What's Ahead: 2024 Digital Economy in the EU & UK

Digital platforms, online content providers and other businesses active in the digital economy face an increasingly complex and evolving regulatory and legal landscape in the EU and UK with privacy and data regulation, online safety, competition and consumer issues increasingly intertwined in the digital sphere, and new regulation such as the EU Digital Markets Act (**DMA**) and Digital Services Act (**DSA**). It is essential to adopt an integrated approach that is consistent across legal areas and is future-proofed so far as possible. Here is our take on key themes this year:

1. **Continuing intensive regulatory reform, which will disrupt how businesses operate:** 2024 will see the implementation of legislation and further consultation on regulation impacting the digital economy. Between the DMA, DSA, AI Act, Data Act, Data Governance Act, NIS2, DORA and Cyber Resilience Act in the EU and the Digital Markets, Competition and Consumers Bill (**DMCC Bill**), Data Protection and Digital Information Bill and Online Safety Act in the UK, 2024 promises to be a year of important regulatory change with significant implications for businesses active in the digital economy.

2. **More aggressive enforcement and higher penalties**: by the European Commission, EU Member States' national competition authorities (**NCAs**) and the UK Competition and Markets Authority (**CMA**). Armed with greater resources, expertise, and enforcement powers, we will see more investigations, pursuit of novel theories of harm, intrusive remedies and substantial penalties.

3. **More private actions**: recent years have seen a significant increase in private proceedings, including class actions, alleging breaches of competition, consumer, and privacy laws. This year, the UK Competition Appeal Tribunal (**CAT**) is hearing *Le Patourel v BT* which is the first opt-out collective action to proceed to trial in the UK. Across the Channel, the DMA is entering the final phases of its enforcement trial and is expected to lead to private litigation as well European Commission investigations. There is also an increase in litigation worldwide in relation to infringement of copyright in the training of AI tools.

4. **Greater coordination between domestic and international regulators**: the increasing intersection of competition, consumer protection, privacy, online safety and data issues is driving greater cooperation between regulators worldwide. In the UK, the Digital Regulators Cooperation Forum (**DRCF**) (formed by the CMA, the Financial Conduct Authority, the Information Commissioner's Office (**ICO**) and Ofcom) is prioritising developing the DRCF AI and Digital Hub, a one-stop shop service for digital innovators, and interacting on key areas of new digital regulation such as the Online Safety Act and the DMCC Bill.

5. **Intensified scrutiny of AI including algorithms, automated decision making and generative AI:** the EU AI Act is the first legal framework for AI in the world. Businesses using AI systems should start preparing for the Act entering into force, including by ensuring human oversight and we expect to see an increase in the number of Chief AI officers.

What's Ahead: 2024 Digital Economy

AI

1. **EU AI Act:** on 2 February 2024, the AI Act was unanimously approved by representatives of the 27 Member States, confirming the political agreement reached in December 2023. The Act was approved by the European Parliament on 13 March with a 523-46 vote and now needs to be formally endorsed by the Council. This is the world's first legal framework for AI and takes a risk-based approach to AI regulation. Most of the provisions will apply from 24 months after the Act enters into force, but provisions relating to prohibited AI will apply from 6 months after the Act enters into force. Other regulations will still apply in parallel, such as the EU GDPR which will continue to police the use of personal data in AI systems.
2. **UK approach:** with the approval of the EU AI Act, hard fault lines are emerging between the UK's non-statutory approach to AI regulation and the rest of Europe. In its March 2023 White Paper, the UK Government confirmed its plans to devolve the work of AI regulation to sector-specific regulators. Despite this, speculation remains that legislation will be introduced at some stage. Regulators are required to base their approach on specific principles, including safety, transparency, fairness, accountability and contestability, and several regulators are revising their guidance on this basis. Meanwhile, central Government initiatives include the creation of an AI Safety Institute to carry out evaluations of advanced AI systems and a central government function to co-ordinate regulatory activity.
3. **New AI agencies:** in February 2024, the EU established the AI Office (within the European Commission), which will provide guidance and assistance in the implementation and enforcement of the AI Act in collaboration with the European Commission and national authorities. The AI Office's role will include monitoring the evolution of the AI sector and risks. This follows the establishment of the first AI regulatory agency in the EU in Spain in August 2023.
4. **Revising the EU Product Liability Directive:** EU policymakers reached a political agreement in December 2023 to revise the Product Liability Directive to cover AI-related risks. The amendments include: (i) redefining "product" to include AI systems, (ii) addressing liability for AI defects, (iii) clarifying supply chain responsibilities and (iv) considering insurance and compensation issues. Member States will have 24 months to implement the revised provisions, suggesting that the local laws may be effective by the end of 2026.
5. **AI Liability Directive:** proposes reforming national fault-based liability systems applicable to claims made by an individual / entity against another individual / entity for faults affecting the AI system responsible for the harm. Currently, it seems unlikely that this Directive will be agreed upon before the end of the current term in Summer 2024.
6. **Generative AI consultations:** interested parties had until 11 March 2024 to respond to the European Commission's two calls for information on virtual worlds and AI. These will inform ongoing work in relation to the AI Act and the development of competition rules in relation to AI. Separately, NCAs in France, Portugal and the UK have publicly engaged with potential competition issues in relation to generative AI and foundation models.
7. **AI & copyright study:** the collecting societies GEMA (Germany) and SACEM (France) conducted the first global study on AI's impact on music, which concluded that 35% of creators currently use AI and 71% are concerned about loss of income. 95% of GEMA and SACEM members supported a requirement for AI providers to disclose when they use copyrighted works as training data.
8. **AI & copyright:** in July 2023, international associations in the music sector sent an open letter to policymakers proposing seven principles for AI regulation: (i) uphold creators' and performers' rights, (ii) provide licensing for AI exploitation, (iii) avoid exceptions for text and data mining without opt-out, (iv) credit authors and performers in AI exploitation, (v) enforce transparency obligations, (vi) hold AI companies liable for rights infringement and (vii) policymakers must clarify that fully autonomous works generated by AI cannot enjoy the same level of protection as works created by humans.
9. **Generative AI and copyright:** in September 2023, the European Publishers Council unveiled Global Principles for AI, which aim to preserve publishers' capacity to produce quality content and to foster responsible AI innovation. Subsequently, a group of French online service publishers issued a position paper emphasising the need for negotiated licenses to safeguard authors against generative AI data and text mining. In January 2024, the CSNP of the French National Assembly released an opinion which calls for an amendment to the EU Copyright Directive to create a stronger framework for the use of AI, the development of an international AI treaty and regular evaluations of the EU AI Act.

Key cases / cases to watch

New York Times v OpenAI: filed in the US, alleging that the training of Open AI infringed New York Times copyright.

Getty Images v Stability AI: filed in the US and UK, alleging that Stability AI's Stable Diffusion system that generates images infringed copyright by using Getty images as data inputs for training purposes.

OQ v Land Hessen and SCHUFA: the CJEU expanded the EU General Data Protection Regulation (**GDPR**) restrictions on automated decision-making, profiling and AI, ruling that credit scoring constitutes automated decision making and is subject to Article 22 GDPR.

Thaler v Comptroller-General of Patents, Designs and Trademarks: on 20 December 2023, the UK Supreme Court unanimously dismissed an appeal to allow an AI machine (DABUS) to be named as a patent inventor on the basis an "*inventor*" must be a natural person.

Consumer group BEUC complaints against Meta's "pay or consent" model on Facebook and Instagram: BEUC's view is that Meta's dominant position makes it hard for consumers to switch and therefore have a genuine choice about whether to consent.

Fines for breaching GDPR: the Italian Data Protection Authority fined the local government of Trento EUR 50,000 for conducting two research projects involving the deployment of AI systems which did not comply with EU GDPR requirements. There are also ongoing investigations into OpenAI's "Sora" and ChatGPT.

What's Ahead: 2024 Digital Economy

Data and privacy

1. **ICO consultation on generative AI:** in January 2024, the UK ICO launched a consultation series examining how aspects of UK data protection law should apply to the development and use of generative AI. The first chapter of the consultation series focuses on the potential lawful bases for training generative AI models on personal data scraped from the internet.
2. **ISO consultation on employment guidance:** the ICO is also consulting on draft employment guidance on (i) collecting and keeping employment records and (ii) recruitment and selection of candidates. The recruitment guidance specifically addresses the use of AI in an employment context: it suggests that it is "good practice" for the overall decision about whether to recruit a prospective employee to be made by a human. It also provides links to key considerations around the use of AI, including algorithmic fairness and issues of bias. Data protection issues in the past year have continued to centre on data subject access requests and employee monitoring. The guidance promises to provide practical help for organisations in relation to these issues. However, challenges remain particularly in connection with hybrid work arrangements where monitoring of personal devices may be undertaken.
3. **Data Protection and Digital Information Bill:** UK data protection law is set to change this year with the progression of the Data Protection and Digital Information Bill through Parliament and there is still much debate as to whether the UK is going to produce separate legislation governing the use of AI. Although the current draft legislation does not include any specific additional rights for data subjects in the UK (indeed its aim is to reduce the burden on data controllers in the UK), experience indicates that legislative change in the field of information law is usually accompanied by an increased awareness of individual rights which manifests itself in an increase in claims for misuse of data. In-house legal teams should keep abreast of these legislative developments but the best mitigation for such claims is usually robust first line processes for dealing with data subject requests, making sure they are identified and dealt within following statutory time periods.
4. **EU Data Act:** the EU Data Act entered into force on 11 January 2024 and is a key part of the European data strategy. It works closely with the Data Governance Act, which became applicable in September 2023. While the Data Governance Act regulates processes and structures that facilitate voluntary data sharing, the Data Act clarifies who can create value from data and under which conditions. Together, these two acts will facilitate reliable and secure access to data, fostering its use in key economic sectors and areas of public interest. They will also contribute to the establishment of an EU single market for data, ultimately benefiting both the European economy and society at large. The Data Act makes more data available for the benefit of companies, citizens and public administrations, through means such as (i) improving the transfer of data between data holders and data users while upholding its confidentiality; (ii) mitigating the abuse of contractual imbalances that impede equitable data sharing; and (iii) creating rules enabling public sector bodies to access and use data held by the private sector for specific public interest purposes.
5. **European Health Data Space Regulation:** in March 2024, the European Parliament and Council reached a provisional agreement on a new law making it easier to exchange and access health data at an EU-level, as well as giving individuals greater control over how their data is used.
6. **Continued challenges for data breach actions in the UK:** last year, the High Court struck out *Prismall v Google / DeepMind* which was an opt-out claim brought against Google and its subsidiary DeepMind for alleged misuse of private information in relation to its data sharing agreement with the Royal Free Hospital London. The High Court found that no entitlement to more than trivial damages could be identified on a representative basis. This illustrates the continuing challenges faced by data breach claims in the post-*Lloyd v Google* environment and the need for representatives to show each member of the class has the same interest. The Court of Appeal has granted permission to appeal.
7. **Scope for biometrics actions:** in the US, there have been an increasing number of class actions relating to biometrics in recent years, prompted by laws introduced specifically addressing the collection and use of biometric data by companies. While the legislative framework is different, the enforcement action taken by the UK ICO against Serco Leisure's use of biometric data earlier this year is an example of the potential scope for biometrics claims to be brought by affected individuals.

Key cases / cases to watch

Prismall v Google / DeepMind: the Court of Appeal will hear an appeal against the strike-out of this data breach action in September this year.

Equiniti claim: claim filed in connection with police officers' pension benefit statements being mistakenly sent to incorrect addresses. In February 2024, the High Court struck out all but 14 of the 474 claims on the basis there was no evidence that they were viable. The remaining claims, if they proceed to trial, may further clarify the "*threshold of seriousness*" requirement for data protection claims.

Gormsen v Meta: claim filed on behalf of 45 million Facebook users in the UK that Meta abused its dominant position including by imposing unfair and excessively complex (and unavoidable) terms and conditions with respect to how users' personal data is utilised. After refusing in February 2023, the CAT has now certified the claim. The decision to certify is a useful reminder of the low-bar for certification in such cases and the possibilities of novel theories of harm in collective proceedings before the CAT.

Record fine for GDPR breach: in May 2023, the Irish Data Protection Commissioner fined Meta EUR 1.2 billion for breaching GDPR requirements on international data transfers when transferring personal data from the EU to the US in connection with delivering its Facebook service. This significantly exceeds the previous highest fine of EUR 746 million, which was imposed on Amazon in 2021.

Record fine from Italian Data Protection Authority: in February 2024, the Garante Privacy imposed a fine of more than EUR 79 million on Enel Energia for failing to protect its databases from access by unauthorised agents, which had "*fuelled… nuisance calls*" etc for years.

What's Ahead: 2024 Digital Economy

Online Safety

1. **UK Online Safety Act 2023:** is being brought into force. The Act aims to protect children and tackle illegal online content. Ofcom (which will regulate online safety) anticipates that, ultimately, more than 100,000 online services could be in scope, with the biggest impact expected to be on social media, messaging, search and online advertising services. The duty of care which a provider must exercise depends on the nature of the provider, the nature of the material in question and whether it is likely to be accessed by children. Video-sharing platforms (**VSPs**) will be in scope regardless of where they are based. Providers will also be obliged to take more responsibility for fraudulent advertising appearing on their platforms. The Act will lead to an increase in regulatory investigations into social media firms and, in due course, civil claims against platforms.
2. **EU Digital Services Act:** alongside the DMA, the Digital Services Act (**DSA**) aims to create a safer digital space protecting the fundamental rights of all users of digital services. The DSA became fully applicable in February 2024 and applies to intermediary service providers providing services in the EU (regardless of where they are located). The DSA rules are intended to increase transparency and help to prevent illegal or harmful online content, including scamming activity. There are five sets of rules under the DSA, with specific rules for hosting intermediary service providers, online platforms, platforms facilitating distance selling and very large online platforms (**VLOPs**) and very large online search engines (**VLOSEs**). While the DSA and UK Online Safety Act have broadly the same core aim, there are material differences between the two Acts so companies providing digital services in both the EU and UK will need to consider the two regimes in parallel.
3. **Intersection with other areas:** online safety (particularly in relation to minors) often intersects with areas such as privacy and consumer protection. These cases may raise issues about which regulator has jurisdiction and it is possible we will see parallel investigations relating to the same conduct. For example, the Italian NCA and Italian Communications Authority recently debated which had jurisdiction to investigate TikTok for breaches relating to the protection of minors and vulnerable people.

Cyber security

1. **Cyber threats:** are now recognised as a significant risk to many companies and the UK Government is keen to improve cyber resilience across the UK economy. Directors' duties have been governed by the same legislation in the UK for the past 18 years, but rapid change is under way. Directors are now expected to have sufficient cyber knowledge, or have access to experts, to keep up with the latest threat landscape and demonstrate effective risk management. A new cyber governance code (see the UK Government "call for views" launched in January 2024), which will bring together the critical governance areas that directors need to deal with and formalise expectations of directors in this area is expected this year.
2. **New Product Security Law in the UK:** from 29 April 2024, manufacturers of consumer "smart" devices (and companies in the supply chains) must comply with new UK law.
3. **Draft Code of Practice on Cybersecurity Governance:** the UK Government's consultation on the draft Code closed on by 19 March 2024. There are five principles around which the draft code is structured: (i) risk management; (ii) cyber strategy; (iii) people; (iv) incident planning and response; and (v) assurance and oversight.
4. **NCSC-A report on the near-term impact of AI on cyber-threats:** concludes that AI will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years.
5. **Regulation to improve resilience of data infrastructure:** has been consulted on by the UK Government, with a focus on third party data centre services, their threat management and resilience, and a perceived lack of cooperation.
6. **Deadline for implementing NIS2:** EU Member States have until 17 October 2024 to adopt legislation to comply with NIS2, which supersedes NIS. NIS2 will apply to more sectors than NIS, and its remit covers more medium and large sized companies. It will also enhance enforcement, strengthen security requirements, and is intended to create more enabling governance between Member States.
7. **EU Cyber resilience Act:** aims to ensure that products with digital features are secure to use, resilient against cyber threats and provide sufficient information about their security properties. It was approved by the European Parliament in March 2024. In parallel, the resilience of the financial sector has received regulators' attention worldwide with initiatives, such as the EU Digital Operational Resilience Act (**DORA**), designed to maintain stability and protect consumers by enhancing financial firms' resilience to pre-empt, withstand and recover from disruptions. With significantly compressed implementation timelines converging in 2025, financial entities and third-party service providers must focus on the key steps needed for compliance with the regulations and better management of third parties.

Cases to watch

TikTok's alleged breach of the DSA: in February 2024, the European Commission opened formal proceedings against TikTok to determine whether it has breached the DSA in areas linked to the protection of minors, advertising transparency, data access for researchers and the risk management of addictive design and harmful content.

Fines for failing to protect minors and vulnerable people: the Italian NCA recently fined TikTok EUR 10 million for breaching the consumer code relating to the protection of minors and vulnerable people. The Italian NCA also fined British American Tobacco and Amazon a total of EUR 7 million in February 2024 for not providing consumers with sufficient information in advertisements about the nicotine content and associated health risks for heated tobacco products and that they are not intended for use by minors.

What's Ahead: 2024 Digital Economy

Consumer law

1. **Unfair commercial practices:** in the UK, the DMCC Bill will restate consumer protections against unfair commercial practices in primary legislation and grant the Government the power to amend the list through secondary legislation. We also expect increased enforcement in EU Member States, particularly in France, Germany, Italy and Spain.
2. **CMA's enforcement powers:** for the first time, the CMA will be able to directly enforce UK consumer protection laws through administrative proceedings, akin to its powers to enforce competition law and to fine companies up to 10% of their global turnover and individuals up to GBP 300,000.
3. **Fake reviews and drip pricing in the UK:** in September 2023, the UK Government consulted on how to improve price transparency and product regulation for consumers. In January 2024 the Government published its response and announced plans to add specific banned practices to tackle fake reviews and drip pricing to the DMCC Bill.
4. **Subscription traps in the UK:** new obligations will clarify and strengthen pre-contractual information given to consumers and nudging obligations to avoid so called subscription "traps".
5. **EU "right to repair":** on 1 February 2024, the European Parliament and the Council reached a political agreement to introduce rules that will grant European consumers the right to have common household appliances repaired after the warranty has expired. The "*right to repair*" will apply to products that fall within scope of the European Commission's ecodesign framework, including common household products such as washing machines, dishwashers, vacuum cleaners, electronic displays, servers and data storage products, and smartphones. In addition, manufacturers will be required to publish details regarding their repair services and the prices for repair. Member States will also be required to provide for at least one national platform to match consumers with repairers, including a search function to find sellers of goods subject to refurbishment and purchasers of defective goods for refurbishment.
6. **Supply Chain Sustainability Due Diligence Law:** approved by the European Parliament's Legal Affairs Committee in March 2024. The law will require companies to address their negative impact on the environment and human rights across their supply chains. The European Parliament now needs to vote on the legislation.

Ex ante regulation

1. **EU:** the DMA is designed to ensure fair and contestable markets, which should deliver a competitive and level-playing field in the digital sector. It enables the European Commission to designate companies as gatekeepers. The first designations were announced in September 2023, with Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta and Microsoft being designated as gatekeepers in relation to core platform services. These gatekeepers had until 6 March 2024 to ensure compliance with the DMA. The list of obligations includes provisions concerning: (i) prohibitions on combining data collecting from two different services belonging to the same company, (ii) the protection of platforms' business users (including advertisers and publishers), (iii) self-preferencing methods used by platforms for promoting their own products, (iv) pre-installation of certain services, (v) bundling practices and (vi) interoperability, portability and access to data for businesses and end-users of platforms. More details on the types of obligations are available in our January 2024 briefing.
2. **EU Member States:** in addition, several EU Member States have introduced regulation at a national level: for example, Germany and Italy. Companies may therefore face parallel investigations even within the EU.
3. **UK:** the DMCC Bill, which is expected to receive the Royal Assent in the coming months, will implement the UK Government's digital markets strategy, including tailored codes of conduct for designated firms and the ability for the CMA to impose pro-competition interventions. The DMCC Bill will also give the CMA a new suite of enforcement powers to regulate SMS firms, including penalties of up to 10% of annual global turnover (or 5% of daily turnover) for SMS firm's breaches of conduct requirements, as well as potential director disqualification. SMS firms will also be subject to a mandatory and suspensory reporting regime for certain transactions where the consideration exceeds GBP 25 million.
4. **Interplay between competition law and enforcement of ex ante digital regulation:** the European Commission is the sole regulator which can enforce the DMA, but the DMA envisages cooperation with NCAs in the EU Member States. The European Commission has indicated that NCAs may investigate alleged non-compliance and report their findings to the European Commission. Depending on how the NCAs perceive their role, we may see more antitrust investigations being opened. In addition, the DMA only regulates specific activities and conduct so competition enforcement will continue in parallel.

Cases to watch

Consumer class actions in the UK CAT: alleging app stores have misused their market power and engaged in unconscionable conduct by restricting distribution and imposing a 30% commission. Hearing scheduled for March to July 2024.

Booking.com a potential gatekeeper under the DMA: in March 2024, Booking.com notified the European Commission that it may meet the thresholds for designation under the DMA. The European Commission has until 13 May 2024 to review the notification. If designated, Booking.com will then have six months to comply with the DMA.

Challenges to "gatekeeper" designations under the DMA: (i) Meta is challenging the inclusion of its Messenger and Marketplace services; (ii) ByteDance challenged its classification as a social network and argued it does not meet the revenue threshold but in February 2024 the EU General Court rejected ByteDance's arguments; and (iii) Apple is seeking the re-classification of its core platform services, arguing each version of its operating systems serves distinct purposes.

What's Ahead: 2024 Digital Economy

Competition & foreign investment

1. **Closer scrutiny of transactions:** both the EU DMA and UK DMCC Bill introduce requirements for designated companies to inform regulators of a wider range of transactions than before. Investments may also be caught by national foreign investment regimes. These factors coupled with the heightened interest in mergers in the digital sector by competition regulators worldwide mean that companies will need to carefully consider the potential impact on deal timelines. Regulators are increasingly making use of powers to call in transactions which do not meet the notification thresholds, including the European Commission reviewing transactions which do not meet the notification thresholds in any EU Member State. Companies should also be mindful of the risk of regulators reaching different conclusions on remedies.
2. **Foreign investment:** in addition to merger control, investment in digital activities may be reviewed under national foreign investment regimes, with semiconductors, digital infrastructure and AI being areas of particular interest from a national security perspective. Several jurisdictions (including the EU and USA) are also contemplating restrictions on outbound investment, with the EU proposals focusing on investments in advanced semiconductors, AI, quantum technologies and biotechnologies.
3. **EU Technology Transfer Block Exemption (TTBER):** provides a safe harbour under EU competition law for technology licensing agreements that meet certain criteria. It is due to expire on 30 April 2026. The European Commission has published the responses to its 2023 consultation: most respondents indicated that the TTBER continues to be relevant, but that certain areas do not provide sufficient legal certainty (e.g. how the guidelines apply to technology pools, the licensing of Standard Essential Patents and requirements relating to royalties, transparency and essentiality). A further update is anticipated in Q3 2024.
4. **Litigation funding reform in the UK:** an outstanding question since the UK Supreme Court's decision in *PACCAR* last year has been what (if any) legislative intervention there may be. On 20 March 2024, the Government introduced the Litigation Funding Agreements (Enforceability Bill) to overturn the *PACCAR* ruling. The Bill provides that litigation funding arrangements are not damages-based agreements (**DBAs**) and therefore do not need to comply with the 2013 DBA regulations.
5. **Continued broadening of claims in the UK CAT:** class representatives have continued to use alleged infringements of competition law to bring a wide variety of claims before the CAT and make use of its opt-out procedure, often based on novel theories of harm. Certification of the data-related claim brought by Facebook users against Meta (*Gormsen v Meta*) is the latest example of this type of claim being waved through by the CAT.
6. **First settlement in collective proceedings in the UK:** the first settlement was reached in the roll-on roll-off (**RoRo**) claim following on from the European Commission's 2018 decision against major shipping firms (*Mark McLaren v MOL*). The class representative agreed with one of the defendants (CSAV) to settle. As this is a collective action, settlements need to be approved by the CAT and this is the first such judgment. It is a unique set of circumstances but does lay down a process for approval of collective settlements. Crucially, as the claim is ongoing against other defendants, the CAT sidestepped the issues of distribution.
7. **Enforcement activity:** as the DMA and DMCC enter into force, regulators will continue to enforce competition law, particularly the prohibition on abusing a dominant position, given (i) practices (such as tying) which are not directly covered by the DMA and (ii) that the DMA and DMCC requirements will only apply to a small group of companies and activities. There is ongoing enforcement activity by the European Commission, the CMA and several NCAs focused on large digital companies.

Cases to watch

Le Patourel v BT: is the first opt-out competition class action to proceed to trial before the UK CAT. This is likely to provide clarity on the CAT's approach to damages and funder returns, which may impact the class action landscape, including by more clearly defining parameters for the potential settlement of outstanding and future claims.

UK Court of Appeal hearings of litigation funding challenges: the CAT has upheld the validity of several litigation funding agreements that have been amended post-PACCAR (*Alex Neill v Sony; Mark McLaren v MOL; CICC v Mastercard*). It remains to been seen what will happen with these appeals given the introduction of the Litigation Funding Agreements (Enforceability Bill) which is intended to resolve the uncertainty created by *PACCAR*.

Google – Adtech and data-related practices: the European Commission is investigating whether Google has breached competition law by favouring its own online display advertising technology services. A statement of objections was issued on 14 June 2023.

Apple – App Store Practices (music streaming): the European Commission fined Apple over EUR 1.8 billion for abusing its dominant position in the distribution of music streaming apps to iPhone and iPad users through its App Store, including through "*anti-steering provisions*" preventing developers from informing users of alternative, cheaper options. Apple intends to appeal the decision.

Google Shopping: in January 2024, Advocate General Kokott delivered her opinion that the Court of Justice of the European Union (**CJEU**) should dismiss Google's appeal and confirm the European Commission's fine. Google appealed the General Court's decision broadly upholding the European Commission's finding that Google had abused its dominant position by favouring its own comparison shopping services. The CJEU's ruling is expected later this year.

Key contacts

Antitrust, Regulation & Foreign Investment

Nigel Parr
Partner
T +44 20 7859 1763
nigel.parr@ashurst.com

Rafael Baena
Partner
T +34 91 364 9895
rafael.baena@ashurst.com

Anna Morfey
Partner
T +44 20 7859 3006
anna.morfey@ashurst.com

Gabriele Accardo
Partner
T +39 02 85423430
gabriele.accardo@ashurst.com

Fiona Garside
Senior Expertise Lawyer
T +44 20 7859 3269
fiona.garside@ashurst.com

Digital Economy Transactions

Amanda Ludlow
Partner
T +44 20 7859 1294
amanda.ludlow@ashurst.com

Nicolas Quoy
Partner
T +33 (1) 53 53 54 33
nicolas.quoy@ashurst.com

Alexander Duisberg
Partner
T +49 89 24 44 21 149
alexander.duisberg@ashurst.com

Patricia Wade
Expertise Counsel
T +44 20 7859 1031
patricia.wade@ashurst.com

Dispute Resolution

Tim West
Partner
T +44 20 7859 2858
tim.west@ashurst.com

Martin Eimer
Partner
T +49 69 97 11 26 00
martin.eimer@ashurst.com

Jon Gale
Partner
T +44 20 7859 1630
jon.gale@ashurst.com

Rosie Stanger
Senior Associate
T +44 20 7859 2689
rosie.stanger@ashurst.com

Risk Advisory

Julia Spain
Partner
T +44 20 7859 2246
julia.spain@ashurst.com

Matthew Worsfold
Partner
T +44 20 7859 1006
matthew.worsfold@ashurst.com