AdTech Round Up

March 2024

ReedSmith

Driving progress
through partnership

Contents

AdTech round-up 2024

As 2024 begins, we reflect on the past few months in the adtech world and look ahead to what this new year will bring. As we publish this round-up, some much needed tying up of loose ends has taken place to finalise some new adtech regulatory requirements such as the EU's Digital Services Act that is now fully in force, the EU Artificial Intelligence Act (AI Act) text that has been finalised and the UK's Online Safety Act, which is gearing up for implementation. In other respects, however, things have not moved on – notably in relation to continued discussion around cookie compliance, a topic we all hoped would have settled by 2024 given advances in technologies and user engagement.

United Kingdom

All eyes on dark patterns

In the past year, we have seen regulators in the UK take a firm, coordinated stance against so-called dark patterns and harmful website designs. In August 2023, a joint effort from the Information Commissioner's Office (ICO) and Competition and Markets Authority (CMA) saw the publication of a position paper: *Harmful Design in Digital Markets: How Online Choice Architecture Practices Can Undermine Consumer Choice and Control Over Personal Information*. Several common advertising practices are covered by the paper, including bundled consent, default settings, biased choices and nudge behaviour. The paper specifically acknowledges the common use of dark patterns as a means to carry out targeting advertising and the subsequent non-consensual processing of personal data within "complex adtech ecosystem supply chains".

While not binding in nature, the paper firmly sets out the expectation of the two regulators when it comes to the use of dark patterns, giving a clear indicator of the direction of travel in the UK for regulation of the practice and demonstrates the joined up approach the regulators are now taking as part of their membership in the UK's Digital Regulation Cooperation Forum. However, no specific dark patterns legislation is on the books in the UK with enforcement primarily taking place (indirectly) through existing regimes such as data protection and consumer law.

For our comparison of UK dark patterns requirements around advertising and other topics with those in the EU, United States and Singapore, see here.

Doubling down on cookie consents

In November 2023, just in the run-up to the Christmas rush, the ICO launched a campaign targeting the UK's top 100 websites' (lack of) "Reject All" buttons on the first layer of their cookie banners, stating that they were in violation of UK data protection laws and cautioning that enforcement measures would be inevitable if remedial action was not taken. The letters sent to the Data Protection Officers, published in full form by the ICO, made clear that compliance (as well as the ICO's auditing resources) goes well beyond the design of a cookie banner, extending to determining with certainty the appropriate categorisation of non-essential advertising cookies and ensuring that these do not drop before valid consent has been collected. Many global organisations, already subject to strict cookie banner design rules issued by EU regulators, had expected this day to arrive, but it did catch others off guard, not least since, to date, the UK had been viewed as being more pragmatic on enforcement in this area.

On 31 January 2024, the ICO published an update regarding its campaign, emphasising the apparent positive response to the exercise and setting expectations for the next steps – the ICO confirmed that hundreds more of the UK's top websites were in the firing line and not safe from enforcement action, pushing the message that businesses should take proactive measures now, rather than waiting for the letters from the ICO.

From the outset, the ICO claimed it was going to name and shame those organisations it contacted but failed to take appropriate steps to address non-compliance – it's unclear as of yet whether this was simply a scare tactic or if the list is actually on the way but, in any event, whilst appearing at IAPP Data Protection Intensive: UK 2024, the Information Commissioner reiterated the ICO's focus on third-party advertising cookies and prioritising their fair use. The Commissioner also announced that the ICO is aiming to create an automated tool to assess cookie banners and alert them when non-compliant.

It's finally here: the Online Safety Act

Shortly after our last round-up, the Online Safety Bill received royal assent and became the Online Safety Act (OSA). Its provisions will become enforceable in iterative stages, with Ofcom already publishing the first round of consultations, draft codes and guidance notes to assist in-scope businesses with compliance efforts. The OSA requires that certain services (Category 1 and 2A) adhere to the results on fraudulent advertising, including promptly removing them and implementing measures to prevent users from encountering them in the first place. Ofcom is planning to release a draft Code of Practice on fraudulent advertising in early 2025, with the final code anticipated to be published by the end of the same year.

For a comparison of the advertising provisions under the OSA with the EU's Digital Services Act, see here.

The slow progress of the Data Protection and Digital Information Bill

Since our previous round-up, we have seen very little movement on the Data Protection and Digital Information (No. 2) Bill. As a reminder, the Bill aims to introduce certain changes to the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018, as well as updating the Privacy and Electronic Communications (EC Directive) Regulations 2003 by relaxing cookie banner requirements for certain low-risk cookies. On 7 February 2024, the Bill received a carry-over motion to continue its progress into the next parliamentary year. As such, we do not expect significant advancements in the Bill until at least the end of the year.

European Union

EDPB: GDPR does not oblige controllers to respect "Do Not Track" browser function

On 15 December 2023, the European Data Protection Board (EDPB) responded to a letter from Mr Moritz Körner, a member of the European Parliament, regarding the "Do Not Track" browser function. The opinion of the EDPB was highly anticipated, especially following the recent decision by the Regional Court Berlin (also discussed in the section below on Germany) regarding the "Do Not Track" function.

The EDPB notes: "While Article 21(5) GDPR may, therefore, be relevant to certain tracking activities, the EDPB notes that this provision should not be read as imposing a general requirement that website operator respect a user's Do Not Track settings."

Consequently, the EDPB does not share the same view as the Regional Court of Berlin and organisations generally do not have to respect a user's "Do Not Track" settings.

The EDPB stresses that even though a user sets its "Do Not Track" browser function to permit tracking, website operators must still actively obtain consent from their users.

Supervisory authorities seek the opinion of the EDPB on "pay or okay" advertising model

The Dutch, Norwegian and Hamburg (Germany) supervisory authority have urged the EDPB to formally address the "pay or okay" advertising model, where users either have to allow targeted advertising or pay to opt out. With new digital legislation in the EU adding to existing privacy rules, a flurry of recent decisions calling into question consent requirements and several EU regulators themselves taking opposing views on the matter, it is becoming increasingly unclear whether such models are in line with law.

The EDPB has eight weeks to adopt an opinion and can request an extension of an additional six weeks if it considers the complexity of the topic requires further consideration. Until then, we await a harmonised approach on a European level.

The European Commission's "cookie pledge" and phasing out cookies

The European Commission's consumer protection department, led by Commissioner Didier Reynders, is coordinating a "cookie pledge" initiative to phase out cookies in digital advertising. Launched at the European Consumer Summit, the initiative includes principles to simplify user consent, offer fewer privacy-intrusive advertising alternatives and require services to record user consent preferences.

The consolidated version of the "draft pledging principles" can be found here. In December 2023, the EDPB replied to the Commission's initiative, welcoming the project and providing detailed feedback on the principles.

AI regulation race: getting close to the finish line

On 8 December 2023, the European Parliament, Commission and Council reached a consensus on the AI Act. It is expected that the European Parliament will formally adopt the AI Act's text at a plenary session on 13 March 2024. The AI Act will enter into force 20 days following its publication in the Official Journal, with the majority of its provisions becoming applicable 24 months thereafter. As mentioned in our previous round-up, the AI Act is unlikely to have a material effect on the world of adtech; however, organisations deploying AI models will need to comply with provisions around transparency and record keeping.

Digital Services Act – time's up!

On 17 February 2024, the Digital Services Act began applying to all online platforms in the EU. We have analysed the various aspects of the new legislation here; however, the most important provisions relating to adtech include categorising advertising content as potentially illegal, implementing measures for transparent online advertising by disclosing specific information in ads and limiting the use of sensitive personal data for targeted advertising.

IAB update

In our January 2023 round-up, we reported that the Belgian Data Protection Authority (APD) fined the Interactive Advertising Bureau (IAB) Europe €250,000 for failures by its Transparency and Consent Framework (TCF) to comply with the GDPR and was ordered to present an action plan setting out how it would address the issues identified by the APD. IAB appealed the decision, with some grounds of appeal being referred to the European Court of Justice (ECJ). The decision was significant because of its implications for a wide range of entities, from websites and publishers to adtech vendors and the IAB itself, and also for users who interact with consent management platforms.

Most recently, on 7 September 2023, IAB announced that the Belgian Market Court had published an interim ruling and suspended the APD's validation decision, pending the ECJ's ruling. Initially, IAB had six months to implement the action plan approved by the APD, which would mean the plan would have to be fully executed before ECJ gives its preliminary decision. The ECJ judgment is due to be published on 7 March 2024.

As a result of the litigation, IAB Europe updated the TCF framework to bolster privacy protections. This includes removing legitimate interest as legal basis for advertising and content personalisation, enhancing transparency in information provided to end-users, simplifying users' consent withdrawal process, and displaying number of vendors who are seeking the legal basis. Companies had until 20 November 2023 to transition to the updated version of the TCF. IAB has announced that they will conduct checks so companies should brace themselves for enhanced scrutiny.

Germany

Regional Court Munich I rules on the termination button

The Regional Court Munich I addressed the rules on the termination button in its 10 October 2023 judgment (docket no. O 15098/22).

The decision is based on section 312k of the German Civil Code, effective from 1 July 2022, which mandates that organisations must allow customers to terminate online contracts through a cancellation button. The termination button must be permanently available and easily accessible. The court found that the practice of requiring email and password login to access the termination button is not in compliance with the law.

The decision is highly criticised as being impractical and preventing companies from properly authorising their customers.

Higher Regional Court Hamburg: ad blockers do not infringe on copyright laws

The publishing industry has been fighting ad blockers for almost a decade. The industry experienced its first setback in 2018 when the Federal Court of Justice ruled that the offering of ad blockers is not unfair competition as ad blockers do not constitute targeted obstruction of competitors, nor do they significantly impair the decision-making freedom of market participants.

In November 2023, the industry experienced its second setback with the judgment of the Higher Regional Court Hamburg (docket no. U 20/22). The court determined that ad blockers do not infringe on copyright laws as there is no unauthorised reproduction and/or modification of copyrighted computer programs within the meaning of section 69a, 69c no. 1 and 2 of the Act on Copyright and Related Rights.

Organisations cannot claim to ignore the “Do Not Track” browser function

The Regional Court Berlin declared that the claim of an organisation to ignore the “Do Not Track” (DNT) browser function and not regard it as an effective objection to data processing is misleading and constitutes an unfair commercial practice under the Act against Unfair Competition.

The court rules that the claim is misleading. It asserts a clear legal position, which must be understood as “use of a DNT signal is legally irrelevant”. However, the DNT signal can be – in the view of the court – indeed a valid objection to data processing, as outlined in Art. 21(5) GDPR. The decision focuses on the “misleading” aspect and it is very questionable whether in its generality it says “DNT must be respected”.

France

Publication by the CNIL of a first series of guidelines for the use of artificial intelligence

While reaffirming its commitment to supporting innovative AI actors, the National Commission on Informatics and Liberty (CNIL) published on 11 October 2023 a first series of guidelines on the creation of learning databases for AI systems. These guidelines aim at supporting actors in the development phase of their AI systems to comply with regulations on the protection of personal data. The CNIL has focused on AI research and development and their compatibility with the GDPR requirements, in particular the principles of purpose limitation, data minimisation and data retention.

The CNIL seems to be showing flexibility regarding the purpose of such AI research and development as it admits that an operator is unable to define all its future applications at the algorithm training stage. Nonetheless, the type of system and the main possible functions have to be clearly defined.

The CNIL will publish the final version on its website in 2024 and have been submitted to a public call for contributions meanwhile.

Update of the certification standards for health data hosting providers and their subcontractors

As part of its commitment to an effective protection of personal health data in France, the French Digital Health Agency (ANS) has updated the certification requirements for hosting providers or their subcontractors (HDS certification). The upcoming modifications were incorporated into a draft decree, which was notified to the European Commission in December 2023.

To be certified under the new requirements, data hosting providers or their subcontractors will be required to store personal health data exclusively within the European Economic Area (EEA) and may only allow simple remote access from third countries. Following the regime for data transfers to third countries, this remote access is conditional on the existence of an adequacy decision from the European Commission (art. 45 GDPR) or appropriate safeguards (art. 46 GDPR). The hosting providers shall publish and update a mapping of data transfers to a country that is not part of the EEA, even in the event of remote access, and a description of the risks.

These new requirements, aimed at reinforcing data sovereignty, shall condition HDS compliance certificate applications and renewal applications submitted to certifying authorities from the second half of 2024 onwards.

Signing by the CNIL and the French Competition Authority of a joint statement entitled "Data protection and competition: a shared ambition"

On 12 December 2023, the CNIL and the French Competition Authority jointly declared their common ambition to deepen their cooperation and review how data protection and competition are considered in their actions. They aim to ensure that the level of data protection is seen as a competitive parameter: the use of personal data can affect the competition between actors, and, in the same way, the market position of actors can reduce their level of data protection.

In order to warrant effective competition, both authorities want to ensure that dominant actors do not abuse their positions by reducing the level of data protection and that the instruments implemented by the actors for compliance with the GDPR take competitive risks into account. Despite the distinct objectives of each of these authorities, their joint action aims to ensure effective protection of the consumers while providing actors with greater predictability and enhanced legal certainty.

This cooperation, which is materialised by a joint recourse to consultative procedures between authorities, is a feature that has recently been introduced in French law. However, this joint statement enhances the cooperation between these two authorities by providing for the possibility of informal consultation and a commitment to confer.

French Data Protection Authority recommendations on the use of APIs

The CNIL has issued recommendations on data sharing, especially regarding the use of application programming interfaces (API). These increasingly used APIs facilitate data sharing between different organisations, whether in the public or private sector.

In these recommendations, issued following a public consultation in autumn 2022, the CNIL aims to promote the secure use of APIs where it is beneficial according to a range of criteria (e.g., the data are frequently updated and reusers can access it regularly). The CNIL recommends best practices in the use of APIs and provides a list of risk factors that the actors should take into account, such as the level of authentication techniques' security used or the categories of data accessible via the API. The authority identifies three main actors: data holders, API managers and data reusers.

According to the CNIL, this recommendation is not binding, except where it refers to the requirements arising from the GDPR.

Greece

Hellenic Data Protection Authority decision no. 24/2023

The Data Protection Authority (DPA) examined a complaint regarding marketing emails being sent without the complainant having provided their consent. In its decision, the DPA analysed the exception of the ePrivacy Directive, providing that where a natural or legal person obtains from its customers their electronic contact details for electronic mail in the context of a product or service sale, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details at the time of their collection and on the occasion of each message in case the customer has not refused such use initially. In the subject case, the DPA ruled that the exchange of business cards alone does not prove that the individual provided consent to receive marketing communications. The defendant was not able to prove the source of the personal data processed for marketing purposes in accordance with the principle of accountability and the DPA issued a warning against the subject defendant for breach of art. 58 par. 2b of GDPR and art. 13 par.1 and 4 of law 3471/2006 (implementing the ePrivacy Directive).

DPA assistance systems

Within the scope of the Restructuring Programme for the Public Sector 2014–2020, the DPA recently launched two new systems through the DPA platform to assist individuals and organisations in exercising their data protection rights, notifying the DPA of a data breach and including a micro-site specifically for children and teenagers to familiarise them with their data privacy rights and the applicable legal framework.

Draft law on the establishment of the National Cybersecurity Authority

A draft law is under consideration in the Greek Parliament, providing for the establishment of the National Cybersecurity Authority (NCA). The NCA will be responsible for the coordination and implementation of the National Cybersecurity Strategy and the effective prevention and handling of cybersecurity attacks in Greece. The draft law contains organisational provisions on the establishment and structure of the new body, given the increasing need for enhanced cybersecurity. Once Directive 2022/2555 is implemented in October 2024, it is estimated that the number of bodies supervised by the competent authority shall increase from 70 to 2,000 from various sectors, including the public sector, express delivery services, and production and distribution of chemical products, for example, urging a new flexible regulatory authority to address the increased risks.

United States

Federal Trade Commission issues proposed revisions to Children's Online Privacy Protection Act

2024 will certainly be another big year of regulatory focus in the United States and beyond for children's privacy. At the end of last year, the Federal Trade Commission (FTC) issued proposed revisions to the Children's Online Privacy Protection Rule (COPPA Rule), focused on further regulating the disclosure of children's personal information to third parties and the monetisation of children's data. The proposed changes would require targeted advertising to be turned off by default and separate verifiable consent to disclose information to third parties – including third-party advertisers – unless the disclosure is integral to the nature of the site or service. This is a stark contrast to the current COPPA Rule, which allows the collection of information from persistent identifiers without first obtaining verifiable parental consent when the operator does not collect any other personal information and uses the persistent identifier solely to provide "support for the internal operations of the website or online service". Under the proposed revisions, operators that rely on this exception would be required to provide a notice specifying the internal operations for which a persistent identifier has been collected and how the operator will ensure the persistent identifier is not used to contact individuals, including through targeted advertising. The proposed revisions also restrict edtech providers' use of children's personal information, stating that the schools and school districts can only authorise edtech providers to collect, use and process children's personal information for school-authorised purposes and not for any commercial purposes. The proposed changes carry forward principles found in several key FTC enforcements in connection with the processing of children's personal information, particularly through persistent identifiers and for targeted advertising.

California Attorney General continues CCPA enforcement sweeps: streaming apps and devices

In January this year, Attorney General (AG) Bonta announced a new enforcement focused on the compliance of streaming apps and devices with the California Consumer Privacy Act's (CCPA) requirements allowing consumers to opt out of the sale of their personal information and the sharing of their personal information for cross-contextual advertising. The AG's announcement reiterated the expectation that businesses selling personal information or sharing personal information for targeted advertising should ensure they allow consumers to opt out of such sale/sharing in a simple manner with minimal steps. With respect to steaming services specifically, the announcement specified that (1) consumers should be able to find and enable the "Do Not Sell My Personal Information" in the device's settings menu, (2) the opt-out request should be honoured across different devices, if enabled, when the consumer is logged into their account, and (3) the privacy policy disclosing the consumer's CCPA rights should be easily accessible from within the device. This enforcement sweep follows prior enforcements focused on "do not sell" and "do not share" compliance across various industries, including mobile apps in the retail, travel and food service industries (January, 2023).

California Delete Act: key changes for data brokers

California's Delete Act went into effect 1 January 2024. The Delete Act amends California's current data broker law, adding further requirements for data brokers. Data brokers are defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Definitions of business, consumer and sell are all incorporated from the CCPA. The new law may, therefore, apply to several entities in the adtech ecosystem.

In addition to registering annually in the data broker registry, disclosing privacy practices and explaining how consumers can exercise rights, the amended law will require data brokers to disclose whether they collect information on minors; precise geolocation information or information on reproductive health care; and whether they are subject to certain federal laws governing personal information. Data brokers will also be required to compile and disclose metrics on (1) the number of CCPA data subject requests and Delete Act deletion requests they have received and complied with (in whole or in part), (2) the median and mean of the number of days it took to respond to requests, and (3) the number of requests the data broker denied (in whole or in part) and the justification for denial.

By 1 January 2026, the California Privacy Protection Agency (CPPA) is directed to establish an accessible deletion mechanism that will enable consumers to direct all data brokers to delete their personal information in a single request. Once a consumer has requested that their data be deleted, data brokers will be prohibited from selling or sharing such information, unless the consumer requests otherwise. And, starting 1 January 2028, data brokers must undergo a third-party audit to assess compliance with the

Delete Act, including submitting the report to the CPPA. Other states with data broker laws include Vermont, Oregon, Texas and Nevada.

California CPPA revises draft regulations on automated decision-making technologies and privacy risk assessments

In accordance with authority granted under the CCPA, the CPPA further revised draft regulations concerning automated decision-making technology as well as privacy risk assessments. The regulations propose to govern any system, software or process – including that derived from machine-learning, statistics or other data-processing or artificial intelligence – that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decision-making, including profiling. The CPPA draft regulations could require companies employing automated decision-making technology to provide a pre-notice about the business's use of automated decision-making technology and consumers' rights to opt out of and access information about the business's use of automated decision-making technology. Profiling for behavioural advertising purposes and processing consumer information to train automated decision-making technology were both flagged in the draft as "for board discussion". The draft regulations on privacy risk assessments would require businesses to conduct risk assessments before selling or sharing personal information, as well as before using automated decision-making technology for behavioural advertising.

Location data under scrutiny

The sale of consumer precise geolocation data has come under intense scrutiny at both a federal and state level. The FTC recently settled allegations against X-Mode Social (and its successor company Outlogic) that the company sold raw location data that was not anonymised and could identify what locations a consumer had visited. The information was sold to various types of companies for their own purposes, including advertising and analytics. However, X-Mode sold this information without disclosing to consumers how the information would be used or shared, without obtaining consumers' consent and without limiting how their downstream customers used the sensitive information. The settlement required X-Mode to delete or destroy previously collected location data and prohibits the company from selling sensitive location data going forward. It requires the company to put in additional technical safeguards around sensitive location data, implement processes to allow consumers to exercise choice in how their data is collected, used and shared, and allow consumers to delete their data. This represents just one of several FTC actions concerning the sale of precise geolocation data.

Pixel litigation continues

One of the highest areas of activity in privacy litigation involves the use and collection of personal data through website pixels. Plaintiffs' lawyers are filing class actions under a number of state and federal laws in relation to companies' use of pixels, including the Video Privacy Protection Act (VPPA), Computer Fraud and Abuse Act, Federal Wiretap Act and state wiretap laws, and the Driver's Privacy Protection Act. In general, such class actions allege that the company is disclosing its website visitors' personally identifiable information (PII) to pixel providers via the provider's tracking pixel without the visitor's consent, violating the applicable law.

Plaintiffs have filed claims alleging that businesses' use of third-party web tracking technologies that (1) track conversations consumers have with chatbots or (2) monitor the consumer's activity on the business' website violate these wiretap laws by disclosing their PII to third-party pixel providers without adequate consent. Plaintiffs have seen mixed results in connection with these cases and the results have largely depended upon the specific facts of that case and the court in which the case was brought.

Plaintiffs have also filed lawsuits under the VPPA claiming that websites that include video content violate the VPPA when they use third-party web-tracking technologies on pages with videos. Plaintiffs allege the websites are engaging in the unauthorised disclosure of the plaintiffs' video viewing history to the web-tracking technology providers. Notably, courts have generally held that firms whose primary business does not involve video content are not subject to the VPPA because they are not "video tape service providers". This provides potential defences to general use sites that may have videos on their site but whose primary business is not video content related. There have also been several other defences that have been successful for defendants against these claims. That said, lawsuits continue to be filed and settled, so it is important to assess the potential risk of a complaint and implement risk mitigating strategies.

Update on state laws

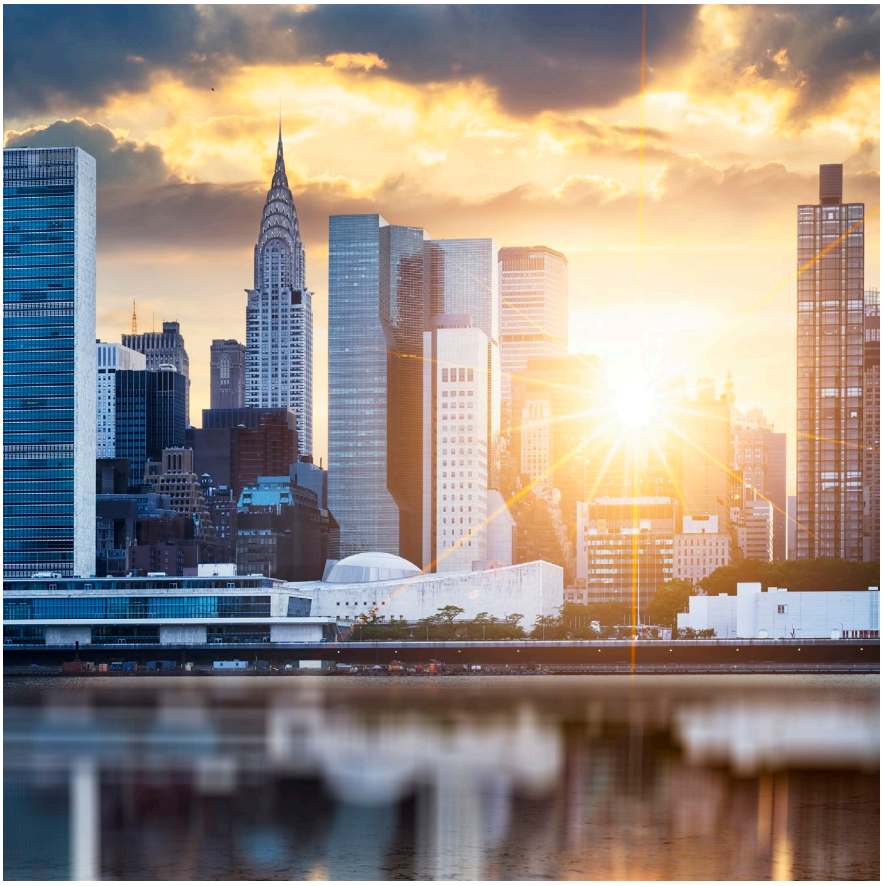
The Utah Consumer Privacy Act, which largely mirrors several existing state privacy laws, went into effect on 31 December 2023.

Three other comprehensive privacy laws will be implemented in 2024; namely, Oregon (1 July 2024), Texas (1 July 2024) and Montana (1 October 2024). These new laws, while largely similar to existing consumer privacy laws, do have certain notable differences. Like most state consumer privacy laws, Oregon, Texas and Montana require that businesses conduct data protection assessments if the business (a) uses personal data for purposes such as targeted advertising and profiling, (b) handles sensitive personal data, or (c) sells personal data. Most state consumer privacy laws require businesses to reveal in their privacy policy the types of third parties to which they disclose personal data. However, Oregon's law requires businesses to include in their privacy policy how the third parties will process the personal data, which is not required in other states. Oregon also provides the consumer with the right to request a specific list of third parties to whom the business has disclosed personal information (the business can provide either a specific list of third parties to whom they have disclosed the consumer's personal data or generally that the business has disclosed any personal data to). Texas' law requires businesses that engage in the sale of sensitive personal data to include a specific notice in their privacy policy provided by the statute. It is the only state that provides specific language to be included in privacy policies in its consumer privacy law.

New Jersey and New Hampshire recently passed comprehensive privacy laws that will be effective from January 2025, bringing the total number of state comprehensive privacy laws to 14, along with Florida, which has limited applicability. These two new laws largely resemble other states' laws.

IAB MSPA certification

IAB Privacy established a voluntary accountability programme through which signatories to the Multi-State Privacy Agreement (MSPA) can demonstrate compliance with the MSPA to earn a "MSPA Certified" seal. Certification requires the MSPA signatory to submit to a compliance assessment that will be conducted by an authorised assessor. The Network Advertising Initiative (NAI) is the first authorised assessor under the accountability programme. The assessment evaluates (1) how end users are provided with transparency and choice mechanisms consistent with MSPA framework requirements, (2) how personal information processed through MSPA-based transactions is limited to MSPA signatories and certified partners only, (3) how the company processes personal information consistent with the MSPA framework's applicable use limitations and (4) how an applicant has implemented technology that processes Global Privacy Platform (GPP) signals in a way that complies with MSPA framework requirements and the integrity of GPP signals processed and shared through transactions covered in the MSPA. The programme is only open to adtech companies that have executed the MSPA.



China

Legislations in the advertising industry

Following the enactment of the Administrative Measures for Internet Advertising (the Measures) in February 2023, China has experienced a rapid surge of internet advertising, with multiple new regulations issued or in the pipeline.

As provided by the Measures, it is imperative that internet advertisements are easily distinguishable by consumers to prevent confusion with non-advertising content. In order to implement such regulatory requirements effectively, China also introduced the Draft Guidelines on the Enforcement of Identifiability of Internet Advertisements (Draft Guidelines) on 28 August 2023, for public comments.

The Draft Guidelines clarify that the identifiability of internet advertisements can be augmented through text annotations and voice prompts that should clearly indicate "advertisement" (in Chinese) and are prohibited from using substitutions such as "sponsorship", "promotion", "recommendation" and "AD". The Draft Guidelines also establish rules for assessing compliance of live streaming and other internet advertisement identifiability requirements.

At the municipal level, Beijing and Shanghai have released specific guidelines and regulations on advertisements. For example, the Administration of Market Regulation in Beijing issued draft industry-specific guidelines on advertisements for financial investment, wealth management and real estate in November 2023, inviting public comments. These draft guidelines, once finalised, will apply to advertisements in any form, including internet advertisements, in the aforementioned industries. On 29 December 2023, Shanghai issued the Measures on the Promotion and Management of Advertisements for Public Service, effective as of 1 January 2024. The said measures also cover internet advertisements for public services, subject to supervision by the local Cyberspace Administration of China.

Data protection in the advertising industry

To craft precise marketing strategies and aim for accurate delivery of advertisements to the intended audience, internet advertisement publishers must deploy technical measures such as profiling and behavioural targeting. However, these methods inevitably involve the collection and processing of personal information from consumers.

China's data laws have been developing at a fast pace and there is an increasing emphasis on enforcing data privacy laws and regulations. Compliance with the People's Republic of China (PRC) Personal Information Protection Law (PIPL) and other data protection and cybersecurity regulations is crucial when collecting, using and processing consumer data. For instance, businesses must follow the related legal requirements under the PIPL and other applicable regulations in terms of securing the required consent from consumers, publishing the appropriate privacy policies and conducting impact assessment when collecting sensitive information (e.g., facial recognition or minors' data). It is important to strike a proper balance between precision of advertisement delivery and protection of the data privacy rights of targeted consumers.

AI regulatory requirements for the advertising industry

Companies are increasingly leveraging AI technology in the advertising industry. China is leading the way in drafting AI regulations and has put compliance requirements in place in terms of using algorithms, facial recognition, deep synthesis and generative AI technologies in the provision of goods and services. These legal requirements will have significant impacts on advertising businesses. As a significant milestone in the AI industry, China released the Interim Measures for Administration of Generative AI Services (Generative AI Measures) on 10 July 2023, becoming one of the first countries in the world to regulate generative AI technology. The Generative AI Measures apply to generative AI services offered to the public in China. According to the Generative AI Measures, companies are required to comply with the following legal requirements:

- Data privacy

  Generative AI service providers are responsible for the processing of pre-training data and optimised data. In particular, service providers must ensure that the data and basic models used come from lawful sources, obtain consent from individuals if personal information is involved, take effective measures to improve the quality of training data by ensuring greater authenticity, accuracy, objectivity and diversity, and comply with PRC data laws and regulations.

- Content screening

  Generative AI service providers must act as the producers of network information content, ensuring that the generated content complies with the relevant laws and regulations. The Generative AI Measures also require generative AI service providers to enter into a service contract with users, setting out the obligations and rights of each party.

- Security assessment

  Generative AI services that enable the public to express opinions or engage socially, such as microblogs, chat rooms, communication groups, social media accounts, short videos, online streaming, information sharing and mini-programs, are subject to security assessment and their algorithms must be filed with the regulator. Additionally, special administrative licences may be required on a case-by-case basis.

Recent law enforcement case on non-competition compliance

In 2023, a significant non-competition case involving the unauthorised copying of content was heard by a court in Beijing. A company used web crawler technologies to copy short videos and comments from a leading short video operator without authorisation, aiming to boost its traffic and advertising revenue. The court held that such actions violated the principles of good faith and business ethics, constituting unfair competition. The court granted an injunction and ordered the infringing party to compensate the infringed company for an economic loss of RMB 5 million (approximately US$71 million). This case garnered widespread attention in the advertising industry, emphasising the importance of compliance with competition requirements for advertising publishers and platforms.

United Arab Emirates (UAE)

New federal media law

In October 2023, after over 40 years on the statute books, Federal Law No. 15/1980 on Press and Publication (Press and Publications Law) was repealed and replaced with Federal Decree-Law No. 55/2023 On the Regulation of Media (New Media Law). The New Media Law came into force on 1 December 2023.

As is common in the UAE, the New Media Law is subject to a set of implementing regulations, which are due to be issued by the end of March 2024, six months from the publication of the New Media Law. Much of the detail and context will be set out under those implementing regulations.

The New Media Law imposes specific obligations on those performing "Electronic and Digital Media" activities (defined as "All platforms that make the media and advertisement content available to the public, through electronic and digital means") and appears to affirm the long understood position that platform operators can be held responsible for the content published on their platforms, including digital advertisements (which must meet the strict content requirements set out in the New Media Law, and must have a "clear and explicit note" that advertising content is such). As a result, publishers in the online advertising ecosystem will likely wish to ensure that: (a) they have processes in place to minimise the possibility of advertisements being served to UAE-based users that do not comply with relevant content restrictions; (b) from a contractual perspective, responsibility (and associated liability) for ensuring that the content of advertisements complies with the UAE media laws and norms rests with advertisers; and (c) they have the contractual right and the technical ability to suspend or remove infringing advertisements.

Trading by modern technological means

Federal Decree-Law No. 14/2023 On Trading by Modern Technological Means (TMTM Law), issued on 4 September 2023, represents the first step towards a more substantive set of requirements specifically applicable to those who engage in the broadly defined "Trading by Modern Technological Means" (i.e., e-commerce). The definition captures trading on websites, platforms, mobile applications, social media, virtual reality connected platforms and blockchain based platforms. The TMTM Law provides a framework covering a broad range of issues, with further detail to be provided by the associated Implementing Regulations (not published at the time of writing). Notably, in the context of online advertising:

1. Those engaged in trading by modern technological means must "[m]eet the conditions and requirements approved by the Competent Authorities regarding the advertising and marketing campaigns and the exchange of consumer data in this regard".

2. Consumers are afforded a right to "choose whether to receive advertising and marketing campaigns or not via phone calls, emails, or social media platforms".

3. There are various broadly worded requirements in connection with the use of consumer data, including an obligation to comply with "standards and requirements pertaining to the protection and security of consumer information and data and refraining from sharing them or making them available except with the consumer's consent".

While the requirements set out above are reasonably high level, further specific guidance may be issued shortly on the use of consumer data in the context of online advertising, either in the Implementing Regulations to the TMTM Law and/or the long-awaited executive regulations to Federal Decree-Law No. 45/2021 on the Protection of Personal Data, which were expected to be published over a year ago but remain outstanding.

DIFC Data Protection Regulations updated

The updated Dubai International Financial Centre (DIFC) Data Protection Regulations (Regulations), issued in September 2023, contain specific requirements with respect to the processing of personal data in the context of behavioural advertising (which includes: (i) direct marketing; (ii) the use of cookies for personalisation, analytics or advertising profile development; or (iii) pixel tracking, in-app tracking capabilities or cross-app tracking and information exchange for targeted marketing). Notably, the Regulations require that privacy preferences must be set by default such that no more than the minimum personal data necessary to deliver or receive the relevant product or services are obtained or collected. The Regulations also provide that the means of selecting privacy preferences available to a data subject on first use of a platform or application enabling "Digital Communications and Services" (including behavioural advertising functionalities) must include: (a) provision

of clear, colour-neutral selection boxes or buttons that neither promote nor discourage any particular setting selections; (b) plain language text explaining the preference settings, so that the data subject may change them and know how to change them; and (c) an easily accessible means, such as a preferences link or dashboard, to further alter privacy preferences upon additional use of the platform or application. Those operating in the DIFC will need to conduct a careful assessment of their existing processes to ensure that they are operating in line with the new, specific requirements.

Singapore

Model framework and advisory guidelines proposed for AI

The Singapore Infocomm Media Development Authority (IMDA) and the AI Verify Foundation have proposed a draft Model AI Governance Framework for Generative AI (Model Framework). The Model Framework is open for public consultation until March 2024 and will be finalised later in 2024. It expands the previous AI Model Governance Framework, last updated in 2020, to include generative AI and now accounts for the unique risks and transformative potential of generative AI.

The Model Framework sets out nine dimensions to facilitate a trusted ecosystem for generative AI. The nine dimensions are accountability, data, trusted development and deployment, incident reporting, testing and assurance, security, content provenance, safety and alignment research and development, as well as AI for public good. The framework aims to contribute towards international discussion and consensus in AI governance.

The Personal Data Protection Commission (PDPC) has conducted a public consultation for the proposed Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems. The guidelines clarify how the Singapore Personal Data Protection Act 2012 (PDPA) applies to the collection and use of personal data to develop and deploy AI systems that embed machine learning models to make decisions, recommendations or predictions.

The guidelines are not legally binding but are likely to be referenced when the PDPC investigates alleged breaches of the PDPA relating to the use of AI systems. The guidelines illustrate how existing exceptions and obligations in the PDPA apply to the use of machine-learning AI systems and provide best practices regarding procurement of AI systems in a business-to-business context.

New initiatives to combat scams

The Monetary Authority of Singapore (MAS) and the IMDA have conducted a public consultation on a proposed Shared Responsibility Framework for Phishing Scams. This proposed framework is in response to the increasing prevalence of phishing scams and requires financial institutions (FIs) and telecommunication companies (telcos) to compensate affected scam victims if these entities breach their duties to mitigate phishing scams.

The proposed framework sets out discrete and well-defined duties for FIs and telcos to encourage the adoption of concrete anti-scam measures. However, scam victims will not receive compensation if they do not exercise vigilance despite the measures taken by FIs and telcos. Individuals should also note that the framework does not cover malware scams, since there are no standardised measures that FIs and telcos can adopt similar to phishing scams.

The MAS has conducted a public consultation on proposed enhancements to the E-Payments User Protection Guidelines. The MAS is proposing to update the guidelines because the original guidelines were in place before the rise in scams and the development of the proposed shared responsibility framework above.

The updates to the guidelines take a two-pronged approach. First, the standards of anti-scam controls in the financial sector will be raised to align with major retail banks. Second, the responsibility of consumers to be vigilant against scams will be reinforced. The updated guidelines and the proposed shared responsibility framework will complement each other when they take effect.

In January 2024, the IMDA announced that it has worked with Singapore telcos to allow subscribers to opt in to block incoming calls from international numbers on their mobile phones. This supplements previously introduced measures to protect the public from scams, such as the SMS Sender ID Registry and marking of calls with a “+65” prefix to warn people about overseas calls masquerading as local calls. The IMDA is planning to introduce similar blocking options for SMS messages from international numbers later in 2024.

Also in January 2024, the Ministry for Communications and Information announced the introduction of a “Safe App Standard” for mobile app safety and a new Centre for Advanced Technologies in Online Safety. The standard is published by the Cyber Security Agency of Singapore and developers of apps that perform high-risk transactions are encouraged to adopt the standard for authentication, authorisation, data storage and anti-tampering.

The Centre for Advanced Technologies in Online Safety will be launched officially in the first half of 2024. It will focus on building and customising tools to detect harmful content such as deepfakes, develop potential interventions to reduce internet users’ susceptibility to harmful online content and test “Trust by Design” technologies such as watermarking and content authentication.

Preventing greenwashing in advertisements

The Advertising Standards Authority of Singapore (ASAS) has found some claims made in a PRISM+ advertisement for air conditioners “not acceptable”. This is ASAS’ first time finding that an advertisement reported for greenwashing breached the Singapore Code of Advertising Practice (Code). ASAS informed PRISM+ that the advertisement breached the Code, in particular the fifth general principle that advertisements should not mislead or misrepresent matters. In response, PRISM+ removed the advertisement from social media.

The Competition and Consumer Commission of Singapore is aware of the rising trend of greenwashing on e-commerce websites in Singapore. In November 2023, before the advertisement above, it announced the development of a set of guidelines to clarify what environmental claims could amount to unfair practices under the Consumer Protection (Fair Trading) Act 2003. Under the act, statutory penalties are applicable for offences unlike the Code above. The guidelines will be published for public consultation when ready.

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