to the act of linking user or device data collected from an app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or

Viewability

Advert viewability is the measurement of whether an advert is actually viewable by an end user and, if so, for how long. There are a number of reasons why an advert might not be seen. For example, it could be hidden deep down in a website page, way beyond the point that anyone would scroll, it might be visible only for a quarter of a second, or it could be overlayed with another advert, meaning that the advert cannot be seen by the human eye.

Clearly, advertisers will want to make sure that an advert is capable of being viewed effectively by the end user. However, UK viewability statistics often hover around 70%, meaning that for every ten adverts that an advertiser has paid for, three will, on average, not be seen by any end users (*www.iabuk.com/opinions/uk-viewability-hits-highest-point-ever*). One practical step that advertisers can take is to state in their contracts with media buying agencies that the agency will monitor advert viewability using available content verification tools, and that the advertiser will not pay for adverts that do not reach agreed minimum thresholds as to the size of the content and the length of time it is viewable. In the UK, a commonly used metric is the Internet Advertising Bureau's Joint Industry Committee for Web Standards viewability product principles (*www.iabuk.com/news-article/viewability-status*).

advertising measurement purposes as well as to sharing user or device data with data brokers.

This extremely wide definition therefore extends beyond the use of app-based tracking or retargeting technologies such as software development kits (SDKs), as it includes the use of any app-collected data where the data is linked with another organisation's data for any advertising-related purpose. This definition would therefore include, for example:

- Custom audience advertising; that is, sharing a list of customer email addresses collected through an iOS app with a third-party social media platform in order to target adverts to customers who are also users of the platform.

- Lookalike audience advertising; that is, sharing that same list with a social media platform to find new audiences that share similar characteristics with the custom audience, based on information that is known by the social media platform about its users.

Accordingly, any tracking will require a permission through an iOS prompt and, in addition, advertisers may need to obtain a separate and more granular consent to comply with the requirements of the UK GDPR or the 2003 Regulations, or both, thereby potentially creating a double opt-in requirement.

Third-party cookies

Cookies are a key component of the internet. Cookies are text files that are stored on a browser and can provide many benefits to users, for example by remembering a user's preferences and providing functional benefits such as shopping carts. However, they can also be used by third parties other than the operator of the website that the user is visiting to track user browsing history and to build detailed user profiles that are then used to deliver targeted adverts to users. These are called third-party cookies. In some cases, based on the content that the user is viewing, the data that is collected may allow inferences to be drawn about a user's health and other characteristics that are considered special category data for the purposes of the UK GDPR. Third-party cookies therefore represent a threat to user privacy.

A number of browsers, including Apple's Safari and Mozilla's Firefox, have blocked third-party cookies for some time. However, in January 2020, Google sent shockwaves throughout the industry by announcing that it intended to phase out support of third-party cookies in Chrome, which according to some statistics enjoys a 69% share of the global desktop internet browser market. Google's intention is to create, through its Privacy Sandbox initiative, alternative technologies that are more privacy friendly (*https://privacysandbox.com/*).

While third-party cookies are not the only way to track users, Google's proposals will limit the capability of third parties to target users and the CMA has concerns that the proposals will impede competition in digital advertising markets (*www.gov.uk/government/news/cma-to-have-key-oversight-role-over-google-s-planned-removal-of-third-party-cookies*). In June 2021, Google acknowledged that there is a clear need "across the ecosystem to get this right" and announced that it is delaying its proposals, setting a new target of late 2023 for third-party cookie support to be depreciated in Chrome (*https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones*).

Brand safety

When offline adverts are bought in an analogue way, advertisers can choose where their adverts are placed. For example, a toy company may not want their advert placed next to an advert for a vaping product, and any brand would likely have concerns about their advert being placed next to content about terrorism. However, when adverts are bought programmatically, there is an increased risk of an advert appearing next to unsuitable content or with unsuitable publishers.

A practical step that many advertisers take is to ask their media buying agency to adopt tools which procure that served adverts do not appear next to unsuitable content. The contract between the media buying agency and the advertiser typically lists the content that is deemed to be unsuitable or prohibited to be next to the advert, and will likely include content such as firearm sales, illegal content, adult content and terrorism, and might include other content deemed inappropriate to the brand such as gambling, cosmetic procedures, nicotine products and alcohol.

HOW ADVERTISERS CAN RESPOND

Advertisers need to consider how best to respond to the various challenges that present themselves in the online advertising environment.

Advertising agency contract

Advertisers will rarely have direct contracts with publishers or the adtech vendors; they will instead have a contract with their advertising agency, which will buy media and procure services from adtech vendors on the advertiser's behalf. Advertising agencies will not necessarily agree to having all of the risk in this evolving area shifted onto them. However, the contract between the advertising agency and the advertiser can usefully set out the advertiser's expectations as to how the agency should engage with adtech vendors on its behalf. In addition, the contract between the advertising agency and the advertiser can set out the advertiser's expectations in relation to advert viewability and brand safety (*see boxes "Viewability" and "Brand safety"*).

First-party data assets

As discussed, it is becoming increasingly difficult to use pervasive third-party tracking technologies to target users (*see "Third-party cookies" above*). Advertisers can mitigate some of the challenges by directly collecting data from their customers or target audience, whether through the use of first-party tracking technologies that observe use of the advertiser's website or other digital property, details of purchase history, surveys, or any other touchpoint.

First-party data is often regarded as the most valuable data asset, as advertisers can have confidence in its quality, accuracy and relevance as well as in the compliance profile around its collection. The data can be as simple as an email address or any other identifier that can be matched with identifiers held by social media and other platforms for targeting purposes, or the advertiser can build more sophisticated assets, such as targeting segments; that is, a group of customers who share similar characteristics and behaviours.

However, finding innovative ways to obtain first-party data is only a part of the solution; care needs to be taken to ensure that both the initial collection and subsequent use of the data complies with data protection laws.

Due diligence

A key pillar of data protection compliance is ensuring that responsibility is taken for the processing of personal data and how data protection requirements, including transparency and lawfulness, will be met. This is known as the accountability principle.

It is critical that advertisers conduct appropriate due diligence in respect of third-party adtech vendors. Where those third parties use the advertiser's first-party data, the key is to understand who the data will be shared with, how and why it will be used, and what security measures will be implemented to protect personal data. Advertisers should consider whether it is necessary to ensure that vendors are restricted from using their first-party data for the vendor's own benefit or for the benefit of other advertisers. If appropriate restrictions cannot be obtained, careful thought will be required to ensure that third parties have any necessary rights and permissions to use the personal data for their own benefit. Advertisers need to be cautious about providing assurances that they have obtained rights and permissions on behalf of others.

However, due diligence obligations extend beyond the use of first-party data. If any adtech services involve the use of data collected by third parties, care should be taken to ensure that the third-party data has been compiled fairly and lawfully, and that the individuals involved understood that their data would be used for the particular purpose concerned. Simply accepting assurances, contractual or otherwise, that data is compliant is unlikely to be sufficient. This is especially true if the third-party data will be received by the advertiser and used to enrich its own first-party data. However, a gold-standard approach to data protection requires due diligence to be undertaken whenever third-party data is leveraged, even if the advertiser will not receive the underlying personal data.

Privacy statements

It is critical to ensure that individuals have a clear understanding as to how and why their data is used and who their data will be shared with. Adtech is complicated and therefore it will be vital for organisations to explain their use of it in plain, concise and easy to understand language. Successfully achieving transparency should lead to individuals having greater control over their personal data, and increase the trust and confidence that individuals have in the advertiser.

This means that organisations should ensure that their use and sharing of first-party data assets and of any third-party data that may be used in pursuit of the advertiser's campaign are described in detail in a privacy policy or statement.

However, advertisers should take care to not be over-reliant on information set out in privacy statements. The ICO has frequently opined that complex use cases should be brought to the individuals' attention using prominent notices as opposed to burying information elsewhere. Accordingly, to achieve gold-standard transparency, advertisers should look to develop a layered approach to transparency through just-in-time notices and sophisticated, but not convoluted, privacy preference centres. Success in this area will also help to demonstrate that the processing activity is within the individuals' reasonable expectations which, in turn, will help to establish that the advertiser has a lawful basis to undertake the activity.

Choice and control

Organisations must establish a lawful basis for their processing activity. For most advertising and marketing purposes, only two of a possible six bases are available: consent and legitimate interest.

Related information

This article is at practicallaw.com/w-032-9223

Other links from uk.practicallaw.com/

Topics

Advertising and marketing	topic/0-103-1114
Consumer	topic/0-103-2038
Cookies	topic/5-616-6218
Data protection: general	topic/1-616-6550
Direct marketing: data protection	topic/9-616-6179
E-commerce	topic/2-103-1274
Information technology	topic/5-103-2074
Internet	topic/8-383-8686
Technology: data protection	topic/8-616-6207

Practice notes

Advertising and marketing toolkit	0-522-4170
Consumer law toolkit	7-525-0330
Cookies: impact of UK GDPR and DPA 2018	w-016-7485
Data Protection Act 2018: overview	w-014-5998
Digital marketing: an overview	8-384-8223
Direct marketing and data protection: consent and preference services (UK)	w-014-7457
Overview of UK GDPR	w-013-3757

Previous articles

GDPR enforcement: a changed landscape (2021)	w-030-5470
Regulating digital services in the EU: A paradigm-shifting legislative framework (2021)	w-030-6172
Challenges in the consumer sector: transformative technology (2019)	w-020-3706
Data assets: protecting and driving value in a digital age (2019)	w-019-8276
E-Privacy Regulation: developing slowly (2019)	w-020-8272
GDPR one year on: taking stock (2019)	w-020-0982
Data use: protecting a critical resource (2018)	w-012-5424

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

In most circumstances, a plain reading of UK data protection law does not mandate that organisations obtain consent for any given processing activity. The 2003 Regulations contain some notable and relatively well-known exceptions, such as the requirement to obtain consent to send unsolicited marketing emails or to use cookies. In theory, therefore, organisations can rely on legitimate interests to use personal data in the adtech sphere, although consent will be required for the collection of data through the use of cookies and, arguably, for the subsequent use of that data (*see "Privacy" above*).

However, the ICO has been at pains to point out that legitimate interests should not be seen as the easy option and that many organisations are not doing enough to ensure that processing activities are within the reasonable expectations of data subjects, which will be fatal to establishing legitimate interests as a lawful basis. Consequently, the ICO advises organisations to seek consent for many adtech-related processing activities.

In practice, advertisers that achieve full transparency will have a much better chance of establishing legitimate interests (*see "Transparency and consent" and "Privacy statements" above*). However, alone this will not be enough and advertisers should look to offer choice and control in the form of opt-outs, where relying on legitimate interest, or opt-ins, where relying on consent, to ensure that their chosen lawful basis is as robust as possible. Again, developing a privacy preference centre and finding other opportunities to obtain permissions will be key to success.

There will often be a tension between offering choice and achieving conversions. However, advertisers that look to overcome these issues by incentivising, but not deceiving, customers and building trust will be more likely to prosper.

Jo Farmer is a partner, Mark Hersey is a senior associate, and Helen Hart is a senior practice development lawyer, at Lewis Silkin LLP.