
# **AdTech** round-up: Summer 2023

ReedSmith

Driving progress
through partnership

# The halfway point of 2023 sees more developments in adtech across technology, regulation, and consumer demands.

Some trends are moving at a slower pace such as the feted move away from third-party cookies in favor of more privacy-friendly alternatives. With regulators continuing to focus on cookies in the last few months the days of reading about cookies are certainly not numbered just yet. Also moving at a slow but steady pace is brand concentration on new first-party data strategies which, even if often less reliant on tracking technologies, brings its own challenges not least around consents and lawful basis for processing, particularly in Europe, with some inconsistent decisions from regulators of late. The use of solutions such as identity resolution and data clean rooms is certainly on the rise in an attempt to placate privacy-conscious consumers and regulators, and more new privacy-conscious technologies are expected to emerge if the mounting guidance around so-called privacy enhancing techniques, or PETs, is anything to go by.

This half year has also seen some faster paced changes. The announcement of the new Data Privacy Framework for personal data transfers from the EU to the US will have everyone in the adtech industry pleased, even if the threat of more challenges always hangs over such initiatives. Also increasing at speed is the use of AI for automation, improvement of targeting, ad fraud and new ad measurement techniques. However, it could be a case of out of the (privacy) pot and into the (AI) fire as regulators around the world race to provide guidance and even regulation in this space.

For more information on how AI, data protection, and advertising laws interact, see The Reed Smith **Entertainment and Media Guide to AI**.

# Contents

# United Kingdom

### *Data Protection and Digital Information (No. 2) Bill*

On March 8, 2023, the UK government presented a new (and improved?) version of the Data Protection and Digital Information Bill (the Bill). As with the earlier version (covered in our previous round-up), the Bill aims to introduce certain changes to the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (but note that it is **not** a complete overhaul of the fundamental data protection principles), with its core objective being to simplify compliance and reduce paperwork whilst maintaining data adequacy with the European Union (EU). The Bill looks to update the Privacy and Electronic Communications (EC Directive) Regulations 2003 by introducing changes to cookie requirements, exempting certain so-called low-risk cookies from requiring a cookie banner or consent mechanism. Unsurprisingly, it has been confirmed that consent will still be needed to carry out targeted advertising using such technologies and, as such, publishers – the parties usually burdened with collecting consent on behalf of the entire adtech value chain – can expect little respite or real change from the Bill. Whilst still subject to potential amendments, the Bill's current form suggests a limited impact on the overall data protection landscape (especially given the global nature of adtech), but there are still calls from industry players for more to be done for cookies that are utilized in audience measurement and ad performance. The Bill is now due to have its report stage, and it will then need to be reviewed by the House of Lords before it can be approved and adopted.

Read more in our article on the Bill here.

### *Online Safety Bill edges toward publication*

As covered in our previous adtech round-up, the UK's Online Safety Bill (OSB) has undergone substantial changes since its introduction in 2021. In its current form, the OSB includes provisions for criminalizing fraudulent advertisements, as well as obligations around removing content that is illegal (or prohibited by the terms of use) and content that is harmful to children. It will also give adult users the ability to tailor the types of content they are offered, to limit the amount of harmful content disseminated to others. This will undoubtedly represent extra work for adtech firms to the extent that they are covered by the provisions. However, it is difficult to know exactly what will be required until Ofcom publishes its new codes of practice, which are currently in production and expected to be released sometime this year.

The OSB has now reached the committee stage in the House of Lords and, after much delay, is expected to become law later this year. Of course, in the meantime, adtech companies are already working hard on implementing the changes required for the EU's Digital Services Act (DSA).

### *ISBA's second Programmatic Supply Chain Transparency Study*

In mid-January 2023, the Incorporated Society of British Advertisers – in partnership with PwC – released its second study of the digital programmatic supply chain. The study highlights key improvements in the last two years, such as better data quality and access, an increase in the ad impression match rate, and a reduction in ad spend.

### *ICO updates guidance on AI and data protection*

The role of artificial intelligence (AI) in advertising is increasing at pace, with new models allowing advertisers to identify and segment audiences, resulting in improved and more accurate targeting, measurement, and analytics. Given the sheer amount of personal data commonly required to both deliver targeted advertising and develop AI systems to facilitate this, there is an obvious cross-over with data protection laws and, more importantly, the regulators behind those laws. In the UK, the Information Commissioner's Office (ICO) published updated guidance on AI and data protection in March 2023. The ICO has prioritized AI for several years and previously released guidance in 2020 and supplementary recommendations in 2022. The updated guidance includes content on fairness (including considerations of potential bias and discrimination), transparency (complementing existing guidelines), lawfulness (with new sections on inferences, affinity groups, and special category data), and accountability and governance (highlighting what organizations should consider as part of their data protection impact assessments).

At present, the complex interactions between AI, advertising, and data protection have yet to be specifically considered by the ICO but the existing guidance provides a general view of how the ICO expects any data controller operating AI systems to behave when processing personal data. This would include most parties in the adtech value chain utilizing AI. It should be noted that, whilst not legally binding, the updated guidance can be seen as best practices for responsible AI implementation that will be of use to adtech firms seeking to integrate AI functionality into their business models.

### *UK takes a sectoral approach to AI regulation*

Sticking with AI but looking more broadly beyond data protection issues, an AI policy paper released by the UK government has outlined a set of proposed rules for the regulation of AI, built upon six principles, which regulators can utilize with flexibility. The aim is to foster innovation while prioritizing the safety and fairness of AI usage in the UK. Instead of a centralized approach to AI regulation, like that in the EU, the UK government has suggested empowering regulators across different sectors to adopt customized and context-specific strategies for AI implementation. This approach will involve the exploitation of sandboxes, guidance, and codes of practice. The UK Advertising Standards Authority (ASA) is taking an increasingly data science-led approach to its own regulation and is automating its processes where appropriate. As AI is increasingly integrated into UK advertising, the ASA will need to implement the government's strategy by publishing codes to regulate firms operating in the sector.

# European Union

### *Authorities use the full range of their toolbox to scrutinize and investigate the adtech industry*

At the beginning of the year, following a study of the impact of recent developments in digital advertising on privacy, publishers, and advertisers, the European Commission (Commission) published a report calling for greater transparency and accountability in the digital advertising ecosystem, stressing the need to increase individuals' control over how their personal data is used for digital advertising and the need to address a number of obstacles that make it harder for advertisers and publishers to know their audience. The report considers that the current legal framework, which combines EU data protection rules and competition and consumer laws, as well as the new Digital Markets Act (DMA) and the Digital Services Act (DSA), still leaves some regulatory gaps that need to be addressed. The report concludes that on balance, the evidence gathered during the study indicates a strong case for reforming digital advertising.

The rollout of the DMA will continue to impact the adtech sector and require big players qualifying as gatekeepers to adapt their business models. For instance, the DMA requires gatekeepers to share information about pricing and fees and to provide advertisers and publishers with access to the gatekeeper's performance-measuring tools, and with the data necessary to carry out their own independent verification. The DMA also prohibits gatekeepers from processing the personal data of end users using their services provided by third parties that make use of the gatekeepers' core services for online advertising purposes unless consent is obtained from those end users. Accordingly, we expect such consents to begin appearing in the coming months, whether built into the existing consent management platform, user account settings, or as an entirely new series of consents altogether.

Over the last few months, the Commission has hosted several public workshops – notably on self-preferencing, interoperability, app store provisions, and data-related obligations – which were attended by several big tech companies. The Commission announced on July 4, 2023 that seven companies had notified the Commission that they meet the DMA's "gatekeepers" threshold and, following their designation later this summer, gatekeepers will have six months to comply with the requirements in the DMA – by March 5, 2024 at the latest.

Finally, the upcoming rollout of the DSA (as discussed in our previous adtech round-ups) cannot be ignored in relation to adtech regulation. There are a number of advertising-specific obligations introduced which relate to information provision, ad transparency, content reporting, illegal ads, and repositories that online platforms will need to be aware of and ensure they comply with prior to February 2024. An outright ban on targeting children or based on sensitive information is also introduced. It should be borne in mind that there are additional obligations for Very Large Online Platforms and Very Large Online Search Engines, 19 of which were designated based on their more than 45 million monthly active users earlier this year.

The DMA and DSA are not the only tools that authorities may utilize to regulate adtech. Traditional antitrust enforcement is still very much present across Europe, and recently, the Commission issued a statement of objections against a major player in the adtech industry, as it suspected that the major player abused its dominant position on the market by implementing self-preferencing practices and favoring its own service – similar themes to the above-mentioned report of the Commission.

### *EDPB publishes its Cookie Banner Taskforce report*

On January 18, 2023, the European Data Protection Board (EDPB) published and adopted a report of the work undertaken by its Cookie Banner Taskforce (EDPB report). The EDPB report summarizes the common denominators agreed upon by supervisory authorities in the EU on their interpretation of local transpositions of the ePrivacy Directive and its interplay with the GDPR.

The EDPB report raises the following points:

- The applicable framework for placing and reading cookies is the ePrivacy Directive and its national implementing laws; the GDPR is the applicable framework for data processing after placing cookies.
- There is no valid consent if there is no "Reject" button on any layer of the cookie consent solution.
- Pre-ticked boxes do not lead to valid consent.
- Cookie banners may not be designed in such a way as to give users the impression that they have to give consent or as to clearly force users to give consent. There is no valid consent if the "Reject" option is embedded in a paragraph of text without any visual support to draw the users' attention to it.

- Reviews must be carried out on a case-by-case basis to determine whether the colors and contrasts of buttons are not obviously misleading and do not result in invalid consent.
- Where personal data is collected unlawfully due to invalid consent or otherwise, all subsequent data processing is also unlawful.
- Cookies that allow a website owner to remember user preferences for a service (if consent was obtained) should be considered essential cookies.
- Website owners should provide easily accessible solutions – such as a small, permanently visible icon or link in a standard location – that allow users to withdraw cookie consent at any time.

Given the onus on publishers to collect valid cookie consent on behalf of the entire adtech value chain, compliance with applicable cookie consent requirements across the EU is crucial to allow for the lawful onward use of personal data.

### *Updated Cookie Guidance from the AEPD*

In Spain, new guidance on cookies has recently been published by the local data protection authority (AEPD). Like the EDPB report mentioned above, the guidance states that a cookie banner must include both an "accept" and "reject" button (or similar) on the same layer, and that those buttons must be of equal prominence and appeal, and their color or contrast must not be obviously misleading for users. Regarding cookie paywalls, the AEPD also appears to suggest that there may be cases where these may now be permitted. Among these key changes, perhaps most notable is that the guidance sets out additional requirements for children where websites or online services are specifically targeted at them. It is made clear that for children under the age of 14, parental consent is needed to use the service (using "reasonable efforts" for verification and taking a risk-based approach) and where cookies are used for analytical purposes only, verifiable parental consent may be obtained by including a simple notice in the cookie banner that children under 14 should tell a parent or guardian to accept or reject the cookies, thereby avoiding gathering additional data from either the parent or the child. But, where cookies are used for personalized advertising, the service must first ask the user to confirm that they are 14 or older, and if the user is not, include a message in the banner for their parent or guardian to accept or reject the cookies on their behalf. Publishers with a Spanish presence should consider the material changes necessary to their cookie banners to ensure compliance with the new requirements, with changes required by no later than January 11, 2024. *Read more in our article here.*

### *AI Act reaches trilogue negotiation stage*

Whilst unlikely to have a material effect on the regulation of adtech, it is worth noting that the EU's AI Act, following a period of review by the three European Union institutions, has reached trilogue negotiations with the view of agreeing a final text. This is expected towards the end of the year, with obligations becoming effective in late 2024 or early 2025. The AI Act itself is generally geared towards the regulation of high-risk and prohibited AI systems, which at the time of writing is unlikely to cover the (reasonable) use of AI in advertising beyond certain prohibited racial profiling activities. For generative AI, foundation models and low-risk AI systems, organizations deploying (that is, using and making available, but not developing) such systems can expect to need to comply with some relatively light touch provisions around transparency and record keeping. Of course, as the trilogue negotiations progress, the scope of the AI Act is subject to change.

### *Third time's a charm: The EU-U.S. Data Privacy Framework*

In July, the Commission issued the long-awaited adequacy decision for transfers between the EU and the United States by way of the Data Privacy Framework (DPF). The European Court of Justice had previously invalidated both the Safe Harbor and Privacy Shield schemes in 2015 and 2020 respectively, after challenges by Austrian privacy activist Max Schrems (with such decisions being colloquially known as Schrems I and Schrems II). Following those decisions, earlier this year, President Biden signed Executive Order 14086 on "Enhancing Safeguards for United States Signals Intelligence Activities," which introduced new binding safeguards. See our previous client alert on how the draft adequacy decision, including in relation to this Executive Order, addresses concerns raised in Schrems II.

### *Doubts cast on lawful bases for behavioral advertising*

A decision by the Irish Data Protection Commissioner (DPC) (following a binding direction by the EDPB) caused ripples amongst the global adtech community by declaring that targeted advertising and profiling of individuals based on contractual necessity is not lawful, even if personalized advertising forms part of the core of an online service. The DPC concluded that, whilst issuing fines for non-compliance, consent is the only viable lawful basis to rely upon to carry out such processing activities. Whilst the position is not disputed for cookie-based targeting, the decision evoked surprise given that some supervisory authorities across the EU had advised to the contrary in their local guidance on the implementation of the GDPR. Many providers are beginning to consider alternatives to contractual necessity as a lawful basis for targeting, including collection of consent and even legitimate interests (although reliance on LI is now also potentially up in the air).

Further to this, on July 4, 2023, the Court of Justice of the European Union (CJEU) issued a judgment in a case involving the German competition authority which, amongst other issues, deals with requirements for the processing of personal data collected by third party websites, apps, and ancillary services on behalf of an online platform. With regards to the lawful basis for processing personal data captured cross-service for personalized services and targeted advertising, the judgment seems to suggest that neither legitimate interests nor performance of a contract would be appropriate, and that consent would be the only applicable legal basis available to rely on. This decision has caused confusion amongst many given that this is a competition decision and contradicts prior guidance and enforcement notices of EU supervisory authorities which have suggested previously that legitimate interests may well be an appropriate lawful basis outside of the use of cookies and similar technologies. As a result, some online platforms have proposed shifting their behavioral targeting of European users to an opt-in model, moving from reliance upon contractual necessity or legitimate interests as the lawful basis for processing the personal data upholding such systems, to a solely consent-based approach.

### *Upcoming rules on children's data in the EU*

Whilst in the UK the Age Appropriate Design Code (AADC) has been around for some time, and certain EU Member States have developed their own guidance (including, notably, the Irish Fundamentals) there is currently no EU wide equivalent. A product of the Better Internet for Kids (BIK+) strategy, the Commission announced that it will facilitate an EU code of conduct on age-appropriate design (the Code), which will build on existing regulatory frameworks. The Code aims to address "the lack of effective age verification, the gathering of personal data, and the commercial manipulation of children as well as the need for child-appropriate communication." Whilst adtech is not the primary focus, the focus on kids under 18 will still be directly relevant to many solutions and digital services which such youth may use and visit.

A working group of up to 30 members is being formed to assist with drafting the Code and establishing a monitoring system with the aim of making the Code public by mid-2024. As these meetings progress, there should be more announcements on the scope of the Code and the potential for enforcement around it. The EDPB's Work Programme 2023-2024 also includes the preparation of guidelines on the processing of children's data, and there is likely to be significant interplay between these future guidelines, which will be issued under the EU GDPR, and the Code, given their similar subject matter. It is highly likely that the Code will set out specific rules on the use of children's data for advertising purposes, similar to the standards set by the AADC.

# France

### *Action plan for the compliance of mobile apps*

The French data protection authority (CNIL) has announced a new action plan to encourage mobile apps to be GDPR compliant. The CNIL is considering starting large-scale investigations, similar to its work on cookies and other trackers which was mentioned in our previous update. In particular, the investigation is likely to focus on data processing operations involving a higher level of risk for individuals (such as the processing of health-related data).

### *New guidelines aimed at pharmaceutical companies' data processing activities*

The CNIL has published two sets of guidelines to help pharmaceutical companies analyze their GDPR compliance. These guidelines are limited in scope and relate mainly to drugs for human use. Specifically, these guidelines refer to the provisions of the French public health code which allow pharmaceutical companies, in some circumstances, to make certain drugs available to patients outside the scope of their marketing authorization. The CNIL guidelines will enable stakeholders to process relevant personal data without the need for authorization from the CNIL. They will also assist pharmaceutical companies in carrying out data protection impact analyses when required.

### *Updates expected to health data hosting standard*

The French Digital Health Agency (ANS) has announced its plans to revise the health data hosting (HDS) standard applicable to companies hosting health data. The aim of these revisions is to: (i) make the guarantees provided to customers by certified hosting providers easier to understand; (ii) clarify the contractual obligations on service providers that are using the services of a certified hosting provider; and (iii) introduce further regulatory protection for data transfers outside the EU.

### *CNIL enforcement actions*

A recent CNIL decision, dated June 15, 2023, demonstrates how the collection of data subjects' consent is a hot topic for the regulator. It recently sanctioned CRITEO, which specializes in targeted advertising, with a fine of €40 million for failing to verify that data subjects had been properly giving their consent to receive targeted ads. Specifically, CRITEO collects browsing data through a cookie tracker to analyze the browsing habits of Internet users and display targeted advertisements. In this case, CRITEO had not put in place any measures to ensure that its partners were validly collecting users' consent. More specifically, the CNIL conducted an investigation into the contracts between CRITEO and its partners and concluded that they did not contain any clauses meaning they would have to provide proof of Internet users' consent to CRITEO. In addition, CRITEO had not vetted any of its partners.

### *Competition rules*

The adtech sector also remains on the radar of the French Competition Authority (FCA). In its 2023-2024 road map, the FCA said that it would focus on multiple stages of the advertising technology chain. In addition, the FCA recently took interim measures against a company active in the online ad verification sector, ordering it to define a set of objective, transparent, non-discriminatory, and proportionate criteria for filtering through those wishing to access its services. These cases overlap with the jurisdiction of the DMA and antitrust regimes, as the practices investigated could also be disciplined by the DMA. On the digital rules enforcement side, on July 4, 2023, the French consumer protection agency (DGCCRF) imposed a fine of €2.015 million on the leading search engine provider for failure to comply with consumer information regulations applicable to digital platform operators. The fine targeted the non-compliance of its search engine, its comparison tool for tourist accommodation, and its app.

A new law in the adtech sector came into force in France this year, aimed at better regulating social media influencers. The goal is to prevent potential abuses of power by influencers on social media (e.g., encouraging others to take up extreme diets, undergo cosmetic surgery, place excessive bets, promote counterfeit goods, etc.). Influencers are people who leverage their following on social media platforms to promote content (e.g., goods, services, and causes) in return for payment. The new law does not quantify the number of followers required for someone to be deemed an influencer, that is, even "minor" influencers (known as micro-influencers) are covered by the rules. The law explicitly also targets influencers' agents and the platforms hosting their activity. In addition, they will have to make it clear when a piece of content is an advertisement. Platforms will also have obligations – in accordance with their DSA obligations – such as facilitating the reporting of illegal content. Influencers breaking these rules will face sanctions, such as imprisonment, fines, and even bans on being influencers.

# Germany

### *German data protection authorities confirm that pay-or-accept models may be lawful*

Many websites, in particular those with journalistic content, have implemented the pay-or-accept model (the so-called PUR model). Following the PUR model, website users are presented with two choices: (1) using the website for free, but consenting to the use of tracking cookies, or (2) using the website without any tracking cookies but having to pay a fee (for example, a monthly fee). The German data protection authority (Datenschutzkonferenz – DSK) confirmed in a statement dated March 22, 2023, that such a PUR model may be used lawfully. The DSK states that the consent is lawful if the pay alternative includes services that are equivalent to those services that are provided when the user consents to tracking cookies for a customary fee. Furthermore, the consent requirements in articles 4(11) and 7 of the GDPR must be fulfilled, for example, granular consent for different purposes, transparency, and sufficient information. If the user chooses to use the pay alternative and does not provide any further consent, only strictly necessary cookies may be collected. The statement by the DSK is in line with a March 31, 2023 decision of the Austrian data protection authority, which also held that PUR models may generally be lawful.

### *First Regional Court Munich rules on the design of cookie banners*

The Regional Court Munich I addressed the design of a cookie banner in its November 29, 2022 judgment (docket no. 33 O 14776/19). In the cookie banner that the court reviewed, users had the options in the first layer to either accept the use of cookies by clicking on the "Accept" button or to click on "Settings" to access the second layer. In the second layer, users could make individual settings for 100 third-party providers and could choose between the visually highlighted buttons – "Accept all" and "Save selection," as well as the "Reject all" link displayed in a pale font. The court held that there was a lack of freely given consent because users could not use the website without interacting with the cookie banner: rejecting cookies required a considerable additional effort, while the consent buttons were clearly highlighted in color.

The Regional Court Munich I follows the opinion of some data protection authorities: in addition to an "Accept" button, a rejection option must also be possible without additional effort, that is, with the same number of clicks. The topic of whether a "Reject" button is required in the first layer of a cookie banner is still a hot topic. Organizations should, however, review their cookie banners in light of recent case law and opinions by data protection authorities.

### *Regional Court Cologne decides on many cookie-related issues*

The Regional Court Cologne ruled in a judgment dated January 12, 2023 (docket no. 33 O 376/22) on multiple recurring issues in relation to the use of cookies. First, the court held that consent obtained in the cookie banner was not valid. The cookie banner included an "Accept" button. The "Reject" option was hidden in the text of the cookie banner. The court found that the user was not provided with two equal choices and thus did not have a free choice. Second, the court also found that the EU-U.S. transfer of the cookie data violated article 44 et. seq. of the GDPR. In that case, the controller used standard contractual clauses to justify the transfer but did not present any supplementary measures as required in the EDPB Recommendations 1/2020.

### *German Federal Data Protection Office comments on clean room solutions*

The German Federal Data Protection Office (BfDI) commented on the adtech clean room solution, TrustPiD. TrustPiD is a project of several major mobile operators that is intended to enable pseudonymized, personalized advertising on websites without cookies. Tracking is based on the mobile connection identifier MSISDN and "unique, pseudonymous" network identifiers created by the mobile network operator. The solution is cookie free, but following the BfDI, it is not free from data protection obstacles: the BfDI requests a separate consent banner, clear information, and a joint controller agreement between the publisher website and the network operator, as well as clear and effective fulfillment of data subject rights. Despite these requirements, clean room solutions like TrustPiD can be more data-protection-friendly than current tracking technologies and, perhaps in an adjusted format, might help in avoiding endless cookie banners.

# Greece

### *Law 4961/2022 on Emerging Technologies and Communications*

In anticipation of the relevant EU legislation, Greek Law 4961/2022 establishes a concise legal framework on emerging technologies and communications, including AI, Internet of Things, the provision of postal services through drones, blockchain, smart contracts, and 3D printing. The law provides a set of obligations for product and service providers operating in sectors that are relevant to AI, the Internet of Things, and general provisions on the use of AI and 3D printing. It also regulates transactions involving the use of blockchain and smart contracts. The law affects the operation of both the public and private sectors and is considered a clear step toward the digital transformation of the state and the digitalization of transactions. Additional ministerial decisions are expected to be issued specifying the details of the various obligations provided by the law.

### *Update on the byDefault project*

This project is funded by the Citizens, Equality, Rights and Values Programme and coordinated by the Hellenic Data Protection Authority. The project is being carried out by the University of Piraeus Research Center, the Hellenic Data Protection Authority, and the Greek company ICT Abovo. The byDefault project aims to raise data protection and privacy awareness among children by developing specialized training programs and other educational activities and create an open source of knowledge for privacy and data protection professionals. The first step toward this goal is to create an online platform to facilitate cooperation and the exchange of views between data protection and privacy professionals. In the next few months, a questionnaire will be circulated to ascertain areas of interest among these professionals, and the findings will be processed and discussed later this year during a series of workshops.

### *Data Protection Authority Decision 5/2023*

The Data Protection Authority (DPA) examined a complaint filed by a consumer against a mobile/Internet provider. The consumer filed an application for a mobile/Internet connection with a specific provider. Soon after, the consumer received a package containing product samples, even though he had specifically objected to his personal data being used for promotional purposes. The provider claimed that the samples were sent to all new customers irrespective of their preferences to be contacted for promotional purposes and that this was not considered a promotional activity but rather a supplemental action following the conclusion of a new contract. The consumer was informed about this through a special banner located on the provider's website. The DPA decided that the transmission of the consumer's data to an advertising company and the respective processing of his data, in order to send the samples, was illegal and carried out for promotional purposes, and it was not proved that the consumer had been adequately informed. The DPA imposed a fine of €10,000 on the provider.

# China

### *Administrative measures for Internet advertising*

On February 25, 2023, the State Administration for Market Regulation published a new set of measures, the Administrative Measures for Internet Advertising (the Measures), which came into effect on May 1, 2023. The Measures supersede the previous regulation, the Interim Measures for the Administration of Internet Advertising, which came into force in 2016.

The Measures define the responsibilities imposed on a variety of companies, including advertisers, Internet advertising operators and publishers, Internet information service providers (ISPs), and advertisement endorsers. The Measures prioritize the regulation of the types of advertising that typically receive the most complaints from the public, such as pop-up ads, splash ads, and ads on smart devices. The Measures also amend the rules in place for advertising in key areas, such as soft sell ads, Internet ads containing links, pay-per-click ads, algorithm recommendation-based ads, Internet livestream ads, and advertising that has not yet been reviewed.

The Measures outline the types of Internet advertisements that are prohibited, such as those for tobacco and prescription drugs; those that are subject to censorship, such as medical services, drugs, and medical instruments; and those that are prohibited on certain media formats, such as advertisements that are not allowed on any website intended for use by children. Compared with the previous regulations, the Measures amend the provisions on penalties by extending the scope to include advertising endorsers and Internet ISPs. The Measures also further increase the enforcement powers of market regulation authorities.

# Singapore

### *Regulations for prospecting and marketing of financial products*

The Monetary Authority of Singapore (MAS) proposed additional regulations on April 25, 2023, for the prospecting and marketing of financial products in public spaces and online by financial institutions (FIs).

The MAS regulates digital prospecting and marketing of financial products through Standards of Conduct for Digital Prospecting and Marketing Activities (Digital Guidelines), which set out best practices for FIs, such as ensuring that key information is not omitted because of word or character limits. The boards and senior management of FIs will be responsible for implementing safeguards, such as providing proper training for FI representatives and monitoring advertisers' activities. The MAS also reiterated that existing legislation like the Personal Data Protection Act 2012 still applies to digital prospecting and marketing activities.

The MAS regulates public prospecting and the marketing of financial products via five measures. For example, FIs and their representatives must inform consumers up-front of their intention to market financial products, and they must obtain consent from consumers. Also, prospecting activities must be conducted in proper and conducive settings and in a responsible and professional manner.

The regulations are expected to take effect in 2024, with a tentative transition period of around six to nine months for FIs to comply.

### *Legislation introduced to combat online criminal activities*

The Singapore government introduced a bill for a new Online Criminal Harms Act (OCHA) on May 8, 2023, to deter scams and other malicious online activities. It also passed bills to amend the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) and the Computer Misuse Act 1993 (CMA) on May 9, 2023, to target scams.

The OCHA allows government directions to be issued once there is a reasonable suspicion that online activity is being carried out to commit certain crimes. The lower threshold helps authorities take preemptive action such as the Stop Communication Direction, which requires the party to stop communicating specified online content. The CDSA amendments introduce new offenses, such as negligent and reckless money laundering, while the CMA amendments introduce new offenses, for example, disclosing and dealing in personal credentials that are used to facilitate crime.

The legislation is expected to take effect in late 2023 or early 2024. Advertisers should review their practices to ensure that they can comply with the applicable laws and government directions.

### *Measures introduced to encourage development of responsible AI testing tools*

Following the 2022 launch of AI Verify, a toolkit for companies to test their AI models for compliance with global ethical standards, in June 2023, the IMDA launched the AI Verify Foundation. The not-for-profit foundation brings together open-source community expertise to collaborate and share ideas on testing and governing AI. The founding members of the AI Verify Foundation include IBM, Microsoft, Google, Red Hat, Salesforce, Adobe, Meta, Singapore Airlines, and DBS.

### *Regulator issues directions under new online harms legislation*

The 2022 amendments to the Broadcasting Act 1994 (covered in our previous adtech round-up) have been put to use for the first time by the IMDA. In June 2023, the IMDA required a social media service to remove pages containing child sexual exploitation material. The material had initially surfaced in police investigations and was taken down by the social media service within 24 hours of IMDA's notification.

### *Increasing use of technology in cross-border scams*

Technology is increasingly used in cross-border scams to target a broad range of victims. In June 2023, the Singapore authorities and law enforcement agencies from other countries cooperated to rescue a Chinese national who was kidnapped in Cambodia after falling for a government official impersonation scam. The victim, a student in a Singapore art college, was rescued unharmed, and no ransom was paid.

Law enforcement agencies have warned that scam syndicates are using sophisticated technology to create misleading advertisements, video deepfakes, and audio deepfakes. Deepfakes have been used to create clones of public figures to spread

disinformation and to trick victims into thinking that their family or friends need money urgently. Increasingly realistic deepfakes of family and friends are now duping younger and more-educated victims, compared to scams of the past. Modern-day scams are especially dangerous as they are more effective in manipulating human emotion and encouraging rash behavior.

Because technology is not constrained by physical boundaries, cross-border scams like the example above are increasing and require greater cross-border cooperation. Interpol has issued an Orange Notice, highlighting the serious and imminent threat to public safety, while Singapore law enforcement agencies have collaborated with their overseas counterparts to take down nearly 40 scam syndicates in the past two years. These syndicates include job scam syndicates and phishing scam syndicates.

# United States

### *Federal Trade Commission ramps up enforcement in digital health space*

In a series of recent enforcement actions, the Federal Trade Commission (FTC) has signaled its focus on consumer health data used in the advertising context that is not subject to the federal health privacy law. Specifically, the FTC has leveraged its Health Breach Notification Rule (the Rule) against companies that allegedly share user health data through tracking pixels for marketing and advertising without adequate notice and authorization. The Health Breach Notification Rule regulates, among other things, the disclosure of electronic health data by non-HIPAA-covered entities. Under the Health Breach Notification Rule, non-HIPAA entities are required to provide notice to data subjects and the FTC where there has been a "breach of security" of unsecured "[personal health records] identifiable health information" maintained by the non-HIPAA entity. Failure to do so would constitute unfair or deceptive trade practices in violation of the Federal Trade Commission Act (FTCA). A "breach of security" is the acquisition of unsecured, identifiable health information in a "personal health record" without the data subject's consent. A "personal health record" includes electronic records of identifiable health information that can be drawn from multiple sources and that is managed by or for the data subject.

More than 13 years after the Rule went into effect in 2009, the FTC established that the disclosure of covered health data to third parties via online trackers for targeted advertising purposes without the data subject's consent constitutes a "breach of security" requiring notice. Specifically, it was alleged that GoodRx, a prescription and telemedicine company, used the information it collected about users' medication purchases and other personal information, including email addresses and mobile advertising IDs, to target users with health-related ads on social media. The complaint alleged that because GoodRx did not obtain sufficient consent, such advertising practices constituted a "breach of security" requiring notice that was never provided. Therefore, it was alleged that GoodRx violated the Rule and engaged in deceptive trade practices in violation of the FTCA. The case settled for $1.5 million.

Shortly thereafter, the FTC settled another enforcement related to the use of health-related data for targeted advertising. Specifically, the FTC claimed that BetterHelp, an online therapy company, disclosed health data to third parties for targeted advertising purposes without consent, which was unfair and misleading in violation of the FTCA. The parties settled for $7.8 million.

In addition to this flurry of enforcement activity, in June of 2023, the FTC proposed amendments to the Health Breach Notification Rule to clarify that the Rule applies to online services, including health-related online sites, mobile apps, and other connected devices.

Taken together, non-HIPAA entities operating in the health, wellness, and beauty industries should closely evaluate cookies and other trackers on any online or Internet-connected technologies to determine whether health-related data is being collected and shared with third parties and to ensure that they have provided adequate notice and obtained the necessary affirmative consents before doing so.

### *IAB Multistate Privacy Agreement*

In an attempt to streamline privacy compliance in light of the expanding patchwork of state privacy laws in the United States, the Interactive Advertising Bureau (IAB) released an updated contractual framework for targeted advertising agreements intended to address the handful of state omnibus privacy laws that are or will be effective this year, including the California Privacy Rights Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act. The Multistate Privacy Agreement (MSPA) builds on the Limited Service Provider Agreement (LSPA) that the IAB produced in 2020 and includes provisions meant to address issues such as:

- "Sales" that may occur because of the lack of a contractual agreement between the relevant parties within the digital advertising distribution chain
- Measurement and frequency capping
- Contextual advertising and advertising on a publisher's first-party segments
- Opt-out frameworks for "sales" and regulated behavioral advertising

Rather than a template agreement, the MSPA was intended to supplement commercial contracts or alternatively fill the gap where contractual privacy terms are lacking between relevant parties in the adtech ecosystem, such as in the context of real-

time bidding. The MSPA also provides privacy frameworks for data flows specific to the digital advertising ecosystem, such as for frequency capping.

### *Legislative update*

As more states pass comprehensive privacy laws in the United States (at least 10 have as of the publication of this writing: California, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Texas, Utah, and Virginia), regulators have also provided supplemental regulations. Specifically, the California legislature finalized the long-awaited California Privacy Rights Act (CPRA) regulations, which were set to go into effect on July 1, 2023. However, California has been blocked from enforcing the CPRA regulations until March 2024. Colorado, on the other hand, finalized its regulations, implementing the Colorado Privacy Act (CPA), which went into effect as of July 1, 2023.

## California

The new CPRA regulations prescribe several requirements related to data subject rights mechanisms and in some instances offer alternatives that are arguably more business friendly. For example, certain businesses have the option of posting relatively long links on their websites (e.g., "Do Not Sell or Share My Personal Information" and "Limit the Use and Disclosure of My Personal Information") or opting for a more concise "Alternative Opt-out Link" (e.g., "Your Privacy Choices," plus the designated logo). The CPRA requires businesses to offer consumers the ability to limit the use and disclosure of "sensitive personal information" (which includes precise geolocation data), and the new regulations shed more light on the exceptions to that requirement. Specifically, a business is not required to offer the right for any of the enumerated purposes set forth under section 7027(m) provided that the use or disclosure is reasonably necessary and proportionate for those purposes. Enumerated purposes generally include performing services or providing goods reasonably expected by an average consumer who requested those services or goods, for purposes of preventing or investigating particular security incidents, and for certain short-term transient use, which may include certain contextual advertising shown as part of the consumer's current interaction with the business.

Although enforcement of the regulations has been delayed, the regulations reflect how the statute may be interpreted and enforced, providing insight into what regulators are likely to look for when evaluating compliance.

## Colorado

Unlike California, Colorado requires controllers to obtain consent before processing sensitive personal data. The regulations detail the requirements around obtaining sufficient consent – notably, requiring the mechanisms to be "separate and distinct from other terms and conditions" (CPA Rule 7.04). The regulations also introduce several disclosure requirements related to "Bona Fide Loyalty Programs," a newly defined term that includes a "loyalty, rewards, premium feature, discount, or club card program" genuinely established to provide certain benefits to consumers. Advertisers that offer covered loyalty programs must include a host of prescriptive privacy disclosures to comply with the new regulations.

With similar requirements to those in Colorado and California, Virginia's and Connecticut's privacy laws are also in effect, while Utah's law will go into effect on December 31, 2023.

### *Children's privacy laws*

In 2023, states have pushed for legislation that would protect minors using digital platforms, suggesting it may become increasingly challenging to target ads to individuals under 18.

For example, state legislatures in Arkansas and Utah passed laws designed to restrict the use of social media by minors under 18. The laws require certain social media platforms to verify the age of their users and require parental consent in order for minors to use the platform. The Utah law additionally requires covered platforms to provide parents with access to their child's social media account in certain instances. The Florida legislature passed a law effectively requiring covered social media platforms in certain instances to implement safeguards to protect minors under 18 from "substantial harm or privacy risks."

Another brand of child-focused law is the Age-Appropriate Design Code Act. California passed the first version in the United States last year, and that has spawned several copycat bills in other states, including Oregon. The California law is modeled after the UK's AADC. California's law applies to platforms and online services "likely to be accessed by children." However, these laws define a "child" as anyone under the age of 18, which is broader than the existing federal children's privacy law, the Children's Online Privacy Protection Act (COPPA), which defines a child as anyone under the age of 13, thereby capturing a much greater pool of users.

In addition to legislative activity, regulators have been hyper-focused on the collection and use of children's data, with several aggressive enforcements for violations of COPPA. So far in 2023, the FTC has brought several enforcement actions against companies accused of violating COPPA, including requiring the retention of personal information for only as long as is necessary to achieve the purpose for which it was collected, failing to collect the proper parental consent prior to processing personal information, and using deceptive measures to induce children into opting into lower privacy settings.

Children's privacy is an important area of emphasis for state and federal regulators, and thus it would be prudent to shore up advertising initiatives involving individuals under 18, particularly where personal information from or about minors is processed.

### *ANA Programmatic Media Supply Chain Transparency Study – First Look*

The Association of National Advertisers (ANA) issued the initial results of its Programmatic Media Supply Chain Transparency Study (Study) in June 2023, calling further attention to the programmatic and adtech ecosystem. Given that advertising spending is one of the largest budget items of a company, a key objective of the Study was to help marketers drive business and brand growth by eliminating "wasteful and unproductive spending" in the programmatic supply chain. As with prior studies, the "information asymmetry" in the programmatic space makes it challenging for marketers to understand and obtain information about price, quality (including whether content is brand safe and ads are viewable and fraud free), and audiences needed to make informed decisions about their media buying. Some of the key findings of the Study were:

- Access to data continues to be an issue. Despite years of industry recommendations for advertisers to take a more active role in their media investments and to obtain access to log file and other supply chain data through direct contracts with the supply chain or through their agency agreements, only 21 of the 67 ANA member companies that volunteered to participate in the study were able to get through the legal and other hurdles in order to gain access to their own log file data from their demand-side platforms (DSPs), supply-side platforms (SSPs), and ad verification vendors. Combining access to such information with analysis among the supply chain partners allows advertisers to make better decisions about how they spend their advertising dollars.
- Advertisers prioritize cost over value. The Study also found that advertisers are too focused on driving costs down versus incentivizing value. Agency performance payments are often tied to the savings they generate for the advertiser, which can lead to value being overlooked and lost. Further, because it can be difficult to measure ROI on a campaign, marketers may be hesitant to focus on effectiveness over cost. But not all inventory is created equal. The Study recommends that advertisers balance the desire for low-cost inventory with ad quality (i.e., viewable, fraud free, and brand safe).
- Made for Advertising (MFA) websites are rampant. The Study found that 21 percent of the impressions measured ran on MFA sites. These websites typically use sensational headlines, clickbait, and provocative content to attract visitors and generate ad revenue. They often also have pop-up ads, autoplay videos, and other intrusive ads that may not align with advertiser objectives.
- Programmatic advertising has sustainability impacts. The programmatic ecosystem contains many supply chain participants. The Study found that the average campaign ran on over 44,000 websites. Every impression and ad call for an ad along the supply chain creates carbon emissions. The longer the supply chain, the higher the carbon emissions. Some websites, especially MFA sites, create more carbon emissions than the average site. For instance, MFA sites are 26 percent higher in carbon emissions because they have many ads per page and indiscriminately make ad calls to as many demand sources (like SSPs, DSPs, and ad networks) as they possibly can. The Study urges advertisers and their media-buying partners to focus on sustainability by streamlining the number of websites on which their ads appear by using inclusion lists instead of exclusion lists and to consider supporting options like Ad Net Zero, the advertising industry's drive to reduce the carbon impact of developing, producing, and running advertising.

The Study coincides with the June 2023 release of the updated ANA Master Media Buying Services Agreement template.

**Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.**

Our belief is that by delivering smarter and more creative legal services, we will not only enrich our clients' experiences with us, but also support them in achieving their business goals.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for the speedy resolution of complex disputes, transactions, and regulatory matters.

For further information, please visit reedsmith.com.




ABU DHABI
ASTANA
ATHENS
AUSTIN
BEIJING
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
ORANGE COUNTY
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

**reedsmith.com**