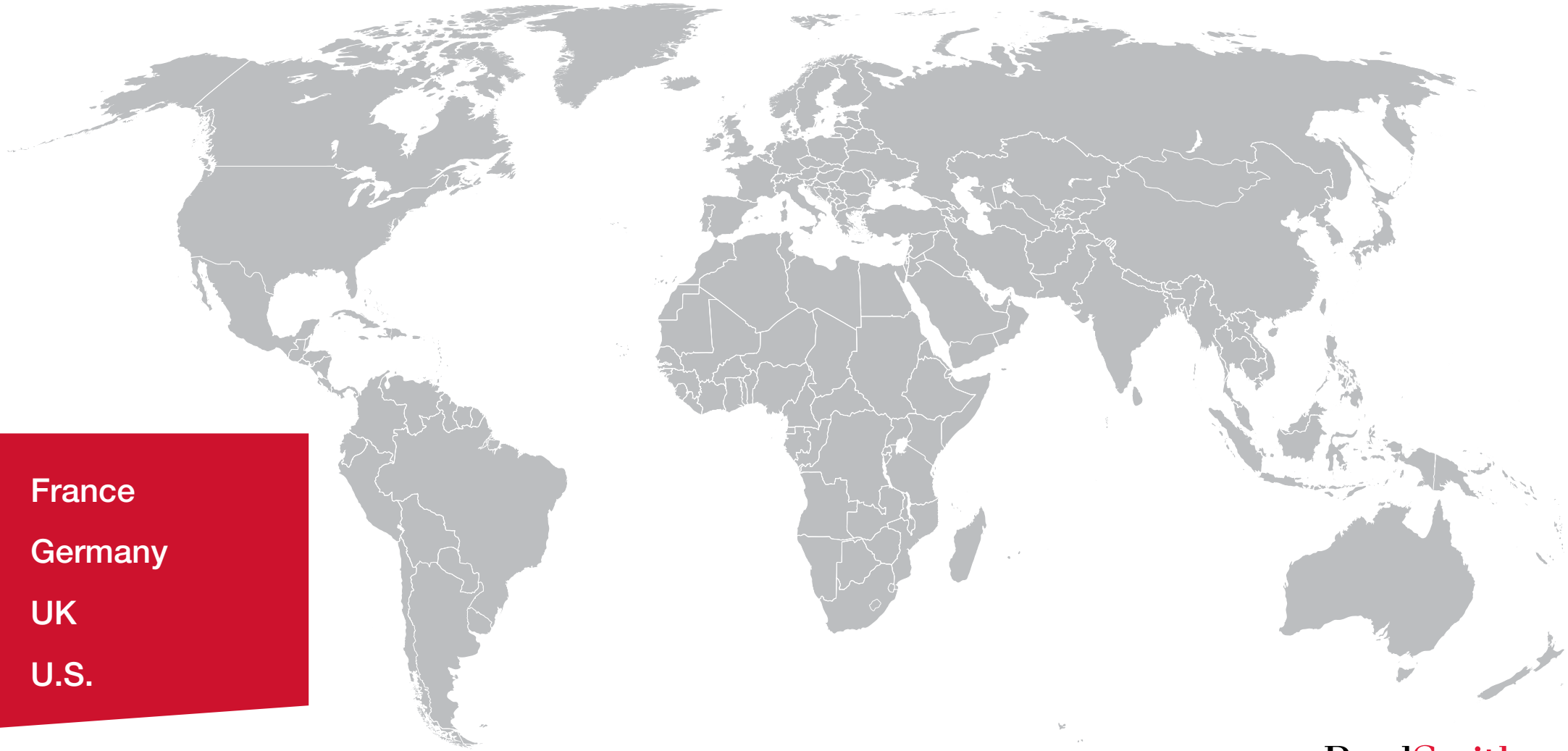
Adtech regulatory round-up
January 2021

This report covers analysis of the key adtech developments we expect to see in 2021 with input from the UK, U.S., Germany and France and with a specific focus on privacy issues. For a look back at adtech developments in 2020, if you missed our December adtech webinar, you can still register to hear a recording here.



France

Germany

UK

U.S.

reedsmith.com

ReedSmith

Driving progress
through partnership

France

by Natasha Tardif and Audrey Augusto

Back to map

New framework for cookies and other tracers

In September 2020, the French Data Protection Authority ("CNIL") published its revised Guidelines and Recommendation on cookies and other tracking devices. The Guidelines set out the law applicable to operations consisting in reading or writing data on users' devices and clarify the CNIL's approach, while the Recommendation aims to guide organisations in their compliance efforts by providing examples of practical methods that can be used, notably to collect consent.

Consent is at the heart of this new framework, and requires an unambiguous positive action from users (e.g. boxes to tick or sliders), and continuing navigation, scrolling down or swiping through a website or app can no longer be viewed as a valid expression of consent. Building on the CJEU's Planet49 decision, the CNIL also specifies that the use of pre-checked boxes will not satisfy this requirement. Another key point to have in mind when setting up cookie management tools is that refusing cookies should be as easy as accepting them (e.g. use of "reject all" buttons). We will see whether these new rules, which require substantial adjustments from all the stakeholders involved, will achieve their objective or lead to 'consent fatigue'.

Cookie walls are no longer prohibited. The CNIL had to revise its guidelines following the decision of the French Administrative Supreme Court, which ruled that the CNIL's guidelines could not impose a general ban on cookie walls. The CNIL, nonetheless, considers that cookie walls are likely to infringe the freedom of consent and will assess their lawfulness on a case-by-case basis.

The Guidelines also provide a non-exhaustive list of cookies exempt from consent. The CNIL adopts a more lenient approach than some of its European counterparts, as it acknowledges that certain audience measurement cookies can be necessary to the functioning of websites or apps and benefit from the exemption. In doing so, the CNIL follows the recommendations issued by the Article 29 Working Party in 2012 and adopts a position in line with the current draft ePrivacy Regulation.

The CNIL announced that all actors would have to comply with the new rules by the end of March 2021 but stressed that it may prosecute certain breaches before the expiry of this grace period, in case of particularly serious violations of the right to privacy. It is therefore recommended to implement the required changes as early as possible.

Enforcement actions by french authorities and consumer bodies

The CNIL reasserted its willingness to use its enforcement powers to prosecute and fine infringements through three recent decisions where it imposed fines totalling 138 million euros. These decisions were also an opportunity for the CNIL to clarify its territorial reach: the CNIL considers that it can prosecute e-privacy infringements committed by foreign data controllers where they have an establishment in France and where the practice at stake was carried out in the context of the activities of that establishment.

In 2021, we expect the CNIL to intensify its enforcement action with respect to digital advertising and to the use of cookies and other tracking technologies. The CNIL already received various complaints from None Of Your Business, which identified potential beaches to cookie rules using the open source extension 'Cookie Glasses' developed by French researchers and from Privacy International with respect to the use of personal data in ad tech.

On the competition side, the French Competition Authority ("FCA") announced that the digital economy would remain one of its top priorities for 2021. It plans to conclude a number of antitrust investigations opened following the publication of its 2018 opinion on online advertising. This notably relates to two pending cases, one on intermediation services in the online advertising sector, and the other one on mass data collection practices.

It is worth recalling that privacy infringements can be tackled under consumer laws as well. Over the recent years, legal action initiated by French consumer organisations against online platforms have led French courts to set aside various provisions of these platforms' privacy policy for being unfair and abusive, notably because they implied that personal data was processed to enhance the services offered to users, where the actual purpose of the data processing was to send targeted adds. French courts also ordered platforms to pay civil damages to the consumer organisations who brought the actions.

Calls for further regulation

In France, like abroad, there have been various calls for further regulation of the main players of the digital market. This relates to the regulation of the largest online platforms, but this is aimed at having a broad impact on the market.

Notably, in February 2020, the French Senate published a draft bill on consumers' freedom of choice online, which is now under review by the National Assembly (French parliamentary body). The bill revolves around three key objectives: ensuring consumers' freedom of choice on their devices, establishing the interoperability of platforms and tackling so-called 'predatory' acquisitions. In particular, the bill provides that OS suppliers should not unduly limit users' freedom to access and share online content and to install third party applications on their device. It plans to grant to ARCEP, the French electronic communications, postal and print media distribution regulatory authority, the power to impose obligations aimed at making online public communication services interoperable. It also includes an obligation for a list of identified 'systemic companies' to notify their planned mergers and acquisitions to the FCA, which could potentially block transactions raising competition concerns.

In June 2020, the Committee on Economic Affairs at the French Assembly published a report on digital platforms calling for an ex-ante regulation of digital 'structuring' platforms in addition to a more extensive reform of competition law. At the French Government's request, the French Court of Auditors and the French Inspectorate General of Finances also published a report in November 2020 on 'Online advertising: for a level playing field', which emphasises that a few players dominate the digital advertising market and calls for further regulation in order to create a level playing field at national level.

These calls sit within a wider context of European legislative initiatives. As part of the European Digital Strategy, the European Commission published in December 2020 two legislative proposals, the Digital Services Act and the Digital Markets Act, which aim at ensuring the protection of the fundamental rights of all users of digital services and at establishing a level playing field in the EU, in particular through the regulation of platforms.

Germany

by Andy Splittgerber and Sven Schonhofen

Back to map

Post Schrems II world

The judgment in Data Protection Commissioner v. Facebook Ireland Ltd., Maximilian Schrems of July 16, 2020 (Case C-311/18; "Schrems II") was the most spectacular data protection judgment in 2020. In its judgment concerning safeguards for transfers of personal data from the EU to a third country, the CJEU held that: (i) the EU-U.S. Privacy Shield Framework was invalided; and (ii) EU standard contractual clauses remain valid, but additional measures might be necessary to ensure an adequate data protection level for the data importer in the third country.

As many adtech providers process personal data of data subjects outside the EU, Schrems II had major consequences for the adtech world. Organisations using services by non-EU adtech providers must conduct a data transfer mapping exercise and determine if sufficient safeguards are in place. There has been fragmentation between German supervisory authorities concerning the question of whether transfers of personal data to the U.S. are still possible after Schrems II. In particular, the supervisory authorities of Hamburg, Berlin and Thuringia apply strict approaches, noting that standard contractual clauses cannot justify a transfer to the U.S. anymore. The Baden-Württemberg supervisory authority on the other hand provided a list of measures in addition to standard contractual clauses that may be implemented (e.g. encryption and contractual amendments such as obligations on the data importer to: (i) inform data subjects of third country data transfers and access requests by supervisory authorities; and (ii) fight data access requests in court). The European Data Protection Board has also released further guidance on additional measures.

The German supervisory authorities commenced enforcing Schrems II towards the end of 2020. Multiple supervisory authorities have sent requests to organisations on potential data protection violations, including: (i) consent procedures for cookies and similar technologies ("Cookies"); and (ii) use of Cookie providers located outside the EU. The supervisory authorities, in particular, asked organisations to stop using non-EU cookie providers if they cannot provide sufficient safeguards for the transfers of personal data after Schrems II.

Developments regarding the transfer of personal data into a third country are still very much in flux. We expect to get additional guidance in 2021 on which additional measures will be necessary for the data transfers, updated standard contractual clauses (a draft was released by the European Commission in November 2020), and likely more enforcement activities by supervisory authorities. While there still are many open questions on how personal data can be transferred after Schrems II, organisations must at least continue to find solutions to be in compliance with the accountability principle under Article 5(2) GDPR.

Enforcement activities regarding cookies

Cookies remain to be the hot topic for supervisory and organisations alike in Germany. Many have moved to Cookie consent management solutions to provide granular opt-in mechanisms for their website and app users. German supervisory authorities were very active in 2020 with reviewing these solutions and providing guidance on the use of Cookies, and will likely continue to do so in 2021.

German supervisory authorities have continued to issue guidance on the use of Cookies. After the "Guidelines for telemedia providers" by the Datenschutzkonferenz, the joint body of all German supervisory authorities ("DSK"), that were released in March 2019, the supervisory authority of Lower Saxony ("LS Authority") has released guidance on how Cookie consent may be obtained. The LS Authority notes that while it appreciates that many organisations are moving to Cookie consent management solutions, it is still necessary to configure these solutions as the Cookies can be used in multiple different ways. The LS Authority provides guidance on the content of Cookie consent language, transparency requirements in Cookie banners with regard to the buttons used, and avoidance of nudging technologies. The DSK has also released guidance on the use of Google Analytics and is of the view that: (i) Google Analytics requires consent; and (ii) Google and the website operators are joint controllers under Art. 26 GDPR, and, thus, require a joint controllership agreement.

Further, Cookie walls remained to be of interest for supervisory authorities. A Cookie wall requires users to accept Cookies in order to use a service. The European Data Protection Board clarified in its guidelines on consent that consent obtained by using a Cookie wall was not valid and genuine consent to Cookies. The German Federal Commissioner for Data Protection, however, confirmed that Cookie-or-pay walls, where the user also has the choice to use a service without Cookies but has to pay a fee, may be permissible.

In addition to the audits concerning the implementation of Schrems II (as described above), the German supervisory authorities have further audited organisations regarding the use of Cookies. The Baden-Württemberg supervisory authority announced in August 2020 a joint Cookie audit sweep, focussing on media organisations and the use of tracking technologies. The LS Authority released the results of a Cookie audit of small and medium sized organisations in November 2020, criticising, in particular, insufficient information for users to make informed consent decisions (in particular in the first layer of Cookie consent management solutions that have multiple layers) and the use of nudging technologies.

Case law regarding cookies

The German courts have provided some further guidance on the use of Cookies. In its "Planet49" decision of May 28, 2020 (case I ZR 7/16), the German Supreme Court confirmed that pre-ticked checkboxes do not constitute sufficient consent for Cookies. In its judgment of September 15, 2020, the Regional Court Rostock (case 3 O 762/19) applied the decision of the German Supreme Court and ruled that a Cookie banner with pre-ticked checkboxes for different Cookie categories (strictly necessary, preference, statistics and marketing Cookies) did not constitute lawful consent. These two judgments highlight that opt-out consent is no longer sufficient.

Legislative update

The ePrivacy Regulation, including its provisions on Cookies and spamming, was supposed to enter into force in tandem with the GDPR in May 2018. However, the Council of the EU still could not agree on its approach. Now it is up to the Portuguese presidency to move the ePrivacy Regulation across the finish line. It published another draft on January 5, 2021, which marks the 14th draft since the initial draft in January 2017. Substantive amendments were made in the latest draft to "simplify the text and to further align it with the GDPR". It remains to be seen if the Regulation will be finalised in 2021. If so, organisations will still likely have at least a one year grace period to get ready.

In parallel, the German government attempted to update national Cookie provisions by introducing the Telecommunication and Telemedia Privacy Act (Telekommunikations-Telemedien-Datenschutz-Gesetz, "TTPA"). Under the TTPA, the use of Cookies required either consent, technical or contractual necessity. Legitimate interests were not considered a legal basis. However, the TTPA has also failed as there was no consensus reached. The German government has now updated the German Telemedia Act, but refrained from clarifying the Cookie provisions therein.

UK

by Elle Todd, Ross McKenzie and Tom Gates

Back to map

Brexit

The extent to which the end of the transition period for the UK's withdrawal from the EU will see a material change in regulatory approach to adtech issues in the UK is not yet clear. As 2021 starts we do at least know, however, that the UK-EU Trade and Co-operation Agreement, brokered at the last hour, means that entities looking to transfer personal data from the EU to the UK, have a further six month grace period in which to prepare compliant transfer agreements or other arrangements. This is additional time during which an adequacy agreement may now be finalised between the EU and UK. Something that was all too faint a glimmer of hope as to be pretty much unthinkable previously, its mention in the Trade and Co-operation Agreement now seems to bring it into the realm of possibility if you can stomach another half year of negotiations and waiting that is. Even if this does not happen, companies relying on model clauses for transfers from the EU to the UK for adtech arrangements should at least be able to use the revised versions published by the European Commission in late 2020 and expected to be finalised in the first few months of 2021. It remains to be seen whether similarly updated model clauses will be published by the Information Commissioner's Office, tailored for transfers outside of the UK. This is very unlikely to happen in the short term, given that the Trade and Co-operation Agreement prohibits the UK from doing so during the six month grace period.

Privacy and electronic communications regulations

One immediate impact of Brexit is that the snail like pace of the revised Electronic Privacy Directive (implemented in the UK by Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), and which currently includes specific rules around cookies and direct marketing email, SMS and phone) means the new ePrivacy Regulation, which will replace the Directive, won't need to be implemented by the UK when it is finally agreed. We still don't know when it will be finalised and what will end up making the cut, but the unpopular proposals around further restrictions on metadata and extension of direct marketing consent rules to wider technologies are unlikely to be pined after. Below, our German colleagues provide a status update on the ePrivacy Regulation for EU member states.

Data protection act changes

Signs of a potential new path for the UK on adtech regulation seemed to show in September 2020 with reports of a potential 'rewriting' of the UK's Data Protection Act 2018 to be more 'pro tech'. Initial reactions from industry were not all positive however, given that any departure from an EU position could jeopardise future adequacy decisions from the European Commission and, specifically, international companies of course already have to comply with EU laws and therefore there is often little relief presented by more national differences. As a result, it seems most likely that such proposals will have little real impact on compliance issues around adtech. Instead we expect that the focus will be more on innovation and data sharing in the context. It is also worth flagging that, in parallel with such chest beating about lightening the load of data compliance, we saw separate consultations around the Data Protection Act 2018's rights for consumer bodies to bring actions on behalf of data subjects with the government calling for views from companies on whether such rights and options should in fact be further extended. That could be a worrying sign for many.

New ICO codes of practice

Companies received a pre-Christmas gift when the ICO published its Data Sharing Code of Practice on 17 December 2020. It will come into force in early 2021 and, as a statutory code, the ICO (and the courts) will take compliance into account when considering any enforcement action. The document isn't greatly changed from the draft published in September 2019 but contains various documentation requirements relevant to data sharing between data controllers which will be as relevant in the adtech field as in any other, albeit often harder to implement in practice given the number of players and lack of privity between such players than can existing. The recommendations for detailed data sharing, due diligence and data protection impact assessments (even if the sharing is not high risk) will not be welcome additions to the admin pile but are unsurprising.

The long awaited Direct Marketing Code of Practice is also expected to be finalised and come into effect in 2021 although it is hoped that the provisions in the draft around custom and lookalike audience requirements will be toned down in the final version. For more, see our summary of the draft here.

Finally, the transition period for implementation of the ICO's Age Appropriate Design Code will end with effect from 2 September 2021. With wide-reaching provisions around profiling and data minimisation in service offerings likely to appeal to children up to the age of 18, many organisations will need to spend a lot of time in the months ahead, thinking through product changes for such audiences which may impact advertising and recommendations.

Digital markets unit

Of course, regulatory developments extend beyond privacy too. In 2021, the Government has stated that it will consult on the form and function of a new Digital Markets Unit ("DMU") to introduce, maintain and enforce a new code of conduct for online platforms with strategic market status. The formation of the DMU, which is expected to sit within the Competition and Markets Authority ("CMA"), follows on from the findings of the CMA's market study into online platforms funded by digital advertising, published in July 2020. That report identified a number of concerns in relation to the largest platforms funded by digital advertising, including concerns over their ecosystems, leading to weak competition in online advertising, and consumers giving up more data than they would like. This report was followed up with work by the Digital Markets Taskforce, led by the CMA, the ICO and Ofcom, which made a series of recommendations to the UK Government in December. The focus is on large platforms with strategic market status, which will face a number of additional interventions, from a code of conduct to stop exploitation of customers and exclusion of competitors, to pro-competitive interventions, such as requiring interoperability and data sharing, to specific merger rules for firms with strategic market status. The CMA recently announced its intention to investigate proposals by Google to remove third party cookies from its browsers, replacing the functionality with a Privacy Sandbox instead, and the potential impact of such changes on smaller advertisers.

Case law and enforcement

2020 did not see any material enforcement action by the ICO in the realm of adtech, which is surprising given its interim report published in June 2019 on the same topic. Instead, fines continued to be focused on direct marketing and security incidents. Even the ICO's key investigation in relation to data broking and resultant enforcement notice against Experian specifically carved out online marketing services. In fact, this lack of action led the ICO to come under fire in November of 2020 with the Open Rights Group announcing that it would sue the ICO for such failure. Subsequently, we have seen the ICO continue to make it clear that it is investigating participants in the online advertising industry separately. Therefore 2021 is anticipated to be the year in which we may see both the results of action by and against the ICO in relation to adtech enforcement. Things could get interesting!

U.S.

by Sarah Bruno and Casey Perrino

Back to map

California consumer privacy act

In the U.S., 2020 began with companies grappling with the impact that the California Consumer Privacy Act ("CCPA") would have on digital marketing. While the CCPA went into effect on 1 January 2020, its enforcement did not begin until July 2020, which gave some companies a much needed window to continue to take steps to establish systems for compliance.

In particular, the CCPA's "Do Not Sell" provision was the biggest hurdle for many organisations, as it requires companies to allow California consumers to opt-out of the sale of their personal information to third parties. The CCPA defines the term 'sale' broadly to cover essentially any transfer of personal information to another party "for monetary or other valuable consideration". There has not been much guidance to date on what constitutes a 'sale' under the CCPA. In the adtech space, a 'sale' might arise via the exchange of a Californian resident's data from pixels or metatags through ad exchanges or other programmatic advertising. This implicated much of the adtech industry, and companies had to develop creative solutions to enable opt-outs, to find other ways of collecting information, or de-identify data prior to sharing with third parties to avoid the opt-out requirement. Companies also took steps to negotiate new contracts or amend existing ones to incorporate language to make the transfer fall within the CCPA's "service provider" safe harbor. If the data flows to a service provider, that processes personal data subject to a written agreement that limits the service provider's use of the data to the provision of services for another company, the CCPA does not consider such an exchange to be a sale and therefore negating the need for an opt-out with regard to that exchange. Many companies whose types of data exchanges allowed them to, took advantage of this "service provider" safe harbor and amended contracts to ensure there was no sale and avoid the onerous work of developing a compliant system for consumers to opt-out.

We also saw industry players get involved with technical solutions to the "Do Not Sell" compliance challenge. For example, the Digital Advertising Alliance developed a 'CCPA tool' that enables consumers to click on an opt-out, notifying all participating companies that the consumer has requested to be removed from the sale of data. Similarly, the Interactive Advertising Bureau developed the 'CCPA Compliance Framework for Publishers and Technology Companies'. The framework includes a master agreement as well as technical specifications to facilitate CCPA compliance through ad exchanges.

In July, enforcement of the CCPA by the California Attorney General began, though a steady stream of lawsuits were filled in California with CCPA claims since 1 January 2020. These cases mainly fell into three categories: data security breaches (brought under the CCPA's limited private right of action), data privacy requirements (under various CCPA provisions), and miscellaneous references to the CCPA (many falling under Section 17200 of California's Unfair Competition Law statute which prohibits unfair and deceptive business practices). By way of example, a number of cases were filed against Zoom Video Communications, alleging that the company did not notify users that their personal information was being disclosed to unauthorised parties like Facebook, in violation of Section 1798.110 and 1798.115. And in Hayden v. The Retail Equation, Inc. and Sephora USA, Inc, Case No.8:20-cv-01203 (07/07/20), the plaintiff alleged that the defendant violated privacy rights under Section 17200 by collecting the plaintiffs' personal information without "consent or knowledge". The plaintiff alleged that the defendant's utility of this information is far outweighed by the damage its collection caused to the plaintiff. This is notable for companies in the digital advertising space, as cases like Hayden indicate that plaintiff attorneys are evaluating whether consumers are provided the appropriate notice and choice under CCPA and making creative arguments under California unfair competition laws. The remaining types of litigation fall under the miscellaneous requirements under the CCPA, such as the notice and opt out requirements. Whether or not these cases make it past summary judgment or motions to dismiss is another story, as the CCPA does not currently provide a private right of action for many of the types of CCPA violations alleged in these lawsuits.

California privacy rights act

As if that was not enough, California ended the year with a new regulation that will serve to be another (and perhaps higher) hurdle for the adtech industry: the California Privacy Rights Act ("CPRA"). On 3 November 2020, Californians voted to approve Proposition 24, a ballot measure that created the CPRA, which amends and expands the CCPA. Concerning the adtech space in particular, the CPRA expands the opt-out right to include the "sharing" of personal information for cross-context behavioural advertising, which will require companies to conduct even further analysis and inventory on the nature and purpose of their data exchanges. The sharing of personal information for first-party (non-personalised) advertising does not require the opt-out, but sharing personal information to facilitate personalised cross-contextualised behavioural advertising will require the opt-out. Most of the CPRA's substantive provisions will not take effect until 1 January 2023, providing covered businesses two years to get into shape. Once operative, the new law will apply only to personal information collected after 1 January 2022. As with the CCPA, we can expect the adtech industry to develop new tools in the coming years to be ready for the CPRA's new requirements with regard to sharing personal information for purposes of cross-context behavioural advertising.

A federal privacy law?

Finally, in the wake of updates to California's privacy law, and the enactment of other state privacy laws this year, it is more possible now than ever before that Congress will take up a federal privacy law in the near future. A number of Federal Trade Commission ("FTC") commissioners have previously testified before Congress in support of federal privacy legislation, and there appears to be bipartisan support for such a bill. While none of the privacy laws that have been proposed in the past few years have gained traction, the growing patchwork of conflicting privacy legislation in the U.S. and hot-button issues such as contact tracing during the COVID-19 pandemic has led to calls from companies and privacy professionals alike for a consistent stance for data protection compliance.

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.

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

UK

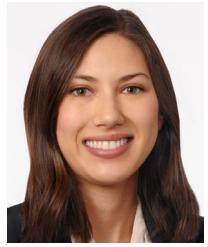
Elle Todd
Partner, London
etodd@reedsmith.com

Ross MacKenzie
Partner, London
rmackenzie@reedsmith.com

Tom Gates
Associate, London
tgates@reedsmith.com

U.S.

Sarah Bruno
Partner, San Francisco
sbruno@reedsmith.com



Casey Perrino
Associate, San Francisco
cperrino@reedsmith.com