AdTech round-up 2022

January 2023

ReedSmith

Driving progress
through partnership

In last year's round-up, we foresaw a busy and unpredictable year for adtech in 2022, and we weren't wrong

In our latest edition, it is clear now more than ever that there is no single source of regulation when it comes to online advertising – globally there have been developments in data protection law, competition regulation and online safety, with adtech being caught in the crossfire at all turns. This patchwork approach to regulation means that practitioners will need to consider a range of legal domains in order to achieve compliance with applicable requirements. In this edition, among other things, we look ahead to the updated UK Online Safety Bill, the finalized EU Digital Services Act, and a potentially even busier year ahead in the U.S. and Asia.

Contents

UK

Online Safety Bill

In 2022, the Online Safety Bill (OSB) came under increased scrutiny and there were even rumors of its abandonment; however it finally returned to the House of Commons on December 5, 2022, with an updated version being published shortly after, containing a number of significant amendments. The OSB of course covers a very broad range of topics, but below we focus on the specific implications around adtech and advertising in the most recent draft. The current draft of the OSB covers advertising in several different respects:

User-generated content

In relation to user-generated content (i.e., content uploaded to a service by a user that may be accessible by other users of that service), certain advertisements may fall within the scope of this definition. Where an advertisement has been uploaded by a user to a service which other users of that service may see (i.e., a sponsored post or video uploaded by an influencer, or a live video where a user is advertising a product), this will constitute user-generated content and will therefore be subject to the OSB's various content obligations (relating to illegal content and content that is harmful to children/adults). The result of this is that a large amount of advertising on social media platforms, which is already regulated in other ways such as by the Advertising Standards Authority, will be subject to further scrutiny by the OSB.

There have been several material developments including, most significantly, the plan to include a "legal but harmful" provision regarding online content being scrapped. The changes mean that platforms will still be required to remove illegal content but have discretion to enforce their own content policies in relation to "legal but harmful" content. The changes seek to protect freedom of speech by prohibiting platforms from removing or restricting user-generated content, or suspending or banning user accounts, provided there is no breach of their terms of service or applicable law.

Paid-for ads

Obligations in relation to other types of advertising have also been introduced by the OSB. Advertisements that are not user-generated content (i.e., have not been uploaded by a user), but have involved the service provider receiving some sort of monetary or non-monetary payment to display that advertisement, also fall within the OSB. This type of advertisement is caught by new fraudulent advertising safety duties. Duties are specific to Category 1 services (the highest reach user-to-user services with the highest risk functionalities) and Category 2A services (the highest reach search services).

Generally, Category 1 and 2A services must use proportionate systems and processes designed to: (i) prevent individuals from encountering fraudulent advertisements; (ii) minimize the length of time fraudulent advertisements are present on the service; and (iii) swiftly take down such content when alerted to its presence or otherwise becoming aware of it. Category 2A services must include clear and accessible provisions in their terms of service about technologies in place to prevent fraudulent advertisements appearing on their service, whereas Category 1 services must publish a publicly available statement containing the same information. Specific steps to address fraudulent advertising will be set out in an upcoming Ofcom code of practice.

Further amendments to the OSB will be considered at the report stage in the House of Commons on January 17, 2023. While the plans were that it would come into force by May 2023, the most recent amendments may cause a delay to this.

Data Protection and Digital Information Bill

The Data Protection and Digital Information Bill (DPDI) was laid before Parliament on July 18, 2022 in response to the "Data: a new direction" consultation. The DPDI is still in its infancy and the second reading, which was due to take place on September 5, 2022, was postponed with no indication as to when it will take place. The impetus behind the DPDI is to update and reform the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation 2003. The UK government has stated that nothing in the DPDI would threaten the UK-EU adequacy arrangement in place, which allows for the sharing of personal data between the UK and EU without the need for standard contractual clauses. While the wider implications for advertising and adtech are forthcoming in future drafts and guidance, the DPDI does aim to "remove the need for unnecessary cookie consent banners" and as such creates exemptions to consent requirements. These currently only extend to low-risk activities such as audience measurement; however the DPDI allows for further consent exemptions to be added via secondary legislation, so this is subject to change.

A year of the Children's Code

September 2022 marked the first anniversary of the Information Commissioner's Office's (ICO) Children's Code (also known as the Age Appropriate Design Code), along with its 15 standards for the design of online services processing children's personal data. Personalization of online advertising is covered by the scope of the code, which prohibits profiling by default and requires that only the minimum amount of a child's personal data should be processed in order to provide them with an online service. In short, this means that advertisements that are personalized based on profiling or some other data processing should be switched off by default for children. In practice, many services using cookies for such purposes already operate a consent model, so the impact is largely on other, non-cookie-based data usage for targeted advertising and on measures to ensure that privacy settings and information are suitable for children. Since the implementation of the code, a number of social media and streaming platforms have introduced changes to their products, often relating to targeting and default settings, to comply with the code. The ICO has said that it will continue to evolve its approach, listening to others to ensure the code is having the maximum impact.

UK government consultation on online advertising

In the summer of 2022, the UK government ran a consultation on its "Online Advertising Programme" focusing on digital innovation and technical changes in the online advertising market. The consultation called for comment on three key proposals: (i) continued self-regulation; (ii) self-regulation with statutory backstop; and (iii) full statutory regulation of the online advertising regime. Aiming to "tackle the evident lack of transparency and accountability across the whole supply chain," the government is currently analysing feedback and a response is expected sometime in 2023.

New direct marketing guidance

In November 2022, the ICO published a suite of new guidance notes and checklists for businesses carrying out direct marketing via SMS, phone and email. All of this information has been consolidated into a single resource which can be found here. Specific guidance is available for SMEs, political campaigners, data brokers and B2B marketers, as well as training modules for businesses to complete.

EU

Implementation of the Digital Markets Act – European Commission adopts an open-dialogue stance

The Digital Markets Act (DMA) entered into force on November 1, 2022 and will apply to gatekeepers from May 2, 2023. Companies that operate digital platforms that have significant market power in the provision of certain digital services are currently preparing their "gatekeeper" self-designation forms ahead of this deadline. While not specific to ad tech, the focus on large platforms will, of course, inevitably mean that there is more scrutiny of the ways in which advertising on such platforms is managed. The European Commission (EC) recently indicated that it is open to discussion, and it is encouraging companies to enter into a pre-notification period for self-designation as early as January 2023, to allow for a three-month dialogue on whether companies meet the thresholds.

The DMA introduces 22 new behavioral obligations (do's and don'ts including relations with integrated services and how gatekeepers must conduct business partnerships in the future), in addition to new merger control and audit obligations. While some, such as the obligation on gatekeepers to inform the EC about transactions they intend to carry out in the digital sector (which could include those impacting adtech), will be applicable from the designation of the gatekeepers by September 6, 2023, most of the obligations will apply from March 2024. Companies that fail to self-designate or do not comply by then risk heavy fines as well as behavioral injunctions.

To assist future gatekeepers in their interpretation of the DMA, the EC has announced that guidelines and orientations will be prepared. In addition, the EC intends to hold workshops on certain aspects of the DMA. It already started with one on how to apply the ban on self-preferencing (December 5, 2022) and launched a one-month public stakeholder consultation on December 9, 2022.

Adoption of the DSA – toward more moderation on large online platforms and search engines

The Digital Services Act (DSA) entered into force on November 16, 2022. The DSA sets out obligations for providers of digital services, such as social media platforms or marketplaces, to minimize the risks of spreading illegal content and misinformation online (especially for large platforms with more than 45 million users), as well as putting mitigation measures in place, including audits and reviews. As covered in our previous adtech round-up, the DSA prohibits the use of personal data of minors to profile them for the purpose of carrying out targeted advertising, and additionally places a ban on the use of special categories of personal data of any individual for the same purpose. There are also obligations placed upon smaller platforms and rules concerning non-systemic issues on very large online platforms (VLOPs) and very large online search engines (VLOSEs) to maintain a publicly available repository of online advertisements they have presented on their service, along with various other data, for a year following the last appearance of the advertisement in question.

The DSA will be directly applicable across the EU from February 17, 2024. By then, member states must empower their national authorities to enforce the new rules on VLOPs and VLOSEs, which will be in addition to the EC's direct supervision over these tools.

Online platforms have until February 17, 2023 to report the number of active users on their websites. Further to this report, the EC will assess whether a platform should be designated a VLOP or VLOSE. Further to such a designation, they will have four months to comply with the DSA, including its first annual risk assessment exercise.

IAB update

In February 2022, the Belgian Data Protection Authority (APD) fined IAB Europe €250,000 for failures by its Transparency and Consent Framework (TCF) to comply with the GDPR – more on this here. 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.

The APD found that IAB Europe was responsible for a number of GDPR violations related to lawful processing, transparency, accountability and controller obligations. IAB Europe was issued with the abovementioned fine of €250,000 and was ordered to present an action plan setting out how it would address the issues identified by the APD. IAB Europe

has appealed the decision, arguing that it is not a data controller in the context of the TCF and as such is not required to comply with these obligations, suggesting that the decision would have major “negative consequences going well beyond the digital advertising industry.” Various grounds of appeals were raised and several have since been referred to the European Court of Justice (ECJ). Substantive appeal points related largely to the definition of “personal data” and “controller” under the GDPR and how these interact with the IAB’s TCF offering. The APD recently published a press release in which it announced that it has approved the IAB's action plan, which is surprising given that the APD’s initial decision remains subject to an ongoing appeal. In addition to this, the substance of the action plan has not been released due to the aforementioned ongoing court proceedings, however we do know that IAB Europe has six months to implement the changes it has proposed.

France

Continued scrutiny of adtech practices under competition law

European competition authorities have been increasingly active in the adtech sector. In 2021, the French Competition Authority (FCA) imposed a fine on a global player for implementing self-preferencing practices and favoring its own advertising technologies over those provided by competitors. The scrutiny into the adtech industry continued into 2022, with the FCA issuing a decision accepting binding commitments from a company to address the competition concerns associated with the implementation of its adtech program.

These recent enforcement initiatives are an important reminder that adtech practices can be caught by competition law. They sit within a wider EU debate on how competition law should be used to help tackle issues relating to the collection and use of data. While data-related issues were not traditionally seen as a matter for competition law, the development of digital markets and the assessment of data as a source of market power led to increased scrutiny from global competition regulators.

Inter-agency cooperation, notably between the FCA and the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), has also increased in recent years. In November 2022, the CNIL's president gave a speech before the FCA announcing that she had entrusted Bruno Lasserre, former president of the FCA, with the mission of assessing the link between data privacy and competition law, with the aim of better integrating the work of the two authorities and increasing their practical impact.

The path forward for cookie walls

Back in 2020, following the decision of the French Administrative Supreme Court, the CNIL had to amend its guidelines on cookies and other tracking devices to lift the ban on cookie walls. The CNIL nonetheless stressed that cookie walls were likely to be non-compliant, in particular where no satisfying alternatives were offered to users. This was in line with a statement from the European Data Protection Board calling for a prohibition of "take it or leave it" solutions, such as cookie walls.

The CNIL has now published a list of criteria for assessing the lawfulness of cookie walls, which gives some guidance to website and app publishers – fairness, proportionality and transparency are the guiding principles.

The CNIL recommends offering a real and fair alternative, allowing users to access a website without having to consent to the use of their data. The website publisher would otherwise have to demonstrate that another publisher offers such an alternative, without making access to its services conditional on users' acceptance of cookies. Special attention must be paid to a potential power imbalance between publishers and users, which could effectively deprive users of a real choice. This could be the case where publishers have exclusivity over the content offered or where users have few or no alternatives, for instance in case of dominant or essential service providers.

Where publishers set up paywalls, making access to their services conditional on payment, the price should be reasonable. Rather than setting specific monetary thresholds, the CNIL noted that this should be subject to a case-by-case assessment. The CNIL specified that financial compensation does not necessarily involve a paid subscription and can take the form of virtual wallets, allowing users to make micro-payments to access specific content or services without having to save their card details.

The CNIL also provides guidance on login walls. The CNIL stresses that the requirement to create an account should be justified according to the intended purpose. For instance, creating an account may be justified when it is necessary to enable users who have chosen to set up a subscription, to benefit from that subscription on other devices. In addition, publishers should inform users about the use of their data and limit data collection to what is necessary for the objectives pursued.

With respect to the extent of the consent given in the context of cookie walls, the CNIL recalls that cookie walls requiring users to accept all cookies, and not each type of cookie separately, can affect the validity of the consent given by users. Publishers will hence be required to demonstrate that their cookie wall is limited to the purposes that allow them to receive a fair compensation for the service offered. For instance, where a publisher considers that the remuneration of its service depends on the revenues it could obtain from targeted advertising, the CNIL considers that only the consent

to this specific purpose should be necessary to access the service. The refusal to consent to other purposes, such as content personalization, should not prevent users from accessing the website or app.

Finally, the CNIL clarifies that in principle, when users opt for the paid alternative, without accepting cookies, no cookie requiring the users' consent should be deposited on their terminals. However, publishers may request the users' consent, on a case-by-case basis, where cookies are required to access content provided by third-party websites or another service requested by the user, for instance to view a video hosted by a third-party website.

CNIL's enforcement actions

This year, the CNIL has again shown its willingness to use the full range of its enforcement powers to ensure compliance with the GDPR and the French Data Protection Act. The CNIL's powers have a wide reach. In this respect, the French Administrative Supreme Court confirmed that the GDPR's one-stop-shop mechanism does not apply regarding cookies and that the CNIL has jurisdiction over foreign companies when they have an establishment in France involved in processing activities. With 18 fines imposed in 2021, totalling more than €214 million, and new hefty fines imposed in 2022, the CNIL is seen as one of the toughest enforcers in the EU.

Germany

CJEU says inbox advertising covered by ePrivacy Directive

In January 2022, the CJEU ruled on a reference from Germany, which asked whether restrictions on sending unsolicited direct marketing communications under Article 13 of the ePrivacy Directive apply to advertising messages that appear in email inboxes and look like normal emails. The practice is referred to as inbox advertising. The CJEU said (in its detailed summary) that the ePrivacy Directive would apply to the type of advertising in question.

German data protection authorities release comprehensive cookie guidance

The new German law on cookies, pixels, fingerprinting, and similar technologies (Cookies) – the Telecommunications Telemedia Data Protection Act (TTDSG) – entered into force on December 1, 2021. The TTDSG must be considered when setting and reading the information in Cookies. The GDPR applies to the further processing of personal data in connection with Cookies. The TTDSG only provides for two categories of Cookies: (i) Cookies that require consent and (ii) Cookies that are absolutely necessary for the provision of the telemedia service requested by the user. The TTDSG does not include the legal basis of legitimate interests.

The German data protection authorities released the first draft of their guidance on the use of cookies (Cookie Guidance) shortly after the TTDSG entered into force in December 2021. Following a public consultation, the German data protection authorities published an updated version on December 5, 2022, accompanied by a comprehensive paper discussing the comments submitted throughout the consultation.

The Cookie Guidance discusses in particular:

- The technologies for which section 25 of the TTDSG (Cookie Consent rule) applies
- Requirements for Cookie consent
- Requirements for Cookies to be considered “absolutely necessary for the provision of the telemedia service requested by the user”
- Legal bases under the GDPR for the processing of the data collected by the Cookies
- Requirements for Cookie banners
- Further data subject rights

Some of the main findings in the Cookie Guidance include:

- The TTDSG does not apply to data that is automatically transmitted by the end user’s browsers (e.g., browser or header information transmitted in an HTTP request, including IP address, URL of the website visited and the user agent).
- The German data protection authorities take the view that it is not sufficient if users only have “Accept” and “Settings” options in the Cookie banner, but no “Decline” option.
- The website operator must clearly inform users of the legal bases under both the TTDSG and the GDPR.
- The German data protection authorities apply a strict approach to Cookies that are “absolutely necessary.” For example, Cookies shall be considered absolutely necessary only in limited cases where they collect specific cookie IDs.
- The German data protection authorities refrain from providing clear guidance on when analytics and reach measurement Cookies fall into the “absolutely necessary” category and so do not require consent.

Whistleblower Protection Act transposing EU Directive 2019/1937

The German Whistleblower Protection Act (Act) is expected to come into force in early summer 2023, transposing EU Directive 2019/1937 on the protection of whistleblowers reporting breaches of EU law. In contrast to the EU Directive, the material scope of application includes in particular criminal law and certain administrative offenses. In addition, the areas of law specified by the EU Directive were extended to a limited extent to correspond with national law. The new law establishes an internal and external system for reporting breaches of EU law in the public and private sector, as well as the channels for reporting, the follow-up process and the protective measures to be adopted in order to avoid retaliation.

Online shops must offer the option to “Buy as a guest”

According to a recent resolution of the German data protection authorities, online shoppers must be given the option to shop by setting up a customer account or by checking out as a guest for transaction purposes only. The German data protection authorities require consent as a legal basis for the processing of personal data in connection with a customer account. Customers must be able to choose between shopping with a customer account or guest account for the consent to be freely given. The resolution has been heavily criticized, in particular as it does not consider other legal bases, e.g., the general provision of the customer account being a contractual requirement.

Greece

The “byDesign” project

In 2020, the Greek Data Protection Authority (DPA) undertook a two-year project named “byDesign” with the goal of facilitating SME compliance with the GDPR by offering a tailored compliance kit, and to promote the creation of data protection by design IT products and services. The project was completed in October 2022 and was presented at the online international conference “Presentation of the project ‘byDesign’ outcomes.” The compliance tool will be particularly useful to SMEs operating in the adtech space.

Guidelines no.1/2020 on the operation of cookies

Further to guidelines no. 1/2020 on the operation of cookies, issued by the DPA in 2020, the DPA recently conducted large-scale investigations on the use of cookies by websites. Among the most common breaches found was the absence of a “Reject” or “Disagree” option in the cookie banner or the presentation of the “I agree” option with more attractive tabs or fonts. All the investigated websites save one adjusted their use of cookies in response to DPA warnings. The DPA continues to monitor closely compliance with the applicable legislation on the use of cookies.

Law 4990/2022 transposing EU Directive 2019/1937 on whistleblowers

Law 4990/2022 came into force on November 11, 2022, transposing EU Directive 2019/1937 on the protection of whistleblowers reporting breaches of EU law. The new law establishes an internal and external system for reporting breaches of EU law in the public and the private sector, as well as the channels for reporting, the follow-up process and the protective measures to be adopted in order to avoid retaliation.

The new law provides for guarantees – especially with respect to the protection of personal data – that should be offered to ensure that any processing of personal data conducted in the course of such reporting is in accordance with the GDPR, while at the same time describing the specific conditions that should apply in order to legally restrict data subjects’ rights to be informed about the processing of their data for public interest purposes.

China

Filing requirements for internet information service algorithms

Pursuant to the Provisions on the Management of Algorithmic Recommendations in Internet Information Services (effective March 1, 2022) (the Provisions) issued by the Cyberspace Administration of China (CAC), Ministry of Industry & Information Technology, Ministry of Public Security and State Administration for Market Regulation, the name of the service provider, service form, application field, algorithm type, algorithm self-assessment report, content to be published, and other information should be filed through an algorithmic filing system within 10 working days of the date of providing services. The Provisions shall apply to "algorithmic recommendation technology," which means applying generation and synthesis, personalized pushing, sequence refinement, search filtering, scheduling decisions, and other algorithmic technologies to provide information to users within the territory of China. Providers of targeted advertising and personalized technology would be regarded as algorithmic recommendation service providers.

Provisions on the Administration of Internet Pop-up Information Push Services

On September 30, 2022, the Provisions on the Administration of Internet Pop-up Information Push Services (the Provisions), jointly issued by CAC together with two other authorities, came into effect. The Provisions govern internet pop-up information push services and service providers, which refers to the push services provided to users in the form of pop-up message windows via operating systems, application software, websites, etc. Since a large number of ads are provided to internet users in the form of pop-up windows, the adtech industry is also caught by the scope of the Provisions.

The Provisions require that service providers ensure sound audit of information content, responsible governance, data security and personal information protection, protection of minors and other management systems. The Provisions also give examples of violations, such as pushing news information without authorization, failing to ensure that pop-up advertisements are identifiable, preventing users from closing ads with a single click, maliciously spreading entertainment gossip, pushing information too frequently, failing to push a range of messages and reasonable proportion of healthy and positive content, inducing traffic fraud, etc.

In particular, the Provisions prescribe that when pushing advertising information through pop-ups, service providers should make such information identifiable by clearly marking it with the word "advertisement," together with a close button to ensure that pop-up ads can be closed with a single click. Further, pop-up advertisements are not allowed to present information, such as third-party links or QR codes, that maliciously drives traffic to other websites or redirects users to other pages by means of pushing pop-up information, or to induce users to click through pop-up information push services for the purpose of carrying out traffic fraud.

Singapore

Legislation introduced to combat online harms

On November 9, 2022, the Singapore Parliament passed the Online Safety (Miscellaneous Amendments) Bill (the 'Bill'), which will amend the Broadcasting Act 1994 to make social media platforms responsible for protecting local users from online harms.

Social media platforms must block egregious content or accounts that communicate egregious content. Egregious content includes:

- Suicide or self-harm;
- Violence or cruelty or other infliction of serious physical harm on human beings;
- Sexual violence, depicting child nudity for a sexual purpose or exploiting child nudity in an offensive way;
- Conduct that is likely to obstruct public health measures or result in a public health risk in Singapore;
- Dealing with race or religion in a way that is likely to cause ill will or contempt or ridicule different racial or religious groups in Singapore; or
- Terrorism.

Social media platforms must also comply with Infocomm Media Development Authority's (IMDA) new codes of practice, which specify requirements for user reporting mechanisms, public accountability reports and other measures to limit online harms. Failure to comply is punishable by fines of up to S$1 million and in extreme cases, the IMDA may block access to the non-compliant social media platform entirely.

The Bill is expected to come into effect in early 2023 while the codes will take effect in Q1 2023 after consultations with certain social media platforms have been completed.

Regulation of gambling

The Gambling Control Bill 2022 and the Gambling Authority of Singapore Bill 2022 (the 'Act') were passed in Parliament on March 11, 2022 and came into effect on August 1, 2022. The Acts seek to update and harmonize gambling laws and repeal several half-century-old acts such as the Betting Act, the Common Gaming Houses Act, the Private Lotteries Act and the Remote Gambling Act.

One particular new feature is a Class-Licensing Regime, which was introduced to regulate gambling products assessed to be of lower risk. Under the regime, designated gambling services may be provided without the need to apply for a license from the Gambling Regulation Authority as long as the conditions set out in the applicable ministerial orders are complied with.

Gambling products covered under the Class-Licensing Regime include:

- Cause-related games of chance and lotteries;
- Survey-related games of chance and lotteries;
- Trade promotion games of chance and lotteries;
- Fundraiser lotteries;
- Remote games of chance;
- Incidental games of chance and lotteries; and
- Mystery boxes.

Each category is subject to a specific order setting out the relevant conditions. Of particular note to advertisers is the order relating to trade promotion games of chance and lotteries, which will take effect from February 1, 2023.

Limits on crypto-advertisements

On January 17, 2022, in a slew of restrictions targeting cryptocurrencies (digital payment tokens (DPTs) in the Singapore context), the Monetary Authority of Singapore (MAS) issued guidelines reflecting its position that DPT service providers should not promote their DPT services to the general public in Singapore. Under the guidelines, the trivializing of the high risks of cryptocurrency trading by advertising directed at the general public in Singapore is prohibited. This includes the placing of any form of advertisements or promotional materials in public areas in Singapore such as public transport (including stations, terminals and stops), broadcast or print media, third-party websites, social media platforms, public events and roadshows. The use of third-party social media influencers and joint promotions is also prohibited, although companies can operate their own websites and social media channels.

California

Do not "sell" or "share" requirements of the CPRA

The California Consumer Privacy Act (CCPA) provided California consumers with the right to opt out of the "sale" of their personal information. Although defined broadly, the determinative factor of whether a particular transmittal of data constituted a "sale" was whether "monetary or other valuable consideration" was offered in exchange for such data. In January 2023, the California Privacy Rights Act (CPRA) will introduce the concept of "sharing," which will focus on whether personal information is used by third parties for cross-context behavioral advertising. Specifically, a transmittal of data to a third party will constitute "sharing" under the CPRA if the disclosure or transfer is for the purpose of advertising based on personal information obtained from a site, platform, application or service that is not the site with which the consumer is intentionally interacting. This reaches certain targeted advertising practices that may not have been captured under the prior CCPA definition of "sell" but still facilitates personalized advertising capabilities.

As such, where a particular transaction is deemed sharing, covered businesses must include a "Do Not Sell or Share My Personal Information" link on all digital locations where personal information is collected.

In relation to the concept of "sharing," the CPRA proposed regulations (currently still in draft form), further clarify that entities that contract with a business to provide cross-contextual behavioral advertising will be deemed third parties and cannot be considered service providers or contractors with respect to cross-contextual behavioral advertising services. The specific example showcases the combined intent of the statutory language and the proposed regulations to address "walled garden" structures:

> "Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them."

Also notable in 2022 was the $1.2 million penalty that was issued by Attorney General Bonta against a retailer in California that Bonta determined did not: (i) disclose to consumers that it was selling their personal information; (ii) process user requests to opt out of sale via user-enabled global privacy controls (GPC), in violation of the CCPA; and (iii) cure these violations within the 30-day period currently allowed by the CCPA. The action serves as a warning to all companies that California's privacy law requires the opt-out as well as the use of GPC controls for digital exchanges that are deemed to be a "sale" or "sharing."

Thus, in addition to modifying consumer facing links, businesses will have to revisit and update data maps and identify those instances in which they may be "sharing" data to understand potential compliance burdens and business impacts. They also should consider technical solutions for GPC controls and opt-outs.

CPRA/CCPA regulations

The amendments to the CCPA made by the CPRA become effective on January 1, 2023. The new provisions under the CPRA will become enforceable starting July 1, 2023, and the California Privacy Protection Agency (CPPA) will be able to bring enforcement actions for violations that occurred on or after July 1. However, it is likely that the CPPA will not approve the final implementing regulations prior to the January 1, 2023 deadline. In October 2022, the CPPA board met to discuss revisions to the initial draft regulations, and approved revisions were then made to the draft regulations on November 3, 2022, triggering a 15-day public comment period. The CPPA is currently considering public comments and will decide whether to further modify the rules at a future meeting.

Notable provisions of the most recent version of the regulations include:

- Opt-out preference signals (e.g., GPC): The proposed regulations reinforce the mandatory nature of GPC signal recognition. The regulations also contemplate that businesses honor opt-out preference signals for any "known" users including users that may become "known" because of the use of probabilistic identifiers that may link a user/profile with certain browsers and devices. The proposed language reads (as of December 9, 2022): "The business shall treat the opt-out preference

signal as a valid request to opt out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information."

- Data minimization: Proposed regulations set out factors to be considered in evaluating: (i) the reasonable expectations of a consumer concerning the purpose for which personal information is collected or processed; (ii) the purposes that are compatible with the context in which the personal information is collected; and (iii) whether collecting or processing personal information is reasonably necessary and proportionate to achieve those purposes. The regulations contain factors for determining when the disclosed purpose is compatible with the context.
- Sensitive information: Sensitive personal information is broadly defined under the CPRA and includes (among other categories) information about a consumer's racial or ethnic origin or their religious beliefs or information concerning a consumer's health, sex life, or sexual orientation. These are broad categories of information that companies may be collecting as a result of identifying what advertisements are appealing to a consumer or what pages are visited by that consumer. The modified proposed regulations clarify that a business does not need to provide a notice of right to limit or a "Limit the Use of My Sensitive Personal Information" link if it only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer. If the business is inferring characteristics about a consumer as a result of this data, then it must allow the consumer to limit the use of this data.
- Contractual requirements: The modified regulations also set out contractual requirements between businesses and their service providers, contractors, and third parties. This includes identifying the "specific [b]usiness [p]urpose" (emphasis added) for which a service provider is processing personal information for a business and examples of what actions may be considered "reasonable and appropriate steps" the business may take to ensure that the service provider is using the personal information consistent with the law. There are similar requirements for contracts between a business and third parties.

Although it seems that the final regulations will not be approved until early 2023, one area of solace for covered businesses is the fact that the CPPA expressly recognized – through the addition of section 7301(b) – the potential impact on compliance efforts from the delayed rulemaking. In particular, section 7301(b) permits the agency to consider the delayed nature of the regulations when deciding whether to pursue potential investigations or violations of the CCPA.

Colorado

The Colorado Privacy Act (CPA) is slated to take effect in July 2023. On September 30, 2022, the Colorado attorney general's office published proposed rules covering the implementation of the CPA, setting off a public comment period scheduled to end on February 1, 2023. As such, the final rules are still months off.

The proposed rules cover a variety of topics, including: (i) the clarification of definitional issues; (ii) the treatment of opt-out signals and mechanisms; (iii) consent requirements related to the processing of particular categories of data, such as (a) children's data; (b) sensitive data; and (c) data targeted for advertising purposes (where the consumer has opted out); (iv) privacy policy requirements; and (v) the secondary use of collected data.

Because the final rules are still months off, businesses should continue to bolster their compliance efforts as they relate to both the CPRA and CPA (as well as the Virginia Consumer Data Protection Act). Although there will be inevitable nuance among and between these regulations that must be addressed, compliance with the core elements found in the laws set to become effective in January 2023 should provide the foundational operational requirements needed to comply with the CPA and other laws slated to become effective in July 2023.

Global privacy controls

Both the California and Colorado privacy laws require that businesses recognize and process global privacy control (GPC) signals. Although there is not much guidance on the technical implementation of GPC, it is clear that compliance is a high priority for the California attorney general in 2023 as evidenced by the CCPA. At a high level, GPC is an automated, browser-level signal that communicates a user's privacy preferences to the server. The aim of GPC is to automate users' privacy choices. Instead of having to manually request to opt out of sale or targeted advertising on each website, users can set their GPC tool to automatically send a signal indicating their desire to exercise their opt-out rights. On the technical front, the current draft regulations indicate that the GPC signal can be either (i) an opt-out signal (e.g., an HTTP header field or JavaScript object) or (ii) given by alternative means such as a "do not sell" list with an automated query tool for controllers. If a business receives a GPC opt-out signal from a user that it recognizes (i.e., via cookies or a user account), it must apply that opt-out throughout all of that user's interactions with the business. Finally, the Colorado attorney general plans to maintain a public list of recognized and compliant GPC tools.

Third-party cookie alternatives

The industry is working rapidly to replace third-party cookies with alternative identifiers, with proposed solutions from industry groups as well as entities in the adtech ecosystem. In addition to the development of more robust first-party data, email-based universal identifiers such as UID 2.0 (linked from users' logged-in states on publishers' properties), and a move back to contextual marketing, LiveRamp has proposed its own Authenticated Traffic Solution (ATS). ATS endeavors to help publishers recognize and match authenticated user data with a RampID (LiveRamp's pseudonymous identifier) in real time, enabling people-based advertising without relying on third-party cookies or device-based identifiers. Currently, LiveRamp's ATS can be implemented in one of three ways: (i) ATS API; (ii) ATS Mobile SDK; or (iii) ATS for Web (Javascript implementation).

IAB Tech Lab developments

In 2022, the Interactive Advertising Bureau Tech Lab (IAB Tech Lab) undertook many initiatives focused on building a stronger digital ecosystem while also balancing consumer privacy needs and ethical data sourcing and usage through the creation of technical standards, frameworks, and open source initiatives. These efforts included launching the Global Privacy Platform (GPP) to consolidate domestic and global privacy signals for digital advertising and the IAB Tech Lab is working on the launch of its Accountability Platform, designed to ensure consumer consent and privacy is enforced. Notably, IAB has stated that the U.S. Privacy Specifications, which were developed to support CCPA compliance, "will be updated to include the state-specific privacy strings that come into effect in 2023, instead these **will only be available using the GPP.**" Further, the IAB Tech Lab invested in research on invalid traffic and other forms of fraud to support the development of new protocols. The group also continued to develop its programmatic guides, focused on outlining the components and standards across an array of issues, including connected TV (CTV) with server-side ad insertion and ad fraud. Lastly, it has taken the initiative in supporting the growth of CTV through investment, research of technical standards, and launch of the OM SDK initiative across the CTV ecosystem.

IAB MSPA

The Interactive Advertising Bureau (IAB) and the IAB Tech Lab have updated their privacy protocols and have introduced a Multi-State Privacy Agreement (MSPA) for advertising agencies, marketers, publishers, and adtech companies. The MSPA seeks to provide a framework and assist the digital advertising industry to comply with various, complex state privacy laws (in, e.g., California, Virginia, Utah, Colorado, and Connecticut). The MSPA enables advertisers to manage consumers' personal information, including covering contractual obligations and gaps and applying a "national approach" option to apply multiple states' privacy laws to see which protections should be applied.

The MSPA seeks to help advertising participants when engaging in digital advertising practices that are subject to opt-out of sale, sharing, or target advertising under state privacy laws because they involve the disclosure of personal information in order to utilize digital ads specific to a consumer. The MSPA creates service provider relationships among various adtech parties and provides a means to incorporate terms in the service provider contracts and agreements, including provisions covering measurement and frequency capping when service providers are undertaking such activities. The MSPA also includes provisions concerning contextual advertising and advertising on a publisher's first-party segments.

FTC ANPR

The Federal Trade Commission (FTC) released an Advance Notice of Proposed Rulemaking (ANPR) aimed at consumer privacy and data security. Specifically, the FTC announced that it is exploring rules on harmful commercial surveillance and data security practices, which the FTC broadly defines as the "business of collecting, analysing, and profiting from information about people." It should be noted that the ANPR allows the FTC to "generate a public record" about commercial surveillance practices that are unfair or deceptive under section 5 of the FTC Act, even if the FTC does not move forward with new regulation rules. The ANPR seeks to solicit comments concerning business practices related to data that is collected directly from consumers, personal identifiers (e.g., when a consumer browses the web or opens an app), and the prevention of secondary uses of data, particularly in the context of behavioral advertising. Consumers include "businesses and workers, not just individuals who buy or exchange data for retail goods and services." The ANPR asks for comment on balancing the costs/benefits of a rule on the matter, including whether a rule would encourage or discourage competition. It also posits questions about general consumer harm and harm specifically related to children and teens. The public comment period closed November 21, 2022.

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
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com