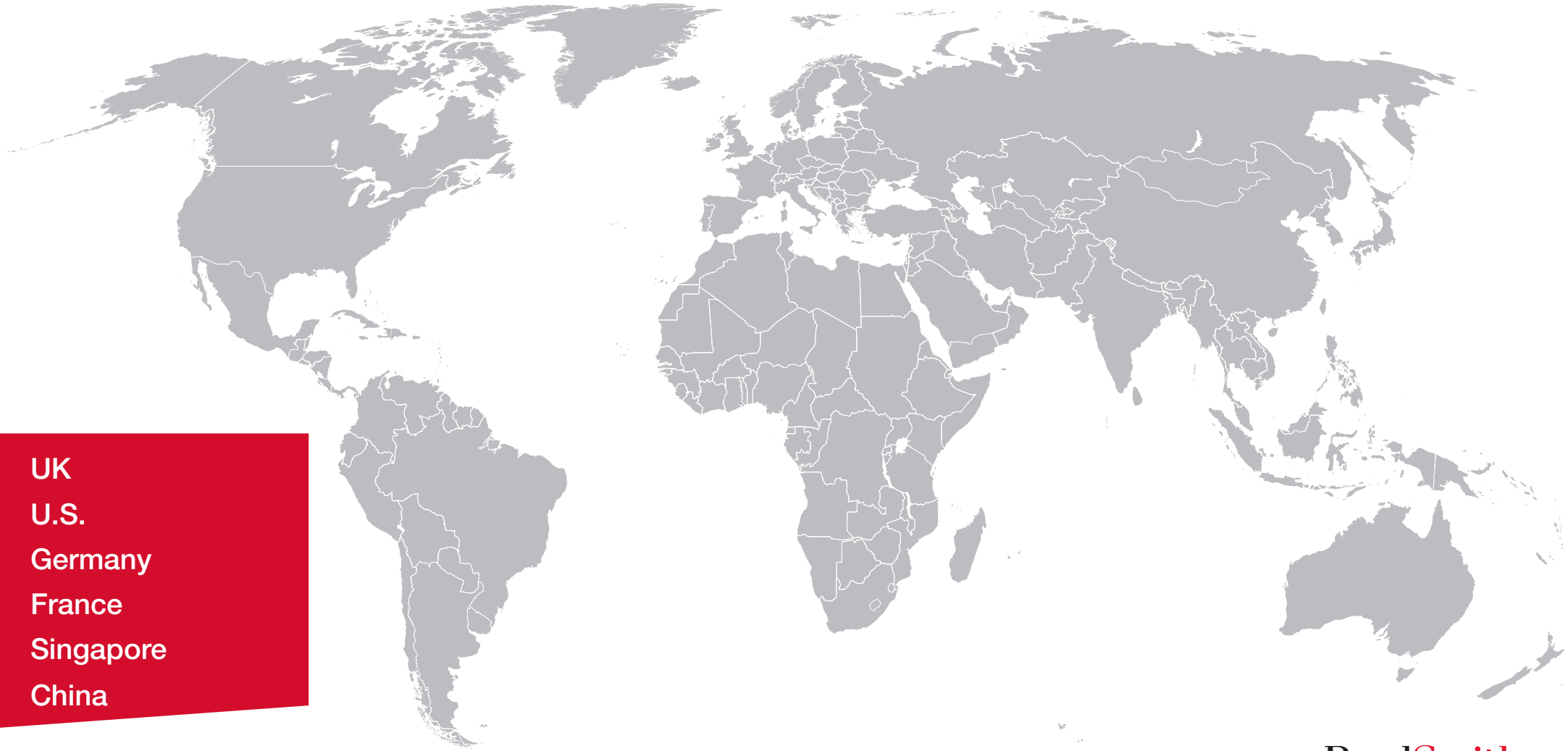
Adtech regulatory round-up
May 2021

The first few months of 2021 have proven to be busy for the adtech industry, with global efforts focused squarely on consumer privacy. Legal obligations together with vendor restrictions are requiring those in the adtech ecosphere to act with more innovation and efficiency than ever before, by constantly adapting to the ever-changing landscape. This report covers our analysis of the key adtech developments we've seen so far in 2021 with input from our colleagues in the UK, U.S., Germany, France, Singapore and China. **Click here** to read our January 2021 adtech round-up.



UK
U.S.
Germany
France
Singapore
China

reedsmith.com

ReedSmith
Driving progress
through partnership

UK

by Elle Todd, Nadia Avraham and Tom Gates

Back to map

Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022

In March 2021, the Digital Regulation Cooperation Forum (DRCF) published its first annual plan of work setting out its priorities for 2021 to 2022. The DRCF was formed between the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO) and the Office of Communications (Ofcom) in 2020, to enhance coordination and cooperation on the regulation of online services. The Financial Conduct Authority (FCA) became a member of the DRCF on 1 April 2021.

The plan of work explains that one of the DRCF's key areas of focus this year will be on digital advertising technologies. Of course, this has already been on the agenda of DRCF's members independently for some time. For example, in late January 2021, the ICO announced that it was resuming its investigation into real-time bidding and the adtech industry, which had been on hold since May 2020 due to the pandemic, and the CMA's own investigation into third party cookies is ongoing. It will be interesting to see how the increased collaboration between these organisations shapes the outcomes of these investigations later on this year.

Back in November 2020, the UK government asked the DRCF to provide its views on the challenges of delivering effective digital regulation. In response, the DRCF published its policy paper on 4 May 2021 setting out its thoughts on how to achieve a coherent regulatory approach. The **policy paper** recommends a review of information sharing gateways of digital regulators, adopting measure to incorporate regulatory coherence in the duties of digital regulators, and allowing the DRCF to input on strategic governmental priorities with respect to digital services and platforms.

Digital Markets Unit launched

As mentioned in our **previous round-up**, the UK government plans to consult on the form and function of the Digital Markets Unit (DMU), which is a product of the July 2019 CMA market study on online platforms and the digital advertising market in the UK. In April 2021, the DMU was officially established within the CMA in a shadow, non-statutory form.

The DMU ultimately plans to "oversee a new regulatory regime for the most powerful digital firms, promoting greater competition and innovation in these markets and protecting consumers and businesses from unfair practices."

The government intends to consult on how the DMU will operate in an official capacity and will then legislate to give the DMU statutory standing. It is thought that such statutory powers will include creating codes of conduct to govern how tech companies work with their users (including businesses), similar to the powers of the ICO to publish statutory codes in the data protection sphere. This would extend to the ways in which tech companies act in their capacities as digital advertisers.

Alternatives to cookies

It would be impossible to miss the industry proposals around "the end" of third party cookies and discussions around suggested alternatives such as "federated learning of cohorts", or "FLoC", which allows "interest-based advertising on the web" without letting advertisers know who you are. This emerged at the end of last year and this year we have already seen UK regulators start to look into it. The CMA made the first announcement in January 2021 with a focus on any potential impact on competition.

ICO launches data analytics toolkit

In February 2021, the ICO launched a new data analytics toolkit. The toolkit explains some of the key data protection points that organisations need to think about from the outset of any project they are planning to undertake involving data analytics and personal data. The toolkit defines data analytics as "the use of software to automatically discover patterns in data sets (where those data sets contain personal data) and use them to make predictions, classifications, or risk scores" and it has obvious use cases within the world of advertising.

The toolkit asks a series of questions under four different themes: lawfulness; accountability and governance; the data protection principles; and data subject rights. Once all the questions have been answered, the toolkit produces a short report containing tailored advice for the data analytics project, including practical actions the organisation can take and links to additional guidance on data protection compliance matters.

The ICO makes it clear that the toolkit should not be viewed as a "pathway to absolute compliance with data protection law", which it clearly isn't, but it is a useful, simple checklist for new data analytics and, as with all such ICO guides, acts as a good reminder of the minimum standards ICO expects companies to meet.

UK

by Elle Todd, Nadia Avraham and Tom Gates

Back to map

Less than four months to go until the Children's Code comes into force

A reminder that the ICO's Age Appropriate Design Code (also known as the Children's Code) comes into force in less than four months (on 2 September 2021). The Code contains 15 standards, and online services are expected to build these standards into the design of their services regarding the processing of the personal data of children up to the age of 18. These standards include providing privacy settings that are high by default; switching off geolocation services that can reveal a child's location to the world; and not using nudge techniques and notifications to encourage children to provide more personal data. The personalisation of online advertising is covered by the scope of the Code, which generally prohibits profiling by default, and sets out that only the minimum amount of a child's personal data should be processed in order to provide them with an online service – this means that ads that are personalised based on profiling or some other data processing must be switched off by default.

Many organisations still have a lot to do to ensure their services comply with these standards by September. It should be borne in mind that this is a statutory code, which means the ICO would consider whether a provider has complied with the Code in deciding whether it is compliant with data protection law. For example, if the ICO was considering a complaint that a provider had breached data protection laws, such as not being fair in its processing of children's data, it would use the Code as a guide to expected standards for compliance. Therefore, all of the high potential fines and enforcement powers that exist under the UK GDPR are applicable here, but there aren't separate fines for the Code specifically.

Processing cookie related data can bring those outside the UK/EU within the jurisdiction of the GDPR

It is well known that the General Data Protection Regulation (GDPR) brought with it extraterritorial reach and so can apply to a non-EEA/UK organisation in certain circumstances. Beyond regulatory guidance, however, in the UK, there has been little case law to test this extraterritorial reach until now. In the recent case of Soriano v. Forensic News LLC and Others [2021] EWHC 56 (QB), the claimant, Soriano, a resident and citizen of the United Kingdom, sued in relation to news articles and a number of social media posts published by the defendants, which included Forensic News, a U.S.-based investigative journalism website. Soriano relied on various causes of action, including data protection (under the GDPR), malicious falsehood, libel, harassment and misuse of private information. The court assessed the extent to which Forensic News could be considered as being subject to either limb of the territorial scope provisions of article 3 of the GDPR.

Whilst much of the case focused on the applicability of the GDPR to Forensic News' personal data processing in the context of the publication of a news article, certain obiter remarks made by the court are of particular relevance to adtech – specifically, remarks relating to article 3(2)(b) of the GDPR, which extends its scope to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the EU/UK, where the processing activities are related to the monitoring of their behaviour as far as their behaviour takes place within the EU/UK. The court stated that there is an "arguable case" that the monitoring requirement under article 3(2)(b) of the GDPR would extend to cookies that perform behavioural profiling or monitoring of individuals in the EU/UK in order to inform advertising choices. The result of this is that some businesses, which otherwise would not be subject to the GDPR, may be caught by the provisions of article 3(2)(b) if they are serving targeted ads to users in the EU or UK. **Read our article on the case here.**

IAB releases new guidance note on LIAs and DPIAs

In March 2021, the Interactive Advertising Bureau (IAB) Europe, in collaboration with IAB UK, released its GDPR Guidance on Legitimate Interests Assessments (LIAs) for the digital advertising sector (which complements its GDPR Guidance on Data Protection Impact Assessments (DPIAs)).

When organisations seek to rely on legitimate interests as the legal basis for processing personal data, they need to conduct an LIA to balance these interests against the rights and interests of individuals. The guide is intended specifically for use by digital advertising companies, advertisers, agencies and publishers in the EU and aims to provide a standardised approach for organisations that rely on legitimate interests for digital advertising activities.

The guide explains what an LIA is and when it should be carried out, and provides examples of how to carry out each of the stages of the three-part "balancing test" in the context of typical digital advertising data types and processing activities. For example, it gives helpful examples of the types of benefits that organisations can derive from particular processing activities, such as frequency capping and last-click attribution. It also has a useful appendix that sets out a non-exhaustive list of common risks in the digital advertising industry (e.g., unwanted disclosure, undue influence and misuse of data).

The guide is a useful starting point for organisations in the digital advertising sector seeking to rely on legitimate interests. However, it's important to remember that legitimate interests will not be appropriate in all situations. For some processing activities, consent will always be required under law (e.g., for setting cookies or similar technologies on a user's device) or more appropriate in the circumstances (e.g., if the processing is particularly high-risk or involves sensitive personal data).

United States

by Keri Bruce, Sarah Bruno and Kile Marks

Back to map

Virginia law impact on adtech

In the United States, the latest state to pass a comprehensive data privacy law is Virginia. Virginia's new consumer privacy law, the Consumer Data Protection Act (CDPA), includes a few components that will likely impact adtech. First, it includes a requirement that consumers must be given the option of opting out of targeted advertising. The CDPA defines a data controller as engaging in targeted advertising if they: 1) collect personal data from a Virginia consumer; 2) spanning "activities over time" and from third-party applications and websites; 3) for the purpose of predicting the "preferences or interests" of the consumer; and then display advertising that is based on the collected personal data.

There are several carve outs to the definition of targeted advertising. The first is advertising that is based on personal data collected from activities on the data controller's application or website. A second exclusion is when the advertising is based on the context of a consumer's search query, visit to a website or online application. A third exclusion is when the processing of the data is for purely measuring and reporting purposes. While these options may be helpful for some publishers, many companies in the adtech ecosphere will have to consider the opt-out if they are collecting or using personal information from Virginia consumers in a cross-context behavioral advertising capacity and are predicting the preferences or interests of a consumer.

Second, the CDPA requires a company to provide notice and obtain consent if it intends to use a consumer's personal information for a secondary purpose that is not reasonably necessary or compatible with the disclosed purpose for the data collection. This means that even if the advertising activity is not considered targeted advertising, advertisers must consider whether their use of data is for a secondary purpose and, if so, they will need to ensure notice was given and consent was provided. These are issues that publishers and brands must consider, and companies in the adtech industry should ensure they develop systems to comply with the CDPA.

Global changes to mobile platforms

While many members of the public may know how to view privacy settings on their phones, very few actually do so, even fewer go so far as to change those settings, and even fewer than that will deny permissions, or uninstall or stop utilizing an app based on the app's settings. Those days may be coming to an end.

Some operating systems have recently begun to shift to a more privacy-centric operating model, regardless of where the user is in the world. This model is giving rise to numerous changes which will impact the way consumers interact with mobile and app-based advertising.

Now that the above changes have taken effect, consumers who in the past ignored privacy settings will be forced to interact with privacy permissions on an app-by-app basis. When a consumer interacts with an app, they will be greeted with a pop-up notification asking them if they would like to share their Identifier for Advertisers (IDFA), as well as a short blurb from the app owner.

The option to refuse to provide their IDFA gives the average consumer a large amount of power. Advertisers who rely on mobile and app data for ad revenues, ranging from the smallest new entrant into the market to the largest data players in the world, have concerns that the changes could be devastating to their advertising revenues, with some players expecting an up to 50 percent decrease after these changes take effect.

There are some mobile advertisers who believe they can avoid compliance with these new privacy-highlighting changes. However, industry players are urging caution when trying to take that route, as potential punishments for improperly tracking or sharing consumers' data without the requisite permission include removal from the app store.

Global media alliance launches first report

The Global Alliance for Responsible Media (GARM), which brings together media agencies, marketers, media owners and industry associations to unite and work together to improve consumer and brand safety in ad-supported digital media, has just launched is first digital measurement report. The report analyses brand safety across the largest digital platforms, and provides a framework for those in the advertising industry to make more informed decisions about their advertising investment. The framework itself focuses on how safe the platform is for consumers and advertisers, how effectively the platform enforces its safety policies, and how responsive the platform is at correcting mistakes. GARM was founded by the World Federation of Advertisers, is supported by a number of industry trade bodies, and aims to address the challenge of harmful content on digital media platforms and its monetization via advertising.

Germany

by Andreas Splittgerber and Sven Schonhofen

Back to map

Continued negotiations on the EU ePrivacy Regulation

On an EU level, the negotiations for a new ePrivacy Regulation continue. On 10 February, after four years of negotiation, the EU Council finally agreed on its approach. Article 8 of the draft ePrivacy Regulation includes rules on the use of cookies and similar technologies, such as fingerprinting (Cookies). Cookies can be used based on either consent, or necessity for a range of things, such as to provide an electronic communication service, to provide a requested service, for software updates, audience measurement, fraud prevention and emergency purposes. Quite surprisingly, the exception from the consent requirement for audience measurement purposes is drafted very broadly and is, for example, not limited to first-party Cookies or only aggregated audience measurement (where the statistical data is not connected to a specific user identifier).

The European Data Protection Board (EDPB) has released comments on the Cookie rules in the ePrivacy Regulation. The EDPB calls for a limitation of the audience measurement exception to cover only low-level analytics Cookies that do not give rise to singling-out or profiling of any user, the provider, or other data controllers, and that do not allow the collection of navigation information related to users across websites or applications. The EDPB also calls for specific provisions on Cookie walls and effective ways to obtains consent and address consent fatigue.

The ePrivacy Regulation will now enter into trilogue negotiations. It will likely not enter into force before 2022, with an additional one or two year grace period for organisations to comply with its requirements.

Proposed new cookie rules in Germany

It seems, however, that the German legislator has doubts about whether the ePrivacy Regulation will actually get through its trilogue negotiations. On the same day as the EU Council presented its mandate on the ePrivacy Regulation, the German Federal Council adopted new Cookie rules in the draft Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutzgesetz) (TTDSG). Section 24 of the TTDSG implements the 12-year-old Article 5(3) of the ePrivacy Directive and limits the use of Cookies to three cases: (1) user consent, (2) necessity to provide the service explicitly requested by the user, and (3) necessity for facilitating the transmission of a communication over a public telecommunications network. Legitimate interests (Article 6(1)(f) GDPR) cannot be used as a legal basis anymore. The TTDSG also does not provide an exception from the consent requirement for audience measurement Cookies. The legal bases in the TTDSG are thus more limited than the legal bases set forth in the ePrivacy Regulation. The timing of the TTDSG is not clear at this point, but we expect that the TTDSG could enter into force before the German parliament's summer break. This would put organizations in a place where they could use audience measurement Cookies only with the user's consent under the TTDSG for a few months until the ePrivacy Regulation enters into force, at which point consent would no longer be required.

There are still a number of open questions regarding the Cookie rules in the TTDSG. For example, the TTDSG does not address the use of affiliate marketing Cookies that enable the payment of a commission from an advertiser to a publisher. User consent is not feasible for such Cookies, but they are also not strictly necessary to provide the website. The TTDSG also does not clearly address cookieless tracking.

France

by Natasha Tardif and Audrey Augusto

Back to map

Further clarification on the use of cookies

In September 2020, the French Data Protection Authority (CNIL) published its revised guidelines and "recommendation" on cookies and other tracking devices and announced a six-month transition period to allow companies to bring their websites and apps into compliance with the new rules. During the first quarter of 2021, as expected, the CNIL focused on guiding stakeholders in their compliance efforts. It published various factsheets and a FAQ clarifying the new cookie framework and providing further practical guidance. It also reached out to both public and private organizations to raise awareness of the risks associated with non-compliance.

As mentioned in our **previous round-up**, consent is at the heart of this new framework. The FAQ devotes several questions to the issue of consent, notably to cookies that are exempt from the requirement to obtain users' consent, to the information to be communicated to users before obtaining their consent and how to enable users to either accept or refuse cookies in a compliant manner.

The FAQ recalls that consent requires an unambiguous positive action from users, such as clicking on an "accept" button. It stresses that continuing navigation cannot be viewed as a valid expression of consent and that, subject to future developments in technology, referring users to Internet browser settings would also be insufficient. Cookie management tools should also allow users to refuse cookies as easily as they can accept them. This is of particular concern to the CNIL, which recommends including "accept" and "reject" buttons on the same screen, echoing similar advice previously issued by the UK's ICO. Enabling users to refuse cookies by closing the cookie banner is another valid option. However, a two-step process, whereby users have to click on a "manage preferences" button and only then on a "reject" button, would likely not meet the CNIL's expectations.

Of course, the FAQ also addresses cookie walls. Following the decision of the French Administrative Supreme Court, the CNIL had to amend its guidelines to lift the ban on cookie walls. The CNIL nonetheless considers that cookie walls are likely to infringe the freedom of consent, in particular where no satisfying alternatives are offered to users. This is in line with the European Data Protection Board's recent statement calling for a prohibition of "take it or leave it" solutions, such as cookie walls.

Ensuring appropriate information is displayed to users is another important topic for the CNIL. The FAQ provides clarification on the content and display of the information included in the cookie banner/window. The CNIL recommends including information on the purposes of the cookies, on the possibility to withdraw consent and on the potential consequences of refusing cookies, and enabling users to consult the list of data controllers, for instance through a button or hyperlink appearing on the cookie banner. The CNIL stressed that cookie banners merely including a general statement, such as "This website uses cookies" or "Cookies are used to improve the efficiency of our services" would not be compliant.

Consent exemption for certain analytics cookies

In a dedicated factsheet, the CNIL sets out the conditions under which audience measurement cookies can be seen as essential to the functioning of a website or app and so exempted from requesting users' prior consent. To benefit from the exemption, audience measurement cookies must be used by the web publisher for the sole purpose of audience measurement in order to produce anonymous statistical data, which should not be combined with other processing activities or transferred to third parties, and cookies should not allow the global tracking of users across websites. The CNIL further recommends limiting cookie duration to 13 months and data retention to 25 months. The CNIL gives examples of measurements that are strictly necessary for the functioning of a website, such as the analysis of the device used to connect and its screen size, what browser was used, the page loading time, the time spent on each page or the actions taken by users (clicking, selecting, etc.).

In March 2021, the CNIL also launched an evaluation program aimed at identifying audience measurement solutions that do not require consent. Companies offering audience measurement solutions for websites hosted in France or having users residing in France can send their submissions by 30 June 2021, and the CNIL will then publish a list of solutions meeting the conditions for consent exemption.

End of the transition period to comply with the new cookies rules

The transition period to comply with the new rules on cookies and other tracking devices ended on 31 March 2021. The CNIL announced that it would start carrying out inspections and potentially issue injunctions and/or fines against parties that fail to comply. The CNIL identified the use of cookies as one of its top three enforcement priorities for 2021. The decisions adopted by the CNIL at the end of 2020, which imposed fines totally €138 million on three stakeholders, show that the CNIL will not shy away from using its enforcement powers to prosecute infringements. The CNIL stressed that it would continue cooperating with its European counterparts with respect to cross-border data processing, through the exchange of relevant information, mutual assistance and joint operations. The CNIL also set up an observatory with the aim of periodically analysing the cookies placed by the 1,000 websites with the highest audience in France, using the CookieViz software.

Singapore

by Charmian Aw

Back to map

Personal Data Protection Act amended to include business improvement exception to consent

On 1 February 2021, the first slew of amendments to **Singapore's Personal Data Protection Act 2012** came into effect. One of these amendments was the introduction of a new exception to consent where personal data is used by an organisation for a business improvement purpose. A "business improvement purpose" is defined broadly to include improving or enhancing any goods or services, or developing new goods or services, learning about and understanding the behaviour and preferences of existing or prospective customers in relation to, or identifying the suitability of and customising, any goods or services to be provided by the organisation.

The conditions for relying on this exception are:

(a) the purpose for which the organisation uses the personal data cannot reasonably be achieved without it being in an individually identifiable form;

(b) a reasonable person would consider such use to be appropriate in the circumstances;

(c) the organisation cannot rely on the exception to send direct marketing messages; and

(d) the organisations involved in sharing the personal data are bound by a contract requiring the recipient(s) to maintain appropriate safeguards to protect the data.

Some similarities to the GDPR's concept of legitimate interests can certainly be drawn from the business improvement purpose. The exception also applies to the sharing (i.e., collection and disclosure) of personal data between group entities, without the need for consent, for any of the above business improvement-related purposes. Given its very wide scope, it is possible for this new business improvement exception to be deployed in a range of adtech-related activities so long as the applicable conditions are met.

China

by Dora Wang and Cindy Shen

Back to map

A new set of advertising marking specifications to serve the digital advertising industry

On 10 December 2020, the China Advertising Association (CAA) released the first set of device marking specifications which apply to online advertising specifically. The Technical Specification for Mobile Internet Advertising Identification (T/CAAAD 003-2020) (Specification) and the China Internet Advertising Delivery Monitoring and Verification Requirements (T/CAAAD002-2020) (Requirements), which came into effect on 1 January 2021, aim to establish advertising identifiers in furtherance of the development of the digital advertising industry.

The Specification defines Internet advertising identifiers for mobile devices and regulates their generation, general principles (with regard to, for example, effective use, information security and the protection of privacy, and the protection of industrial interests), functional requirements and security requirements. The Specification also provides various implementation schemes for advertisers and other market participants in the online advertising industry to comply with the Specification.

The CAA stated: "The implementation of the Specification is conducive to the development of China's independent advertising marking system and the deployment of Internet advertising marking solutions which take into account data privacy and personal information protection; meet the requirements of relevant laws and regulations, and national information security standards; meet the needs of industry developments; and provide basic services for the Internet advertising industry."

Under the unified and regulated Internet advertising standards, the Requirements aim to define the scope of monitoring and verification of Internet advertising; ensure the standardization and replicability of the activities of the Internet advertising industry; and ensure uniformity in the monitoring and verification of Internet advertising. While these specifications are not compulsory, they are nevertheless relied on by regulators as being the industry standards based upon which other related laws and regulations, such as the Advertising Law, are enforced.

Measures for the Supervision and Administration of Online Transactions – an important supplement to the E-Commerce Law

On 15 March 2021, China's State Administration for Market Regulation issued the Measures for the Supervision and Administration of Online Transactions (Measures). The Measures set out provisions on the registration requirements for network operators, the supervision of new business models, the responsibilities of platform companies involved in online transactions, the protection of consumer rights, and the protection of personal information.

Companies that provide promotional and advertising services to network business operators must promptly assist government agencies that are responsible for market regulation in investigating and cracking down on illegal online transactions and provide any relevant information in their possession. Network business operators must not send commercial information to consumers without their consent or request such information from consumers.

Necessity as basis for apps to collect personal information

On 22 March 2021, the Cyberspace Administration of China, the General Office of the Ministry of Industry and Information Technology, the General Office of the Ministry of Public Security and the General Office of the State Administration for Market Regulation jointly released the Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications (Provisions), which came into effect on 1 May 2021.

The Provisions prohibit mobile app operators from refusing to provide a mobile app's basic functions to users if they decline to provide personal information that is unnecessary for the app's basic functions. The Provisions outline 39 categories of apps and the scope of personal information that is considered to be "necessary" for these apps' basic functions ("necessary personal information"). Among them, 13 categories of apps are considered to have no personal information requirement; as such, apps in these categories must provide basic functions or services to users even if the users refuse to provide any personal information. It is expected that the Provisions will drive Internet companies that use direct marketing and targeted advertising as their main profit model to innovate in ways that optimize the use of big data without the unnecessary collection of personal information.

Meet the authors

Back to map

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors – listed below – or the Reed Smith lawyer with whom you regularly work.

UK

Elle Todd
Partner, London
etodd@reedsmith.com

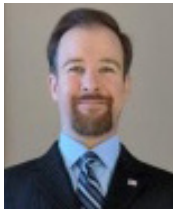
Nadia Avraham
Associate, London
navraham@reedsmith.com

Tom Gates
Associate, London
tgates@reedsmith.com

U.S.

Keri Bruce
Partner, New York
kbruce@reedsmith.com

Sarah Bruno
Partner, San Francisco
sbruno@reedsmith.com



Kile Marks
Associate, San Francisco
kmarks@reedsmith.com

France

Natasha Tardif
Partner, Paris
ntardif@reedsmith.com

Audrey Augusto
Associate, Paris
aaugusto@reedsmith.com

Germany

Andreas Splittgerber
Partner, Munich
asplittgerber@reedsmith.com

Sven Schonhofen
Associate, Munich
sschonhofen@reedsmith.com

Singapore

Charmian Aw
Counsel, Singapore
caw@reedsmith.com

China

Dora Wang
Partner, China
dwang@reedsmith.com

Cindy Shen
Legal Consultant, Shanghai
cshen@reedsmith.com

ReedSmith

Driving progress through partnership