Linklaters

Tech Legal Outlook 2025

A global perspective

Contents

Introduction

2025 heralds a period of change after a year of elections, with new governments pursuing growth and navigating significant challenges. With rising global tensions and the US-China tech rivalry impacting the sector, the backdrop for businesses is complex.

AI is accelerating digital change, bringing disruption and opportunities, with organisations seeking to harness the potential of AI for competitive advantage. Major tech companies are investing heavily in AI, digital infrastructure and sustainable solutions to AI's growing energy demands.

The regulatory landscape is evolving. Governments are continuing to regulate across digital domains and with new administrations in the US, the EU and the UK, we could see a change in policies. Litigation is increasing, sustaining a heightened risk environment for businesses.

The tech investment outlook is more positive with signs of a recovery in 2024 that could gain momentum in 2025. While investors remain cautious, tech M&A and investment is expected to recover as markets stabilise with political clarity. With record amounts of dry powder ready to be deployed, key areas such as AI, cyber security and defence tech are expected to continue to attract significant investment.

In this publication we explore the key global trends in the technology sector that we believe will shape the legal outlook for businesses in 2025 and beyond.

1.1 Growth in tech M&A and investment

With growth in the value of tech M&A and investment in 2024, there is a more positive outlook for 2025 despite the geopolitical and economic headwinds. The decisive outcome in the US elections has brought more stability to the markets and a post-election bounce in deal-making is expected in Q1 2025.

Tech M&A

In the last three years deal-making has been constrained by geopolitical volatility, persistent inflation, higher interest rates and increasing regulatory intervention. We have seen a fall in tech M&A activity with buyers adopting a more cautious approach to deals with greater attention to due diligence, earlier focus on regulatory risk strategy, and valuation gaps between buyers and sellers.

However, in the first nine months of 2024, the value of global tech sector M&A increased by more than 25% compared to the same period in 2023, reaching level with the full year total for 2023. 2024 has seen the return of a high number of mega deals, including Synopsys' $35bn acquisition of Ansys, the $16bn acquisition of AirTrunk and Hewlett Packard Enterprise's $14bn acquisition of Juniper Networks.

North America accounted for 60% of global tech M&A in the first nine months of 2024, with deal value up 37% year-on-year, underscoring its pivotal role in the tech sector. European deal value was up by 50% year on year and accounted for 17% of global activity. Asia saw a decline in tech M&A value during this period and global market share fell to 20% of the global total.

Tech was the most targeted sector for M&A by corporates and funds in 2024 by value and volume, with software the most targeted sub-sector. We expect that activity in the tech sector in 2025 will continue to outperform other sectors while AI and digital transformation remain strategic objectives for acquirors.

Tech investment

Global tech investment has shown signs of recovery in 2024. While deal volumes have fallen, the value of investment was up by 10% year on year at the end of the third quarter and total annual investment is on course to exceed the previous year's investment for the first time since the record highs of 2021.

The US has driven this uptick in global tech investment and AI has been key. AI companies account for a growing share of new unicorns and the largest funding rounds including ByteDance ($9.5bn), xAI ($6bn) and Anthropic ($4bn).

With growing investment in digital infrastructure, data centre operator Vantage ($9bn) and cloud infrastructure platform Coreweave ($8bn) secured some of the largest funding rounds in 2024. Big Tech is predicted to spend $1trillion on AI in the coming years, with companies in the infrastructure layer likely to be key beneficiaries: from those designing and producing chips to data centre operators and power utilities.

More broadly in the tech sector, we have seen a flight to quality in a challenging market with some businesses doing well and others running out of cash. Beyond AI and digital infrastructure, other tech verticals that have performed better include cyber security, defence tech, climate tech and more recently, fintech.

With rising global tensions, conflicts in Ukraine and the Middle East and a focus on national security, we expect defence tech and dual-use tech to attract increasing investment. And while the energy transition faces a setback with the Trump presidency, progress continues and there is a positive long-term outlook for climate technologies given the necessity of tackling climate change.

Public markets

While US Big Tech stocks reached new highs in 2024, recent tech IPOs have not returned to their previous highs. The number of IPOs increased slightly in Q2 and Q3 2024, but it remains significantly lower than the levels seen in 2021, and we have seen the rise of continuation funds, and the sale of minority interests to give investors a liquidity opportunity.

There is a backlog of companies looking to exit and IPOs remain a key focus. Exchanges are competing to attract IPOs as the market rebounds with the UK, for example, making significant changes to its listing rules

Looking ahead to 2025

Political clarity and stable interest rates should encourage activity, providing momentum to the signs of recovery which emerged in 2024. With record levels of undeployed (and ageing) capital held by venture capital and private equity sponsors, and a backlog of tech companies looking to exit, we expect valuation gaps to narrow, deals to pick up and significant investment in key areas including AI, climate tech, fintech, cyber security and defence tech.

> "Corporates are seeking strategic M&A and investment opportunities to drive growth, leverage AI and gain competitive advantage in what remains a challenging environment."
>
> Derek Tong, Corporate Partner, London

1.2 The US - China tech rivalry intensifies

Geopolitical tensions and a fragmented international order complicate cross-border business. One notable example is the US-China technology bifurcation. The rivalry between the world's superpowers for tech supremacy affects economic development, altering supply chains, restricting trade and investment, imposing controls on data flows, and challenging AI development through national security measures.

The impact of the re-election of Trump in the US

The US-China tech rivalry is likely to intensify with the re-election of Trump who is focused on ensuring America's ability to dominate the tech industry and to win the battle for AI supremacy. He has emphasised restricting exports of critical technologies and implementing tariffs on imports of Chinese goods.

Reshaping global supply chains

Decades of globalisation and the scarcity of various raw minerals and production capacity led to an interconnectivity of tech supply chains across the globe. Now geopolitical tensions between the US and China are prompting multinational companies to reconsider their supply chain strategies to improve their resilience.

This decoupling is primarily being driven by escalating threats of tariffs and renegotiation of trade agreements to favour sustainable domestic production or near-shoring for economic and national security reasons. And this decoupling is already impacting US and China tech champions. Companies must adapt by diversifying their market approach to mitigate risks and/or seizing new opportunities.

A noticeable shift away from China-centric supply models has positioned countries like Vietnam and Thailand as key alternatives for manufacturing hubs, and Southeast Asian tech companies have benefited from inward investment that might otherwise have been directed to China.

Regulatory barriers to tech M&A

Trade restrictions between the US and China have introduced regulatory hurdles affecting cross-border M&A and investment in businesses with critical advanced technologies including AI, semi-conductors and quantum information technologies. Governments across the globe are seeking to protect national interests in these dual-use technologies that can be used for civilian and military purposes. This October, the US issued final regulations implementing an outbound foreign investment programme to further scrutinise investments by firms linked to China. Concurrently, China has introduced export controls on vital minerals but relaxed foreign investment rules.

These dynamics necessitate strategic and financial investors to review and adjust investment strategies to focus on less sensitive sectors or negotiate more deal protections within permitted regulatory frameworks.

Strategic considerations for digital infra, IT and cyber security

A priority area of investment for major tech companies and investors in 2025 will be data centres to meet the growing demands for data processing and storage, and other digital infrastructure considered critical to supporting tech advances and the growing adoption of AI. However, this too is an area being impacted by geopolitical tensions.

For multinationals, location has become a critical factor in assessing the availability and suitability of data storage. This is driven by concerns about data sovereignty and the heightened risk of government intervention in some markets like China – and broader cyber security considerations – due to the inevitability of security incidents such as the recent CrowdStrike failure.

Increasingly, businesses are segregating their tech stack in certain regions with the goal of mitigating perceived threats to their IT systems and operational viability.

Regulation of cross-border data flows

China is perceived to have the strictest regulation of data exports, but recent developments signal a shift in the global norm. China, through reforms in March, is seeking to ease its uniform controls to promote cross-border trade and services. However, the US has moved towards greater regulation with Executive Order 14117, which aims to manage data transfers involving sensitive personal information to countries of concern (including China).

These changes mark critical shifts in global data governance requirements. As regimes bed down in 2025, bringing greater complexity for international operations, businesses must prepare for increased scrutiny and enforcement.

Fragmented regulations on AI

The development of AI will be affected by and largely dependent on each of the trends identified above. We expect a shift in the supply chains which underpin the growth and maintenance of IT architecture essential for AI deployment.

Meanwhile, stringent restrictions on data sharing are starting to impact training of AI models and content management. As the US, China, and the EU develop AI legislation, fragmented regulations pose operational challenges across jurisdictions. Navigating this landscape requires businesses that want to deploy cutting-edge technology to adapt to these diverse regulatory frameworks with robust compliance programmes that allow and protect operational efficiency.

> "US-China geopolitical tensions are redefining the tech industry, necessitating strategic shifts in supply chains, data management, and AI governance as companies navigate increasingly intricate regulatory landscapes and national security demands."
>
> **Alex Roberts, TMT Partner, Shanghai**

1.3 Data Centres and AI: the shape of things to come

Major technology companies at the forefront of AI advances are shaping the future of data centres, driving growing demand for data centre capacity and sustainable solutions to power them. With demand for data centre capacity expected to grow more than threefold within 5 years, we expect significant demand for data centres with more reliable and carbon free power.

The role of nuclear

Data centres require a consistent and uninterrupted supply of power to maintain their vast networks of servers, cooling systems, and other critical infrastructure. To achieve this stability, operators employ a combination of strategies, including on-site power generation and purchasing arrangements with energy providers, of which renewable power is an increasing component.

Nuclear power is emerging as a potential energy source for data centres due to its ability to generate a stable, reliable, and low-carbon electricity supply. Unlike intermittent renewable sources such as wind or solar, nuclear energy can consistently meet the high power demands of data centres without service disruption.

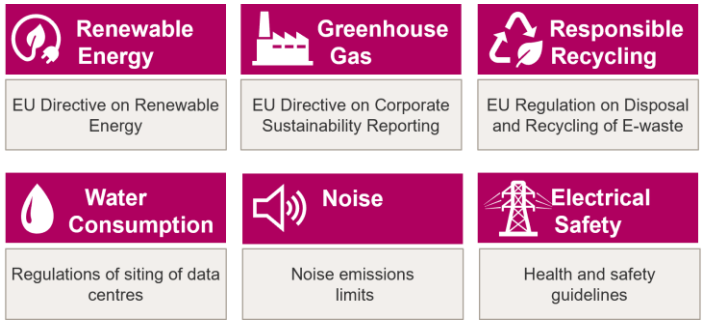
The past year has seen substantial investments in nuclear energy by large technology firms. Examples of this include Microsoft partnering with Constellation Energy to restore the Three Mile Island nuclear plant, and Google and Amazon investing in advances in small modular reactors (SMRs). SMRs are more flexible and can be deployed closer to data centres, mitigating some logistical and safety concerns related to traditional large reactors.

There has also been renewed interest in nuclear fusion technologies, with Microsoft signing a power purchase agreement for the future supply of fusion power with Helion (which is reportedly also in discussion with OpenAI).

Despite its advantages, the use of nuclear power in data centres is not an instant solution and it faces challenges related to high initial capital costs, regulatory complexities, and public perception issues concerning safety and nuclear waste. Widespread deployment of nuclear is still some years away and there are energy demand challenges that will need to be met before then through a range of different power generation and distribution strategies.

Advances in construction and deployment

An ability to quickly deploy new data centres will be vital in managing the growing demand for data processing and storage. The challenges to building data centres are multi-faceted and span regulatory, technical, logistical, and environmental considerations, making the process a complex undertaking. The diagram below shows the main areas of regulation that apply to data centres.



The advantages of building low-latency, edge data centres close to the people that use them can often be frustrated by a lack of suitable land and a pressure on resources. Building data centres in remote areas has its own challenges, not least of all, finding a committed work force. Against this complex construction landscape, data centre operators are looking toward prefabricated and modular construction techniques for better flexibility and speed to market.

Another key technology being integrated into data centres to meet AI demand is liquid cooling. As processors become more powerful, air cooling is often insufficient to manage the heat generated.

Liquid cooling systems, which use coolants to transfer heat away from server components, can significantly reduce the energy required for cooling. However, transitioning to this technology can be resource-intensive, complicated and costly, often making it a barrier for smaller operators.

A project to watch is the world's first GW data centre currently being built in Atlanta, US, which features a modular campus tailored for high-density AI applications and cutting-edge, waterless cooling and highly efficient energy systems. It anticipates saving approximately 664 million gallons of water annually compared to standard data centres. However, the project is so enormous that a mini city will first have to be built to house the staff who will work on it.

As technology continues to advance, overcoming these deployment challenges will be vital in enabling data centres of the future to meet the increasing demands of generative AI workloads without compromising on sustainability goals.

> "Nuclear energy is emerging as a sustainable energy solution for data centres, driven by growing power demand, maturing technology and innovative financing models that make advanced nuclear projects more viable."
>
> Maryam Adamji, Energy & Infrastructure Partner, London

1.4 New beginnings in merger control: a wave of change?

2025 is set to be a year of significant political change on both sides of the Atlantic. This leaves a question mark over the implications for merger control policy. With the last decade characterised by increased scrutiny and intervention rates, we wait to see whether 2025 will have more of the same in store or mark an inflection point.

Merger control trends in 2024

Regulators globally have paid ever greater attention to the tech sector over the last decade: reviewing transactions that previously would have passed without review and probing a broader range of potential issues with such transactions.

The last year has been no different. In keeping with the zeitgeist, European and US regulators have displayed significant interest in the emerging strategic partnerships between the major cloud computing firms and generative AI developers. The UK's CMA has used its flexible jurisdictional rules to review several partnerships (albeit concluding in many cases that it did not have jurisdiction). The Chinese SAMR has also been looking into some of the partnerships in the AI space and paying close attention to the supply of potential AI related products in its merger review.

In the US, the FTC has initiated an inquiry into generative AI investments and partnerships, focusing on major tech players like Alphabet and Amazon, signalling an interest in maintaining oversight over the tech sector's evolving dynamics.

The European Commission has also scrutinised a number of partnerships to establish whether they fall within its merger control powers (or may raise issues under its antitrust powers). However, the Commission's ability to review transactions falling below its conventional turnover thresholds suffered a significant setback when the EU's highest court overturned the Commission's "Article 22" policy in *Illumina/Grail*.

The policy had given it wide ranging powers to review transactions falling below existing jurisdictional thresholds. Member States have sought to close the perceived enforcement gap through new "call-in" powers enabling national competition authorities to refer transactions to the Commission.

In China, the authority has also used its "new" power to call in transactions that are below turnover thresholds but believed to have anti-competitive effects. This has happened in (at least) two instances and both are in the tech space. In other cases, the authority is also applying new analytical frameworks or new theories of harm to take into account the impacts of geopolitics, for example in *MaxLinear / Silicon Motion*.

Looking forward to 2025: a change in regulatory oversight?

The possibility of change is, however, in the air with a range of competition policy initiatives signalled for 2025.

In the EU, there will be a new Commissioner for Competition, Teresa Ribera, after a decade of Margrethe Vestager. Ribera has signalled her support for a number of merger control reforms proposed in an influential report by Mario Draghi, which advocates in particular for the EU's merger review process to afford greater weight to how mergers may enhance innovation.

Ribera has committed the Commission to review the guidelines to assess mergers between competitors, but any changes will not happen overnight. She has also signalled that the Commission needs to find a pragmatic solution for the circumstances in which the Commission can review transactions falling below its turnover thresholds.

In the US, it remains unclear what next steps the FTC will take in relation to generative AI investments and partnerships. The FTC is also pursuing enforcement action through the US courts in relation to other historical deals. This remains a space to watch closely. This also applies to the change in presidency in the US, which may give the green light for M&A activity in certain sectors. However, we anticipate that under the new administration tech companies will likely remain under scrutiny.

In the UK, the CMA has announced a review of its approach to merger remedies, noting that it aims to foster a dynamic economy that rewards innovation and attracts investment. There is no doubt that this will have an impact on the review of tech mergers in the coming years.

In China, geopolitical factors (especially with the new US administration) will continue to play an important role in the Chinese merger control process, both as impacts on competition and on the national economy. The SAMR will continue to use the call in power in particular in the tech sector. The Horizontal Guidelines are also expected to be finalised in 2025, with a consultation draft already foreshadowing a more stringent approach to competition issues than many of the SAMR's overseas peers.

Regulatory vigilance to remain

There is, in sum, much in train that may impact when and how regulators will approach transactions in the tech sector, and beyond, in the coming 12 months. That said, the initiatives suggest more evolution than revolution: we will, however, be keeping a close eye on what more concrete proposals, if and when they emerge, will mean for firms' M&A activity in the sector.

> "Following elections in 2024, new administrations in the US, the EU and the UK could bring a significant shift in competition policies that will shape the tech sector in 2025 and beyond."
>
> William Leslie, Antitrust & Foreign Investment Partner, Brussels

2.1 International data transfers under scrutiny

In 2025, businesses will face a dynamic regulatory landscape where data laws are increasingly influenced by geopolitical tensions. We anticipate heightened scrutiny of international transfers of personal data from the EU, with regulators broadening their focus beyond transfers from the EU to the US, to focus on transfers from the EU to jurisdictions lacking EU adequacy decisions.

The expanding scope of regulatory scrutiny

European data protection regulators are increasingly enforcing stricter compliance with the GDPR for international data transfers. Recent cases against Uber, Meta, and Microsoft have resulted in substantial fines and orders to halt transfers.

With the Data Privacy Framework currently validating transfers to the US, we anticipate that European regulators will begin to place transfers to other major jurisdictions which do not benefit from adequacy decisions under the microscope. We expect regulators will also increasingly scrutinise arrangements where data is localised within the EU but accessed by entities and individuals based in third countries.

Geopolitical tensions and data nationalism

Heightened regulatory scrutiny coincides with an increasingly polarised geopolitical landscape. With an incoming US administration that will likely deprioritise EU interests, we expect European regulators to react by asserting greater control over EU data. This trend towards 'data nationalism' is evident in the EU's Digital Package, particularly with the EU AI Act which represents a stringent regulatory stance on AI, contrasting with approaches in the US.

The UK's stance: a new safe harbour?

The UK's data protection regulator (the ICO) has shown less appetite for enforcing international data transfer requirements, potentially positioning the UK as a more attractive jurisdiction for businesses needing to access European personal data from third countries. This less assertive stance is complemented by innovation-friendly policies in relation to AI, alongside the recent Data (Use and Access) Bill, which would introduce broader grounds for data processing under the UK GDPR.

Key Recent Cases

Uber: The Dutch Data Protection Authority (DPA) imposed a €290 million fine on Uber for inadequate safeguards in transferring EU drivers' data to the US. Uber argued that both its US and EEA entities were joint controllers making the US entity directly subject to the GDPR.

Following guidance from the European Data Protection Board that the 2021 Standard Contractual Clauses (SCCs) are not suitable for transfers of personal data between joint controllers who are both subject to the GDPR, Uber opted not to implement any measures to justify the transfers under Article 5 of the GDPR. However, the Dutch DPA dismissed this argument, emphasising the importance of strict technical compliance with the GDPR when undertaking third-country data transfers.

This ruling, although under appeal, serves as a warning to businesses regarding the increasing appetite of DPAs to investigate data exports to assess whether the detailed requirements regarding data exports have been complied with. The Dutch DPA applied a strict application of the GDPR fining guidance (0.8%-4% of global turnover), despite a lack of demonstrated individual harm.

Microsoft 365: The European Commission relied on SCCs to transfer personal data to Microsoft in the US when using the Microsoft 365 suite of products. The European Data Protection Supervisor (EDPS) found that the European Commission could not explain which types of personal data fell under service-generated data, as Microsoft did not provide a clear schema. Consequently, the EDPS mandated the suspension of all data transfers. Though currently on appeal to the CJEU, an unsuccessful appeal could have considerable impact upon Microsoft and the multitude of businesses that use Microsoft 365 daily.

Longevity of data privacy framework

Several major exporters of data (such as Meta) have been able to rely on the EU-US Data Privacy Framework to continue its transfers once the IDPC order took effect. However, the longevity of the Data Privacy Framework remains uncertain – with the case of *Latombe v Commission T-555/23* being one to watch once a date for the hearing is set.

No longer just a European issue

Data export regimes are proliferating around the world, with new variants of standard data export contracts being published by regulators across the US, LATAM, APAC and Middle East. As a result, the use of such contractual arrangements to legitimise data transfers across a global enterprise group is becoming an increasingly complicated issue.

> “Recent cases have shown that the EU will apply strict interpretations of the GDPR to data exports and compliance with international data transfer rules is not a low-risk box-ticking exercise.”
>
> Julian Cunningham-Day, TMT Partner, London

2.2 The EU's increasing action on online safety

The European Commission (EC) has started to flex its powers under the EU's landmark online safety legislation, the Digital Services Act (DSA). It has issued Requests for Information (RFIs) and initiated infringement proceedings against a number of Very Large Online Platforms (VLOPs), and we expect further regulatory intervention and litigation to follow in 2025 and beyond.

The DSA takes effect

The DSA is designed to enhance platform accountability, manage illegal content and disinformation, improve transparency and safeguard user rights. It imposes obligations on those hosting content and those providing online platforms in the EU (including social media, online marketplaces and search engines).

The DSA started applying to the first VLOPs and Very Large Online Search Engines (VLOSEs) in 2023 and to all other online intermediaries in the EU in February 2024. While the VLOPs and VLOSEs have more extensive online safety obligations and have been in the spotlight to date, all online intermediaries in the EU will need to take steps to ensure they are compliant.

Enforcement and investigations

The EC has wide ranging powers to access information and issue fines under the DSA for the VLOPs. To enable the EC's investigations, key powers include: issuing requests for information (RFIs) to verify compliance, mandating access to data and algorithms, interviewing relevant individuals and inspecting premises.

Non-compliance with the DSA can, among other things, result in: the issuing of significant fines of up to 6% of a platform's global annual turnover; interim measures backed by periodic penalty payments and, if an infringement persists despite enforcement and causes serious harm, temporary restriction of the access to the service concerned; and periodic penalties up to 5% of the average daily worldwide turnover for each day of delay in complying with remedies.

Recent actions by the EC

The RFIs sent to VLOPs have mainly concerned their compliance with various regulatory aspects of the DSA. These include managing illegal content and disinformation, with specific attention to terrorist content and hate speech, as seen in requests sent to platforms such as X. Additionally, the EC has focused on risk assessments and mitigation measures against illegal content spread, consumer protection, and minors' online safety, addressing platforms such as Amazon.

There have also been platform-specific concerns raised such as concerns about Google's systemic risk management. Other areas of focus include online marketplace integrity: concerns with transparency in recommender systems and ad repositories, particularly with platforms like Amazon and concerns regarding illegal content and minor protection seen in requests to, for example, Pornhub.

Formal proceedings and litigation

The EC has opened a number of formal infringement proceedings against VLOPs based on the information it received pursuant to RFIs. For example, X is facing investigations concerning risk management, content moderation, dark patterns, advertising transparency, and researcher data access.

In some cases, the EC's intervention is forcing platforms to reconsider the scope of the services they provide in the EU. And we have already seen follow-on litigation with claimants relying on the direct right of action for consumers harmed by breaches of the DSA.

Risk assessment and audit reports

The first 19 designated VLOPs and VLOSEs were required by the DSA to publish their first risk assessment and audit reports by the end of November 2024. These reports were to include comprehensive evaluations that detail the risks stemming from their services, such as illegal content dissemination, disinformation, and minors' protection, along with the mitigation strategies they have instituted. As these detailed reports become publicly available, they will offer critical insights that will guide the EC's enforcement actions in 2025.

Looking ahead to 2025 and beyond

Henna Virkkunen has been appointed as the new EU Commissioner responsible for tech policy and will oversee the DSA. She is expected to issue guidelines on the protection of minors under the DSA in Q2 2025 and to present two new initiatives to complement the DSA: a 'European Democracy Shield' (tackling foreign interference on social media) and a Digital Fairness Act (regulating dark patterns, addictive designs and influencers' marketing).

The EC's focus is expected to remain on managing illegal content, combating disinformation, and safeguarding public safety. Platforms will be compelled to conduct robust risk analyses and implement effective mitigation measures to align with these regulatory expectations, ensuring enhanced user protection and a safer online ecosystem. Online platforms will need to navigate this evolving landscape with care and anticipate increased regulatory intervention and heightened litigation risk.

> "The EU's Digital Services Act marks a transformative shift towards increased accountability for online platforms. We anticipate stringent enforcement with an emphasis on transparency, systemic risk management, and user safety in 2025."
>
> Ceyhun Pehlivan, TMT/IP Counsel, Madrid

2.3 The era of digital platform regulation is here

2025 will mark another year of evolution for digital markets regulation: new regimes (notably in the UK) will come into force, while more established regimes (particularly in the EU) continue to shape the digital landscape. Navigating this patchwork will require strategic coordination, by both regulators and firms alike.

Established digital platform regimes continue to bite

2024 saw the establishment of a number of digital platform regimes around the world, which began settling in (and showing their claws) for the first time.

Alongside the EU's Digital Services Act coming into full force for all online platforms in February 2024, the obligations in the Digital Markets Act (DMA) applied to gatekeepers from March 2024. Designated gatekeepers made changes to comply, and the European Commission (EC) has opened investigations into whether several firms fell below the standard of effective compliance. It has also opened "further specification" proceedings under which it can give legally binding direction on what compliance should look like.

Whether the changing of the guard at the EU, with the replacement of the outgoing Competition Commissioner Margrethe Vestager, will significantly alter the EC's hard-stance trajectory is unclear. If not, this sets the stage for a possible showdown between designated firms and the EC, which may ultimately see the appeal courts playing a more significant role in the DMA regime in 2025.

Similarly, Germany's digital platform rules for firms with "paramount significance" continued to expand designations in 2024, while the Chinese industry regulator also continued to take steps (through "regularised supervision" or "full chain regulation") to ensure digital players follow the guidance already given in 2021 on competition and consumer-protection compliance key apps and platforms.

Emerging digital platform regimes poised for the spotlight

As established regimes bed-in, more significant regimes will begin operation in 2025.

Most notably, the UK's eagerly anticipated Digital Markets, Competition and Consumers Act (DMCC) received Royal Assent in May 2024, with commencement of the digital regime expected in January 2025.

The DMCC will empower the UK's Competition and Market's Authority (CMA) to designate firms as having 'strategic market status', imposing tailored codes of conduct and sweeping pro-competition interventions (including structural separation) on those firms.

The broad discretion and scope of tools under the DMCC looks set to supercharge the CMA's role in policing digital markets, potentially even surpassing that of the DMA. While the CMA has waited over three years to prepare for these powers to take effect, it will have to wait a little longer before showing them off: a large part of 2025 is expected to consist of a slow build as the CMA moves through the process of designating the first firms.

The UK is not the only country with new law on its books: in Japan, the new Smartphone Act now imposes DMA-style restrictions on owners of smartphone operating systems and is expected to make an impact over the next year.

What's next on the horizon?

Looking further forward, there are also proposals for new ex ante digital markets regulations in a number of other jurisdictions, including in Australia, Kenya, South Korea and two of the largest developing economies: India and Brazil (although recent reports suggest the Indian proposal may be put in "cold storage").

In the US, legislative efforts to impose special obligations on large tech platforms are unlikely to proceed in the coming years despite past support from some prominent Republicans. Instead, the future of digital platforms will likely be shaped by the landmark public and private enforcement cases against Google (see article 2.4 below).

While inspiration will no doubt be drawn from existing digital markets regimes, the benefit of hindsight also means that some divergence is to be expected as regulators seek to build and improve on practical learnings.

As the number of regimes pursuing the same goals through slightly different means multiplies, so does the compliance burden. Firms also need to consider how these "platform regulation" regimes intersect with other digital and general regulation, in particular content regulation, privacy and consumer law.

A key question for affected companies is whether to "build to comply" or simply remove functionality from particular jurisdictions (or not launch there in the first place), potentially depriving or delaying users' access to the latest features and tools. This – along with governments' responses where their citizens are deprived access to the latest features and tools – will be an important dynamic to watch as the platform regulation regimes develop.

> "In 2025, competition regulators will have more tools at their disposal than ever before, and the stakes are high as they walk the tightrope between rigorous enforcement and chilling "overregulation"."
>
> Verity Egerton-Doyle,
> Antitrust and Foreign Investment Partner, London

2.4 Navigating novel enforcement remedies against Big Tech platforms

In 2025, the US may pave new ground in implementing novel remedies in Big Tech enforcement cases. Remedies could include behavioural mandates to open platforms up to third parties and potential divestitures to break up perceived conflicts. Courts will grapple with the appropriate standard for what remedies should achieve and how they can be effectively administered.

Key aspects of the cases against Google

Landmark public and private enforcement cases against Google will be cases to watch closely in 2025, with the appeal of the court's broad injunctive relief in the Epic v. Google case over Android app stores and the DOJ's proposed remedies following its search monopoly verdict.

Fundamental to the question of remedies policy is the objective and lawful scope of proposed remedies. Beyond prohibiting the challenged exclusionary conduct going forward, the current debate focuses on what additional measures are appropriate to "pry open" monopoly positions and prevent future harm in adjacent markets.

In particular, the parties are split on whether a remedy can require the parties to take measures to support entry of competitors or remove conflicts of interest that would not otherwise be required under the antitrust laws. The parties also disagree on whether remedies should extend to conduct related to related products or services where the target has not been found to have a monopoly. So far, the trial court in the Epic Games case has taken a broad interpretation to find that special obligations are required to support new entrants to remedy past harm – a key issue in Google's appeal to the 9th Circuit.

In the meantime, all eyes are on the approach that the trial court takes in the Google search case launched under the first Trump administration, where the DOJ and state plaintiffs have just proposed a broad set of potential remedies. While the approach will likely be reviewed under the new agency leadership, the DOJ is currently pushing for a broad remedy package, which could include both structural and conduct remedies.

Prohibiting (potentially) exclusionary agreements

The narrowest focus is on prohibiting agreements that were found to be unlawful. For example, the Epic remedies prevent Google from entering into agreements with device manufacturers to preinstall the Google Play store or not support competing app stores. Similarly, the proposed Google search remedies would prevent preferential search placement arrangements with key device manufacturers that were found to be exclusionary. However, the DOJ's proposed remedies would take this further to prevent preferential treatment for new access points for search (e.g. AI assistants) where it has not been found to have restricted competition in the past.

Requiring notice to support consumer choice

Both cases also consider mechanisms that would give more notice to consumers. In the Epic remedy, for example, the injunction would prevent Google from restricting developers' ability to communicate with users about offerings outside the Play Store. The proposed DOJ remedies would require choice screens for search engines and other access points in certain situations.

Providing key inputs to competitors

The Epic decision and the DOJ's proposed remedies in the search case also require the parties to go significantly further in requiring Google to deal with third parties and provide key inputs. In the Epic remedy, for example, Google would be required to distribute third party app stores and provide access to its own catalogue of apps on the Google Play store. In the proposed search remedy, Google would be required to go so far as to provide qualified competitors real time access to all data used to train its search engine to allow competitors to build equivalent quality.

Breaking up target firms with divestitures

The DOJ's proposed remedies go even further in seeking divestiture of Google's Chrome browser to remove conflicts with placement of search in its browser. Equally, the proposed remedy would give the court discretion to require divestiture of Android if the conduct remedies are not effective.

The challenge for the courts in 2025 and beyond

A key challenge for courts in devising antitrust remedies is evaluating whether they can be effectively administered over time and if they will ultimately cause more harm than good. Claiming significant government overreach, Google cites security, privacy, and consumer safety risks arising from requirements to open their systems to competitors.

Lurking in the background is a fundamental policy question of whether the court should require a monopolist to deal with third parties or divest a lawfully developed business at all, or whether the full scope of potential remedies would significantly chill innovation.

Overall, the developing precedent on judicial remedies in the US will be closely watched in 2025 and beyond as other cases against large tech platforms proceed. Even if all (or most) of the proposed remedies are not successful, precedent that expands the potential scope of remedies to open key inputs to competitors and opens the door to breakup of Big Tech firms would have substantial global impact.

> "The landmark US antitrust cases against Google which are currently before the courts could introduce novel remedies that could open the door to significant changes to global business models."
>
> John Eichlin, Antitrust and Foreign Investment Partner, New York

2.5 Litigation funders' focus on tech

Tech companies are increasingly at risk of large-scale litigation in the UK and the EU due to increasing regulatory scrutiny and strong political and legislative support for litigation funding and class actions. Antitrust actions have increased dramatically in recent years, and we expect that to continue in 2025 and beyond.

Desire to diversify

When it comes to weighing up where to invest their capital, funders seek areas which offer (i) a large class of potential claimants (promising a large damages pool), (ii) claims that are unlikely to be brought individually, and (iii) almost invariably, regulatory scrutiny from which to launch private litigation.

The UK's competition law collective action regime has attracted huge amounts of funding and awaits its first substantive judgements by the end of 2024. Funders have therefore committed substantial amounts of capital without yet benefitting from concrete returns. With significant uncertainty remaining as to the direction of the competition law regime, funders are almost certainly looking for opportunities to invest elsewhere.

Now that the EU collective active regime, introduced by the Representative Action Directive (RAD) has largely been implemented, this has opened more fora for funders to choose from. In addition, given funders' desire to piggy-back on smaller scale litigation trends and regulatory action, data privacy and online safety may top funders' wish lists for 2025 and beyond.

Data privacy

The UK has had a steady diet of regulatory action and smaller scale data privacy claims (for example, Experian has faced scrutiny from the Information Commissioner, which we helped it successfully defend). Private litigation has already been brought, both following data breaches and as freestanding claims, alleging the misuse of data, and claimant lawyers and funders are seeking to expand this activity into class litigation.

In the EU, the CJEU's largely claimant-friendly interpretation of the General Data Protection Regulation (GDPR) will be of comfort to funders. For example, the CJEU's position that the concept of "damage" under the GDPR must be interpreted broadly, and that the right to compensation for non-material damage does not require a "noticeable disadvantage", will only encourage more claims to be brought.

Online safety

Another area funders are no doubt watching is online safety. The EU has already initiated compliance investigations under the Digital Services Act (DSA), and the UK's new Online Safety Act (OSA) will inevitably lead to further regulatory probes.

Claimant law firms will likely prey on these regulatory interventions (irrespective of whether a finding of infringement is made), looking for opportunities to bring funded class actions, particularly against household tech names.

In the EU, Article 54 of the DSA contains an explicit basis for compensation claims to be brought by users following a violation of the DSA's provisions. Though the OSA does not have an equivalent direct right of action, claimants could use any regulatory findings by Ofcom as the grounding for other types of claim (for instance, claims of negligence or breach of the terms of service).

Class action mechanisms

The implementation of the EU's RAD means Members States now have clear frameworks by which class actions can be brought, including those causing harm to consumers via data privacy and online safety legislation. The EU therefore looks set to become an emerging battle ground for class actions against tech companies.

In the UK, we have seen cases concerning data privacy framed as competition law claims to benefit from the Competition Appeal Tribunal's opt-out regime (see *Meta v Gormsen*). We have also seen attempts to bring such claims under the stricter requirements of representative actions under the Civil Procedure Rule (CPR) 19.8 (which require the class members to have the same interest) and by seeking Group Litigation Orders (GLOs) (which are opt-in).

So far, CPR 19.8 and GLO claims have been successfully defended in this context (see the High Court's recent decision in *Smyth v BA*, in which we acted for the successful defendant). However, those results have turned on the facts, and further claims are already pending before the courts.

Looking ahead, we expect to see more claims in the UK in respect of breaches of data privacy and online safety legislation and, as in the EU, the UK will continue to attract a growing number of class actions against tech companies.

> "Litigation funders have invested heavily in antitrust claims against large tech companies. That and increasing digital regulation are likely to attract class actions against tech companies in increasingly diverse areas, with strong support from funders."

James Hennah,
Litigation, Arbitration and Investigations Partner, London

Read more - The Digital Markets, Competition and Consumers Act: what you need to know about the risk of private litigation

Contacts

Niranjan Arasaratnam
Global Tech Sector Leader
Corporate Partner, Singapore
Tel: +65 66 92 5858
niranjan.arasaratnam@linklaters.com

Harriet Ellis
Global Tech Sector Leader
Litigation, Arbitration and Investigations
Partner, London
Tel: +44 20 7456 5515
harriet.ellis@linklaters.com

Julia Schönbohm
Global Tech Sector Leader
Global Head of TMT/IP
IP Partner, Frankfurt
Tel: +49 69 71 003 138
julia.schoenbohm@linklaters.com

Lisa Chang
UK Tech Sector Leader
Corporate Partner, London
Tel: +44 20 7456 2838
lisa.chang@linklaters.com

Joshua Ashley Klayman
Global Tech Sector Leader, U.S. Head of Fintech
Head of Blockchain and Digital Assets
Senior Counsel, New York
Tel: +1 212 903 9047
joshua.klayman@linklaters.com

Derek Tong
Global Tech Sector Leader
Corporate Partner, London
Tel: +44 20 7456 2863
derek.tong@linklaters.com

Julian Cunningham-Day
Global Tech Sector Leader
TMT Partner, Dublin / London
Tel: +44 20 7456 4048
julian.cunningham-day@linklaters.com

William Leslie
Global Tech Sector Leader
Antitrust & Foreign Investment Partner, Brussels
Tel: +32 2501 9047
william.leslie@linklaters.com

Verity Egerton-Doyle
UK Tech Sector Leader
Antitrust & Foreign Investment Partner, London
Tel: +44 20 7456 3389
verity.egerton-doyle@linklaters.com

Alex Roberts
China Tech Sector Leader
TMT Partner, Shanghai
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

Contributing authors

Maryam Adamji

Energy & Infrastructure Partner, London

Tel: +44 20 7456 4995

maryam.adamji@linklaters.com

James Hennah

Litigation, Arbitration and Investigations Partner, London

Tel: +44 20 7456 5343

james.hennah@linklaters.com

Ceyhun Pehlivan

TMT/IP Counsel, Madrid

Tel: +34 91 399 6182

ceyhun.pehlivan@linklaters.com

Guillaume Couneson

TMT Partner, Brussels

Tel: +32 2501 9305

guillaume.couneson@linklaters.com

Clare Murray

Technology Strategy Consultant, London

Tel: +44 20 7456 2126

clare.murray@linklaters.com

Arthur Peng

Antitrust & Foreign Investment Partner, Beijing/Shanghai (Zhao Sheng Law Firm)

Tel: +86 10 65 350 651

arthur.peng@linklaterszs.com

John Eichlin

Antitrust & Foreign Investment Partner, New York

Tel: +1 212 903 9231

john.eichlin@linklaters.com

Ben Packer

Litigation, Arbitration and Investigations Partner, London

Tel: +44 20 7456 2774

ben.packer@linklaters.com

linklaters.com