Linklaters

Tech Legal Outlook 2021

linklaters.com

Tech Legal Outlook 2021

Contents

Introduction

After the seismic events of 2020, the new year offers new hope for tackling the Covid-19 pandemic, for economic recovery and for "building back better". Technology and data will continue to have a critical role in all aspects of the global economy, and this will present opportunities and challenges for tech companies. Businesses will be the subject of increased scrutiny and will need to navigate a climate of heightening risk and increasing regulation of the digital economy.

In this publication we explore the key global trends in the technology sector that we believe will shape the legal outlook for businesses in 2021 and beyond.

We consider three macro-themes:

1.0 – The shifting global dynamic

Covid-19 dramatically shaped 2020 and the pandemic will continue to influence geopolitics and the global outlook for 2021. Following a number of major breakthroughs in vaccine development, there are expectations of recovery in 2021. In the meantime, it is clear that continuing to live with Covid-19 will involve more living and working online, sustaining higher demand for digital services. This digital dependency will continue to fuel the growth of tech investment and we expect investors to focus on the key verticals that have attracted significant investment in 2020: fintech, digital health and digital infrastructure.

While there is an expectation that in 2021 President Biden will bring a more predictable and multi-lateral approach to U.S. foreign relations, the U.S. and China will remain rivals, vying for tech supremacy and related economic power and geo-political influence. These two superpowers, along with many other nations, are likely to continue to take steps to protect their economic and security interests, such as controlling foreign investment in certain tech and restricting the international transfer of personal data. Tech companies, especially those with relationships with the U.S. and/or China, will need to reconsider and adapt their global operations in light of these developments.

2.0 – Viewing the future through an ESG lens

Tech is considered critical to recovery from Covid-19: businesses are accelerating their digital transformation; investors see greater returns in tech investment and governments see tech investment as critical to economic recovery. As governments across the globe seek to "build back better" and to promote a green recovery, there is an increased focus on Environmental, Social and Governance (ESG) issues and tech will have an important role to play in enabling these objectives.

In the wake of the pandemic, extreme weather events such as the Californian wildfires, and recognition of inequalities highlighted by the Black Lives Matter movement, we have seen ESG considerations feature prominently in: investor scrutiny; demands from stakeholders; business decisions; new regulatory initiatives; and conditions in the award of public funding.

In 2021 ESG and, in particular, the social aspect, should be a priority for tech companies under pressure to address online harms and to improve their diversity, and more generally for organisations which need to address the legal and ethical issues arising from commercialising data and deploying advanced technologies.

3.0 – Regulation and redress in the digital economy

In a world where we have become dependent on digital services in almost all aspects of our lives, and businesses and governments are reliant on technology for future prosperity, there are fears that major technology companies have become too powerful, and the digital economy cannot be allowed to develop unchecked.

In 2021 we are likely to see continued scrutiny of Big Tech, increased regulation of the digital economy, greater enforcement by regulators and heightened litigation risk as individuals pursue collective actions for alleged failures. We expect a new wave of competition law regulation and enforcement led by Europe, the U.S. and China.

1.1 Trends in tech investment and funding

As predicted in the 2020 outlook, 2020 proved to be another strong year for tech M&A. Global VC investment for the year to Q3 2020 is up 15% on the same period last year and we expect 2020 to be a record year in Europe for VC investments. Covid-19 has brought new momentum to digitalisation and there has been significant growth in investment in the tech verticals that support the new ways of living and working – a trend we expect to continue into 2021 and beyond.

Winners and losers

Some clear winners emerged in the tech sector with the surge in demand for digital services including fintech, digital health, e-commerce, cloud computing and gaming. However, Covid-19 saw a number of tech verticals adversely affected such as travel tech and ride-hailing apps and some defensive action taken to ensure that otherwise strong businesses had the necessary liquidity, in some cases resulting in down-rounds.

Where there has been uncertainty in the market, investors have had more leverage to negotiate favourable funding terms and valuations. In Asia, we are seeing stronger terms from investors: focusing on financial performance with earnout metrics and seeking to exert more control over their strategic tech investments through control deals or investments with options to control.

We see those trends continuing even as the world (hopefully) starts to return to normal and we anticipate that fintech and digital health companies will continue to attract capital as the changes in consumer behaviour prove to be a long-term shift. Alongside that, AI, big data and cyber plays will remain at the front of the queue for funds, notwithstanding the continuing ethical debate over wide-spread data usage.

Read more in our Fintech Year in Review 2020 Year to Come 2021 (available from 9 December)

Digital infra

Digital infrastructure will continue to flourish as an asset class. Data centres and telecoms infrastructure will continue to benefit from the demand from pension funds and other investors looking for stable revenue assets and the need for such infrastructure has only been enhanced by the steepening of the digitisation curve. We see the demand for assets spreading beyond the U.S., Europe and China as the rest of Asia and Africa provide both brownfield and greenfield opportunities.

Read more about our Digital Infra offering and content

Impact of ESG

In addition, the increased focus on green investing and the forthcoming expansion in climate change reporting is sharpening the focus of the investment community on companies that are driving developments in energy efficiency and the net zero transition. We expect e-mobility and energy storage to remain beneficiaries of this.

"The macro-trends that emerged in 2020 as a result of lockdown will continue to drive growth throughout 2021, with investments in digital services, digital health and digital infrastructure remaining centre stage."

Stuart Bedford – Global Tech Sector Leader, Corporate Partner, London

Europe

While Europe has had a strong early stage VC market for a number of years, we saw more later stage rounds building on the trend of companies staying private for longer. With an increased list of active investors in the European late-stage space, we see this trend strengthening further in 2021 and beyond, enabling more of the European champions to find funding as they scale their businesses.

The exit market in Europe remains dominated by M&A, with aggressive competition for the prize assets. While this will remain the case in 2021, we see a resurgence in the European IPO market. This is in part just a reflection of businesses hitting maturity in both the fintech and e-commerce verticals, but is also indicative of a trend towards more active engagement by European and UK regulators to stem the flow to the NYSE and Nasdaq and counter the recent and renewed success of the U.S. SPAC.

Asia

In the first half of 2020, VC investment in Asia was down on 2019 and then in Q3, there was a significant rebound led by China and India. China is investing significantly more in tech than the U.S. or Europe and has pledged to invest $1.4tn to build high-tech industries. With escalating tensions between the U.S. and China, each has sought to become more self-sufficient in critical technology and to turn to better allies. In particular, we expect to see continued investment in the semi-conductor industry as the U.S. and China take steps to decouple their tech supply chains.

Time will tell whether the U.S. election affects the developing U.S.-China tech cold war, but there is a chance for Europe to position itself as a neutral territory, for businesses who seek to maintain a foot in both camps.

Interventionist government

Lastly, all of the trends above will be underpinned by more interventionist government. In the 2008 financial crisis, the existence of start-ups barely registered. During the Covid-19 crisis, the importance of start-ups to major economies outside the U.S. led to a raft of policy-making. Governments will increasingly look to ensure that funding is available to both establish and retain high growth companies and that will drive the private investment market in the tech sector.

1.2 Foreign investment and technology

The Covid-19 pandemic has accelerated the rise of foreign investment controls across the globe and this has been particularly pronounced in the tech sector. Fifteen OECD countries have introduced tighter foreign investment controls and a further seven are planning changes, with new rules aiming to protect the tech sector. While 2020 was about putting in place rules and powers, authorities are now thinking about ways of applying the rules to avoid killing off foreign investment. However, FI control is here to stay and across Europe there are more changes looming each month.

Key global trends

Over the past 12 months, we have witnessed a number of notable trends across jurisdictions:

> **A race to the bottom** for transactions that warrant foreign investment approval, with many jurisdictions requiring approval for non-controlling minority shareholdings;

> **A growth in mandatory filing regimes**, often coupled with civil law invalidity of transactions until clearance has been obtained, and subject to severe sanctions for non-compliance (ranging from multiples of the transaction value to criminal charges);

> **Long and rather non-transparent processes**, featuring behind the scenes co-ordination and a certain political element in decision making. A good working relationship with the authority can help navigate these processes;

> **A higher degree of intervention in many countries**, where typically an assurance on the continuation of business lines or the preservation of national capabilities is required when transactions are subject to in-depth investigation.

Read more: Foreign investment and minority shareholdings, a race to the bottom (September 2020)

European Union

The EU FI Regulation is now in force and looks set to increase the level of scrutiny over current and future transactions. The Regulation targets, among other things, critical and strategic technologies, data and access to sensitive information. This was bolstered by guidelines issued in March 2020, which urged greater vigilance in light of Covid-19 – and the tech sector is certain to feature prominently in the EU's update of its industrial strategy.

Read more: EU endorses new foreign investment screening mechanism (March 2020)

Of practical importance for transaction parties is the enhanced co-operation mechanism between Member States and the EC, which will mean that all regulators will become aware of transactions notified in other Member States and may well inquire as to whether they should also have received a notification.

Fifteen Member States already have foreign investment screening regimes. Following the EC issuing Guidelines calling on Member States to set up a fully-fledged screening mechanism, Belgium, Ireland, the Netherlands and Sweden are in the process of adopting their own regimes.

Read more: Foreign Investment Control – Covid-19 and the Sectors to watch (March 2020)

"The number of FI filings has reached record highs across key jurisdictions despite reduced M&A activity, and we're seeing longer and more complex reviews which can run to six months or longer."

Christoph Barth – Competition Partner, Düsseldorf

Germany

Germany, having updated its rules three times during 2020, is set to have another update in early 2021, which will bring advanced and future technologies into the scope of the mandatory regime, which means that acquisitions of 10% or more of voting rights need to be notified.

Read more: Once more…a third adjustment of foreign investment rules in Germany in 2020 (October 2020)

UK

With a potential hard Brexit approaching, UK acquirers face the prospect of being treated as any other foreign acquirer, thereby facing more foreign investment proceedings across EU Member States. This will also be important for financial investors with fund structures located in the UK or the Channel Islands.

In November 2020, the UK Government announced comprehensive and wide-ranging proposed reforms to its powers to scrutinise foreign investment, reflecting political concerns over foreign investment in critical national infrastructure and in sensitive sectors such as technology. The long-awaited National Security and Investment Bill marks a step-change to the Government's enforcement powers, by introducing a standalone CFIUS-style foreign investment regime for the first time in the UK.

Read more: Will regulation kill the exit? Foreign investment screening in the UK tech sector (November 2020)

U.S.

In the U.S., 2020 was a year of major change for FI reviews by the Committee on Foreign Investment in the United States (CFIUS). Reforms included a mandatory pre-closing notification requirement for certain investments in companies involved with critical technology, critical infrastructure or sensitive personal data. The outcome of the U.S. election is expected to have little effect on the breadth of CFIUS's reach, but there is likely to be a return to its traditional technocratic approach to national security, leading to longer deliberations and more transactions (including acquisitions from China) surviving, but subject to mitigation conditions.

Read more: Navigating CFIUS: A series

Planning ahead

In the tech sector most of the funding typically comes from foreign investors and the intense focus on foreign investment control is resulting in record numbers of filings and deals subject to longer review processes. For example, the proposed UK regime is predicted to review more than 1,000 cases per year compared to c.60 merger cases reviewed by the CMA per year.

Transaction parties now, more than ever, need to ensure that foreign investment filing requirements are factored into the timetable and associated risk assessment for deals involving assets in affected sectors.

Read more on Foreign Investment Control at Linklaters and access our Thresholds for Key Jurisdictions guide

1.3 Deglobalisation demands a different approach from business

Events in 2020 have disrupted the flow of global commerce and brought new momentum to the recent trends towards protectionism and deglobalisation – trends set to continue into 2021. Governments keen to protect and maintain their technological and data sovereignty have introduced protectionist measures and even bans on inbound investments, as well as increasing the self-sufficiency of their home markets. The tech sector witnessed intensified rivalries between the U.S. and China, and significant legal developments such as the EU's *Schrems II* decision and the new Hong Kong national security law. These developments have prompted international organisations to consider recalibrating their global operations and cross-border data transfers.

U.S. – China Tech Rivalry

In 2020, the rivalry between China and the U.S. has intensified, particularly in the race for technology leadership. This growing tech nationalism – favouring national tech over others – was promoted by some governments as bringing economic benefits and providing data and cyber security. Stark examples of this trend were seen in the acceleration of steps to decouple U.S. and China tech, notably through the executive orders issued by the U.S. Administration in its efforts to ban the data-hungry mobile applications of Chinese-owned TikTok (ByteDance) and WeChat (Tencent).

This action against TikTok and WeChat marked a change in the U.S. approach, moving from restricting network-level digital infrastructure (for example, through sanctions and other enforcement actions against China's Huawei), to protecting data, addressing "soft power" issues such as censorship and information bias, and restricting access to consumer-level software.

It remains to be seen whether TikTok's proposed restructure (involving the quarantining of data in the U.S. and minority investment from U.S. players) will be sufficient to pass muster with the U.S. authorities. However, recent developments could also force many other companies, regardless of jurisdiction, to localise data and create separate supply chains for their Chinese and rest-of-the-world markets.

International data transfers

A key aspect of tech nationalism is the protection of personal data. In the last 12 months, several jurisdictions, including India and Russia, have introduced or tightened data localisation laws, requiring certain data to remain within their national borders.

Wider fragmentation of the digital economy is seen in Europe, where the European Court of Justice's decision in the *Schrems II* case rendered the EU-U.S. Privacy Shield invalid as an instrument to enable personal data transfers from the EU to the U.S. More broadly, the decision also requires companies to assess the adequacy of their cross-border personal data transfers conducted under controller-processor standard contractual clauses (or SCCs).

Companies with an international footprint will need to reconsider their cross-border data flows in light of data localisation requirements and, in the case of European personal data, the *Schrems II* decision. In particular, businesses will have to determine whether their European personal data will be adequately protected in jurisdictions that are seen as having strong state security and surveillance laws, such as India, Russia, mainland China, Hong Kong SAR and the UK post-Brexit.

We will be likely to see more companies starting to restructure operations to reduce or remove international data transfers. For some companies, this is part of a broader question about how they structure their organisation, manage their supply chains and operate across the U.S., Europe and Asia to foster greater operational resilience following the disruption caused by Covid-19.

Read more: The future of international data transfers (November 2020)

Read more: EU – data flows post Brexit – choppy waters ahead? (November 2020)

Learn more: Webinar – The future of international data transfers. What does "Schrems II" mean for your business (August 2020)

Corporate structuring

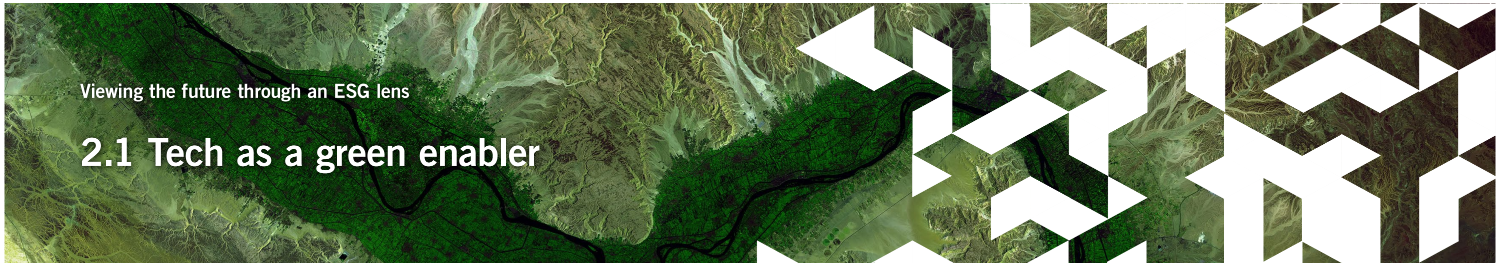
Growing tech nationalism has had an immediate impact on businesses specifically targeted by the U.S. administration and it is not yet certain what the approach of the new U.S. Administration will be. However, there is heightened awareness in tech boardrooms that changes are required for the long-term sustainability of their operations to comply with the current and proposed regulations in the U.S., China and other countries.

These changes include Chinese tech companies re-domiciling headquarters, restructuring business divisions, altering governance structures, quarantining data and other separation measures to disassociate business operations in the rest of the world from those in China.

Businesses will also want to factor in opportunities: for example, jurisdictions such as Taiwan and Japan continue to provide lucrative incentives to repatriate offshore operations and facilities. Tech companies will need to adapt to an evolving legal landscape in order to sustain their success and realise their international ambitions.

> "Technology is being used as a geopolitical tool and businesses are being forced to adapt to an evolving risk landscape."

Niranjan Arasaratnam – Global Tech Sector Leader, Corporate Partner, Singapore



2.1 Tech as a green enabler

Low carbon technologies and digital infrastructure will have a critical role in 2021 and beyond in enabling nations to "build back better" and in helping the economy transition to net zero by 2050. However, tech companies and their green credentials are under scrutiny from a broad range of stakeholders, who are particularly focused on the risk of greenwashing. Tech companies will need to ensure that they are considering the environmental and social impacts of their own corporate activities together with those market actors in their upstream and downstream value chain (and the technologies they provide). As stakeholder and regulatory pressure evolves, they will need to take steps – including due diligence – to ensure that they are meeting emerging standards and managing corresponding risks in their supply chains as well.

Tech is fundamentally tied to the green agenda

The response to the climate emergency and the need to achieve net zero emissions by 2050 will be one of the most transformative business drivers of the next few decades. The ambitious recovery plans that governments are pursuing to counter the damage caused by the pandemic are also providing the opportunity to drive much greater investment in key energy technologies, such as more efficient vehicles and buildings, renewables, alternative fuel-powered vehicles and state-of-the-art electricity grids.

The UK has committed to "build back better and build back greener" and the European Union has proposed a €750bn recovery plan that builds on the European Green Deal (which aims to make Europe the first climate-neutral continent by 2050) and digital transformation. A Biden administration in the U.S., as well as recent net zero pledges from China, Korea and Japan among others, will also enhance global focus on climate change and the energy transition.

Read more: A net zero system (October 2020)

Read more: EU blueprint for net zero by 2050: new 2030 target and green recovery plan (November 2020)

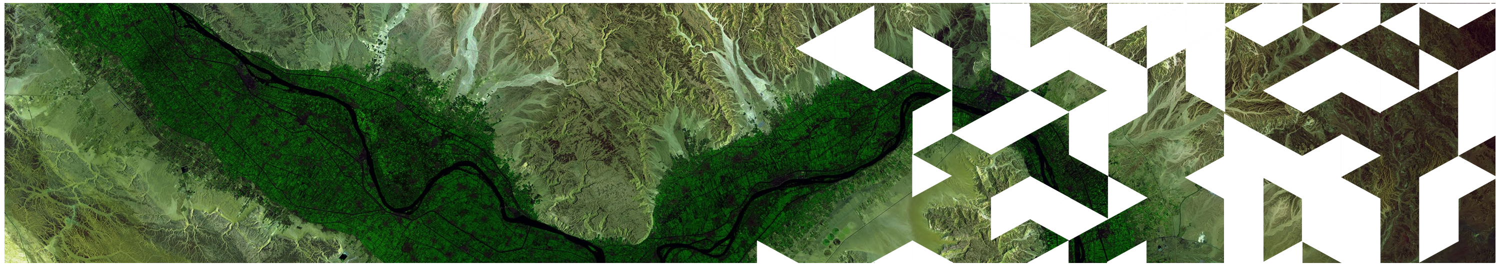
Digital technologies will enable green solutions

The World Economic Forum has predicted that, over the next decade, the technologies of the Fourth Industrial Revolution – particularly 5G, the Internet of Things (IoT) and artificial intelligence (AI) – will provide essential tools for increasing efficiency in the economy and preparing for a post-fossil fuel society. The WEF has suggested that solutions enabled by existing digital technology can reduce global emissions by 15% in 2030, more than the footprint of the EU and U.S. combined. Examples include: satellite monitoring of carbon and methane emissions and deforestation; blockchain to verify claims about the sustainability of products; and the use of AI to analyse data created.

Tech companies have a key role in delivering the smart solutions core to the transition from fossil fuels to renewable energy and to a range of connected sustainability objectives: smart cities and clean transport hubs, the circular economy, pollution abatement and reduction, monitoring of carbon offset projects, and efficient agriculture and land use.

> "The world is experiencing a profound energy transformation, from fossil fuels to renewable energy - this needs significant investment in all kinds of sustainable technologies, systems and infrastructure."
>
> **Vanessa Havard-Williams** – Global Head of Environment & Climate Change, Corporate Partner, London

Smart cities use smart solutions to enable traffic management; public transport; pollution management; waste collection and other services. Clean transport uses tech, for example, in analysing transport data to increase efficiencies in journeys and in collecting data needed to demonstrate that the energy used is clean.



Increasing investment

We continue to see significant investment in smart cities and growing investment in green tech areas such as climate tech and agritech, and we expect this to continue in 2021 and beyond. But commitment to net zero emissions by 2050 will only be achieved with significant new investment in tech by governments, corporates and institutional investors, together with rapid technological changes in how we source and manage our consumption of energy and natural resources.

ESG expectations and legal requirements

Tech companies and their green credentials are under scrutiny from a broad range of stakeholders. In providing tech solutions to tackle climate change, focus is needed on the energy usage and carbon footprint of the technologies and the tech companies, and the ethical use of big data used in the process.

The EU Sustainable Finance Disclosure Regulation will force asset managers to gather detailed quantitative data on the adverse sustainability impacts of tech companies from 2022 and many investors are expected to start this early in 2021. A new emerging regulatory standard on sustainability, the EU Taxonomy, is beginning to create new markets for financial products which invest in "dark green" businesses that also meet stringent social and governance standards.

Another EU regulation taking effect from the end of 2020, creates requirements for Paris aligned and Climate Transition benchmarks – including that to qualify, companies must have credible climate transition plans consistent with the Paris Agreement and report on scope 1, 2 and 3 emissions.

There is also a raft of national and supranational legal initiatives driving a wholesale shift to embed ESG in corporate business strategy, such as a planned expansion of the EU Non-Financial Reporting Directive, planned EU proposals for mandatory human rights due diligence, and enhanced climate disclosures for listed companies in the UK from 2021.

Learn more: Webinar – The ESG mega trend – what and why now? (November 2020)

Increasing pressure on the Tech Sector

As ESG climbs the agenda of financial institutions and corporates, expectations will likely morph over time into contractual representations, enhanced disclosures on ESG matters and greater regulatory scrutiny. Internal systems and controls will be needed to ensure commitments and disclosures can be verified and so that emerging risks can be monitored and addressed.

Consumer appetite is becoming greener; employees expect more from their employers and are willing to use social media to amplify their messages and take action. Proactive stakeholder engagement is likely to become a key part of any tech company's toolkit in this area.

These developments mean that the tech sector is under increasing pressure to operate more sustainably and be more transparent about its economic, social and environmental impacts – these issues will continue to impact business models and drive change.

2.2 Prioritising ESG in digital strategies

The potential social impact of technology is greater than ever. The lockdowns of 2020 demonstrated the value of tech as a force for good in bringing people together, enabling the economy, facilitating scientific progress, and tackling a pandemic. However, incidences of the mis-use of data and the spread of misinformation have shown how technology can also be used to cause harm. At a time when ESG has come to the fore, organisations will need to address the legal and ethical issues that arise in relation to their use of data and technology.

Changing business priorities

Covid-19 has been the ultimate disruptor: business priorities have changed, with business-as-usual superseded by the need to respond urgently to the pandemic. Initially a crisis response, businesses subsequently started to review their longer-term strategy as it became evident that certain changes in consumer behaviour and working practices would be irreversible. Implementing an effective digital strategy became a business imperative.

Digital natives, most notably big U.S. and Chinese consumer-focused tech companies, have out-performed the market in 2020 and have proved well positioned to continue to adapt to changing consumer and employee needs. Other organisations started 2020 with lower levels of digital maturity and needed to accelerate their digitalisation programmes.

Those which were able to adapt quickly have seen some upside, and are in a potentially stronger position going into 2021.

Digital strategies

In the digital economy, businesses need to engage with their customers and counterparties in a digital way and to adapt to changing marketing practices. They must keep their customers' data safe and secure. Businesses need to know who owns the right to that data and who can commercialise it to leverage both the statistical and behavioural value.

Businesses that successfully leverage data can, for example, better understand customer preferences, improve user experience and generate a range of new revenue streams. In the current climate, where businesses are seeking to expand their digital services, businesses are adopting more ambitious data strategies.

Implementing ambitious and potentially intrusive data strategies without consideration of the legal and ethical issues runs the risk of significant regulatory sanctions as well as material brand damage. We expect data practices to be in the spotlight in 2021 with increasing data regulation and enforcement across the globe, including a number of enhanced regimes inspired by the EU's GDPR (e.g. Thailand, China), and an enhanced awareness by consumers of the rights and redress available to them.

Supply chain resilience

The operational impact of the pandemic on complex international supply chains and the reputational impact of recent perceived failures in supply chain governance have revealed fault lines which business and regulators are rushing to address.

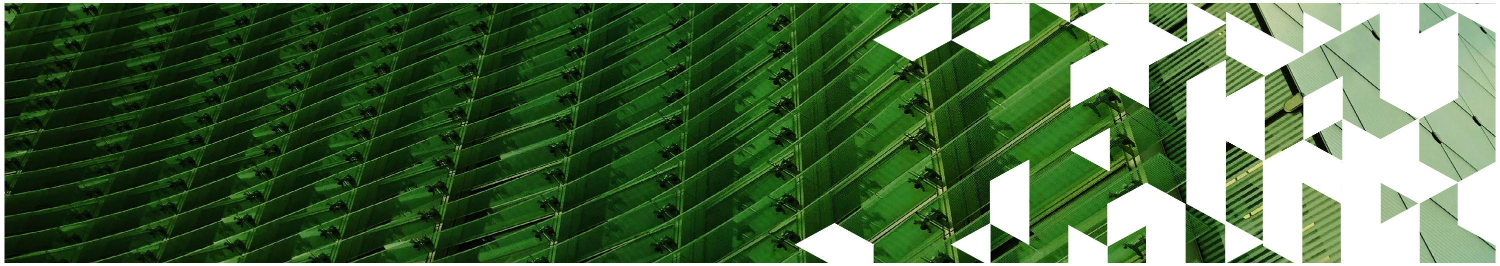
Technology has presented opportunities for businesses to create direct channels to consumers and to leverage remote workforces much more extensively. This has presented significant first mover advantages to businesses that are capable of pivoting rapidly into new operational processes, and existential risks to those that are incapable of keeping pace with changing market imperatives.

Capitalising on these opportunities has often necessitated short-circuiting cumbersome procurement and new business approval processes. While this has demonstrated to many businesses that their processes could rapidly become much more efficient, the risks associated with these changes may take much longer to materialise.

While tech-focused regulators have exhibited a degree of forbearance in light of the recent challenges that businesses have faced (for example, in the UK, the scaling back of fines levied by the Information Commissioner, and recent emollient statements by the FCA), this is clearly only a temporary amnesty, with regulators around the world rolling out comprehensive new operational resilience regimes, and financial services regimes in Europe and the U.S. seeking to regulate tech companies much more extensively.

Learn more: Webinar – Resilience in supply chains (November 2020)

Read more: ESG-related supply chain issues (August 2020)



Increasing liability of online platforms

2020 has brought a renewed focus on the law governing digital services and, in particular, the liability of online platforms. For example, in the wake of the pandemic and divisive U.S. elections, platforms have had to take action to moderate content, including banning adverts discouraging vaccinations. In 2021, we are likely to see the progress of a number of regulatory initiatives in the U.S., EU and the UK increasing the regulation of platforms, including in respect of online harms.

Read more: UK Government announces final proposals for regulating online harms (December 2020)

Read more: European Commission proposes impactful reform of rules for digital platforms (December 2020)

Regular online harms updates can be found in our Tech Insights blog

Adaptive capacity to ESG risks and opportunities will be key

Organisations that are prepared to increase efforts on ESG risk management will be able to improve the efficiency and resilience of their business, achieve compliance and enhance their corporate reputation. In the medium term, they may also benefit from easier and cheaper access to finance. Steps taken now will determine how well-equipped businesses are to deal with related and potentially much more challenging events far into the future and could prove to be a competitive differentiator in 2021 and beyond.

> "Most regulators and investors will have the benefit of hindsight when they judge the decisions that companies have made during the pandemic."
>
> **Julian Cunningham-Day** – Global Tech Sector Leader, TMT Partner, London

2.3 Building diversity into the tech workforce

2020 has presented some fundamental challenges to the diversity agenda of many businesses. The tech sector has been one of the few sectors to continue to grow during the crisis, but the experiences of employees and consumers this year create a powerful argument to put Diversity & Inclusion at the forefront of business strategy as we move into the recovery phase, both to appeal to the widest talent pool and to reflect the expectations of consumers.

> "In an increasingly competitive market for customers and talent, Diversity & Inclusion has become a true differentiator, with failure to act coming at a competitive cost."
>
> **Laure de Panafieu** – Head of Employment and Incentives, Asia, Employment Partner, Singapore

Increased awareness of diversity

The world of work has been fundamentally changed by our experiences during 2020. A global pandemic, the need to balance working from home with the rest of life and the global impact of the death of George Floyd and the Black Lives Matter movement have affected all of us. But although the causes may be the same, the way we have experienced these issues has increased our awareness of our own diversity.

In contrast to many other sectors, the technology sector has flourished in this environment, with companies and consumers embracing its products as a matter of necessity. Despite this financial success, the expectations of consumers and employees in the field of Diversity & Inclusion remain as relevant in the tech sector as in any other. As the demand for technology solutions continues to grow, the need for tech companies to really reflect the populations around them becomes more pressing, not only as employers but in light of the unique role that the tech industry has as a developer of content and products.

Benefits to business of a diverse workforce

The attraction of diverse talent can bring significant benefits to businesses. Beyond profitability, which in itself creates a major driver, research has also demonstrated a clear link between Diversity & Inclusion and characteristics such as resilience, innovation and cohesion, all fundamental qualities required for businesses to weather a time of crisis.

While employers acknowledge that recruiting, retaining and promoting from a diverse pool can deliver these qualities, the reputation of the tech sector has made diverse recruitment a real challenge. Representation of diverse groups remains lower in this sector, with only 17% of the UK tech workforce being women. The BAME community appears well represented, with 15% of the UK tech workforce being from BAME backgrounds, but when the figures are broken down further, the low representation of black people in tech becomes apparent. Once established, low levels of representation of particular groups can create a reputation which is difficult to shake. But there are very real competitive gains to be made in the battle for the highest quality talent from the widest pool.

An enhanced social licence to operate

Diversity & Inclusion also provides opportunities to enhance the reputation of a business to consumers, with a diverse and inclusive culture offering businesses an enhanced social licence to operate. This is not just a question of the employee base, but an awareness that the diversity of the workforce may impact the characteristics of the products being developed by that workforce.

The tech sector remains beset by examples of algorithms failing to recognise the diversity of the community, or stereotyping consumers in a way that undermines the product. An open awareness of, and better understanding for, diversity issues would help to avert the use of input data which serves to reinforce and even to exaggerate existing inequalities in society.

The well-publicised concerns over the gender-driven disparities in relation to Apple's credit assessment of applicants for its credit card, or the racial profiling risks of facial recognition technology, for example, arise from data inputs which might have been dealt with differently by designers if they had been tested and challenged further in their assessment of the diversity risks in the design process. While a diverse workforce does not entirely mitigate these risks, it does significantly increase the chance of relevant questions being asked before the product is put to consumers to test.

D&I outlook for the tech sector

The tech sector has weathered the current crisis well, but as we recover from a year of crisis, the pressure from employees, consumers, regulators and investors for businesses in all sectors to look to their culture and to address their diversity issues will only grow stronger. This year, we have all become more aware of our own diversity through the way that we have experienced the crisis, but in the coming years employees and consumers are more likely to expect to see their own diversity being reflected in the workforce and products of the businesses with which they choose to engage. Companies who deliver on that expectation will have a true differentiator in the market for talent and for customers.

Read more about our Linklaters Diversity Faculty including our D&I featured content

3.1 Data – enforcement, litigation and redress

Data protection became a board issue with the introduction of the EU's General Data Protection Regulation in 2018, followed by equivalent regimes across the globe which provide rights of redress and sanctions of a much greater scale. The right for individuals to claim compensation for damages, the availability of collective procedures to enforce individual rights, and the availability of litigation funding to drive collective claims means that the exposure of the biggest companies for data protection failings could run to billions of pounds. Developments in collective redress will shape the risk outlook for 2021 and beyond.

Collective redress and the potential challenges for tech companies

Major tech companies and their platforms touch the lives of billions of consumers every day. When something goes wrong (for example, a data breach, or misuse of data either on the platform or via a third party), it can potentially affect millions of users. Although the personal impact on consumers can be significant to *them*, at the level of the individual consumer, the financial value of the harm or loss suffered is often very limited.

That said, when modest losses suffered by a large number of consumers are aggregated, the total damages can be significant. We have seen ever more substantial examples in other jurisdictions in recent years, in particular in the U.S. For example, the 2017 Equifax data breach (in which the U.S. Federal Trade Commission alleged that Equifax had failed to take "*basic steps*" to protect against loss of personal data) resulted in a settlement worth only a few dollars per claimant. However, with over 147 million people affected, the cumulative value of the settlement was up to U.S. $700m, still the largest FTC data breach settlement to date.

Until recently, in the UK there was no truly economically viable mechanism for individual consumers to pursue modest claims of this kind, as their legal costs would far exceed the damages that would be recovered by any individual. Historically, UK collective redress mechanisms therefore offered limited recourse. However, in the UK and EU we are continuing to see a number of claimant-friendly developments which will shape the nature of litigation risk for tech companies in 2021 and beyond:

Collective Proceedings Orders

In the UK, collective actions were historically limited to certain competition claims, personal injury claims, and pensions disputes, and would typically be dealt with under a Group Litigation Order which is "opt-in" and requires individual claimants to decide to bring proceedings. Under the Consumer Rights Act 2015, the position evolved for competition claims, through new Collective Proceedings Order (CPO) measures to implement "opt-out" collective actions in respect of private actions for breaches of competition law. In an "opt-out structure" the claim is made on behalf of everyone who is a member of a particular class of claimant.

Seven CPO applications have been brought since May 2018, all of which are at an early stage or were stayed pending the Supreme Court's decision in *Merricks v Mastercard*. The Supreme Court decision was issued in December 2020 and is likely to have huge implications for competition litigation because the judgment significantly lowers the hurdle for certification of collective proceedings applications. The judgment will highly influence the Competition Appeal Tribunal's approach to the pending CPO applications before it and it greatly increases the chances of there being a collective action certified in 2021.

Read more: Supreme Court paves the way for UK collective actions in landmark *Merricks v Mastercard* decision (December 2020)

> "A number of developments in 2021 could enable the pursuit of collective redress in a way that was not previously thought possible and this will change the nature of litigation risk for business."
>
> **Harriet Ellis** – Dispute Resolution Partner, London

Aggregating data protection claims
In a further landmark decision, the Court of Appeal in *Lloyd v Google* allowed a representative action against Google to proceed under part 19 (Part II) of the Civil Procedure Rules in a form of "opt-out" litigation. It was held that the procedure was available in that case because each claimant had the 'same interest' in claiming damages for the loss of control of their personal data. This opt-out structure allowed Mr Lloyd to claim on behalf of more than 4 million affected individuals in England and Wales. Mr Lloyd suggested they should receive approximately £750 compensation each, which would indicate a total liability for Google of up to £3 billion.

The *Lloyd v Google* decision is also being appealed to the UK Supreme Court, and there is a lot of interest in its outcome given that it could potentially open the way for opt-out class actions for privacy breaches. It would have significant implications for Big Tech but it would also have massive consequences for central and local government, the UK's NHS and any other organisation with large amounts of personal information in the UK.

Read more: *Lloyd v Google:* A one-off or the floodgates opening for privacy class actions? (October 2019)

"Lloyd has been presented as a case mainly about big tech vs small consumer. But its implications go far beyond that. If Lloyd wins, it would give the UK the toughest privacy regime in the world, combining the EU's detailed GDPR obligations with a U.S. style class action compensation regime."

Richard Cumbley – Global Head of TMT/IP, TMT Partner, London

EU collective redress directive
In the EU, the EU institutions have agreed a new directive (2018/0089(COD)) requiring Member States to implement collective redress procedures for consumer claims. The directive imposes opt-in requirements for collective action in certain circumstances (in particular where a consumer does not habitually reside in the state where a collective action is brought). Further, the directive requires proceedings to be initiated by 'qualified entities' (which will typically be consumer organisations or public authorities), which may seek either injunctive relief or other redress (for example, compensation).

The directive is expected to be approved by the European Parliament in December 2020. It will be implemented into Member States' national law by 2023 (i.e. after the Brexit transition period ends, such that it will not affect the UK).

Read more: Collective Redress within the European Union (December 2020)

Read more: Collective Redress Directive – the European class action is coming (Part 1 and Part 2) (August 2020)

3.2 A revolution in anti-trust regulation of digital platforms

Governments and competition agencies have different views on how to tackle Big Tech, but despite their differences in approach, the consensus is clear: overcoming concerns in digital markets remains a top priority for 2021 and beyond, and existing competition tools are not sufficient. These upcoming reforms could have wide-ranging consequences and will be closely watched by both online platforms and other businesses that are impacted by their conduct.

What's the challenge?

The exponential importance of technology means that ensuring that digital markets function and evolve competitively and efficiently has become a top priority for enforcers and policymakers.

Traditional competition investigations have faced criticism for being unfit for purpose to address concerns in dynamic, fast-moving digital markets. They are inherently slow-moving, and it can take years before remedies are implemented, by which time markets may have moved on. And even high-profile interventions – often resulting in eye-watering fines – are said to be failing to influence commercial practices across the sector.

EU's big plans to tackle Big Tech

Following a public consultation this summer, the Commission is on track to make its ambitious plans for digital markets a reality. It published two significant legislative proposals at the end of 2020: a Digital Services Act to address e-commerce and online harms, and a Digital Markets Act focusing on new antitrust measures currently comprising two key pillars:

> **Mandatory do's and don'ts for big platforms.** Instead of waiting for competition complaints and cases to address perceived competition problems, the proposals would impose sanctionable do's and don'ts on so-called "digital gatekeepers" – a designation based predominantly on a company's size and core platform service offering. Identified harmful practices like self-preferencing will be prohibited, while others will be mandated – like equal access to data in certain circumstances. Gatekeepers will also need to inform the Commission of any contemplated mergers or acquisitions involving another digital services provider, regardless of its reportability under EU or national merger control rules.

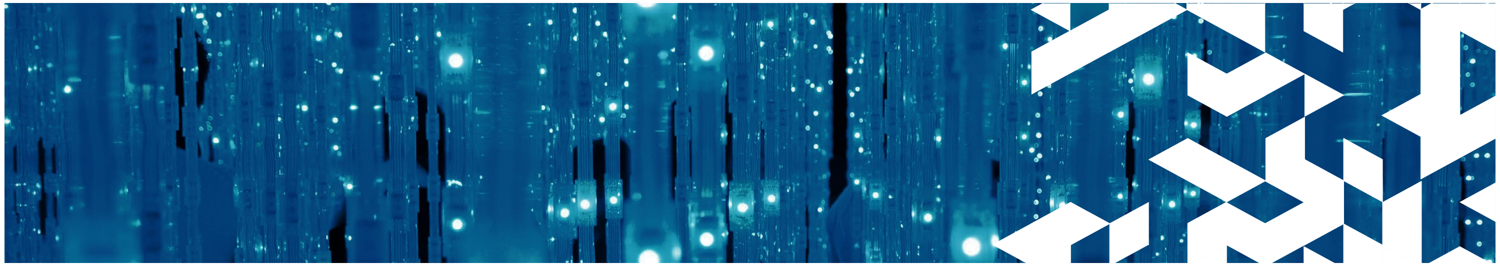
> **Harmonised market investigation function.** This stemmed from the controversial proposals for a "New Competition Tool" discussed over the summer. The current proposition has been significantly reduced but will still play a pivotal – albeit more ancillary – role to ensure the continued effectiveness and enforcement of the DMA. It will allow the Commission to: (i) designate companies not captured by the core platform service test as gatekeepers; (ii) expand the list of core platform services and gatekeepers' obligations; and (iii) impose stringent (including structural) remedies on gatekeepers who systematically breach their obligations under the DMA, with the aim of preserving competition before it's too late.

In a similar vein, the UK's Competition and Markets Authority plans to introduce a tailored "code of conduct" for each platform with "strategic market status", enforced by a new Digital Markets Unit. The regime would also allow for pro-competitive interventions (like imposing interoperability requirements) and enhanced merger powers to increase scrutiny of relevant deals. The UK government has committed to consult on the proposals in early 2021 and to legislate when parliamentary time allows. But given the dual pressures of the global pandemic and Brexit, it is likely that any new legislation is still some way off.

Read more: The European Commission's Digital Markets Act Proposal: Regulating systemically important digital platforms (December 2020)

Read more: European Commission proposes impactful reform of rules for digital platforms (December 2020)

Read more: Competition regulation in digital markets: Five Themes in Five Minutes (November 2020)



> "Competition authorities are facing increasing evidence that past intervention to ensure that digital markets function has not been effective – and are now proposing both radical new tools and sector-specific regulation of digital platforms."

Christian Ahlborn – Global Tech Sector Leader, Competition Partner, London

Several proposals for evolution rather than revolution

Rather than add brand new tools to their toolbox, other agencies plan to enhance their existing rules:

- **Germany:** Germany is planning amendments to its existing competition rules to give the Bundeskartellamt additional powers where a company has "paramount significance" across markets – like the EU's "digital gatekeepers".
- **China:** Seen as the first big step to directly tackle the market power of its tech giants, SAMR is drawing up specific antitrust rules. This follows the commitment by the major Chinese platforms to compete fairly after increased scrutiny of their market power during the pandemic.
- **U.S.:** Policymakers are reviewing a range of measures to expand the competition toolkit. While it is too early to say when or if any of them will become law, they demonstrate a broader trend of U.S. policymakers looking overseas – especially Europe – to solve "the Big Tech problem".

Read more: Changing of the guards: U.S. elections likely to drive further international cooperation on competition in tech markets (November 2020)

Read more: U.S. looks overseas to revamp competition in digital markets (October 2020)

Ramping up traditional enforcement while we wait

While reforms gather pace, Big Tech remains subject to intense scrutiny via traditional competition tools. Barely a day goes by without news of new or ongoing investigations. For example:

- **EU:** The Commission is investigating Apple's rules on the distribution of apps, Amazon's use of sensitive data, and Facebook's data gathering practices as part of its digital advertising business.
- **U.S.:** Federal and state antitrust enforcers have brought enforcement action against Google. Longstanding investigations into other tech companies are also said to be close to reaching the courts.
- **China:** The State Administration for Market Regulation authority is reportedly preparing an investigation into alleged abusive practices by mobile payment platforms following a complaint by the People's Bank of China.

Looking to 2021, we can expect antitrust enforcement to start to pick up again across all sectors – with tech staying front and centre of agencies' focus.

We can also expect agencies to use their merger control powers to the fullest, with the elasticity of jurisdictional rules expected to be a global theme next year.

Learn more: Video – Tech merger control – global hotspots and focus areas for regulators (October 2020)

3.3 Digital Europe – plans for a single digital market for finance

Since the invention of bitcoin over ten years ago, regulators have been grappling with the question of whether, and how, to regulate digital assets. Facebook's ambitions for the independent payment system Libra has refocused regulatory efforts and the EU has been first to respond with a comprehensive Digital Finance Package. This includes specific proposals for an EU-wide regulatory framework for cryptoassets. The EU vision goes far further than anywhere else to define and regulate innovative financial technologies. If the vision of harmonisation can be achieved, a unified and competitive European market for digital finance could shape the direction of the global digital asset industry, drawing greater investment to Europe.

Drivers for digital finance regulation

As markets in cryptoassets have evolved, authorities across the world have become concerned about gaps in existing regulatory frameworks and whether a lack of legal certainty is a barrier to safe innovation in digital finance.

EU authorities have also been concerned that differing national responses may lead to fragmentation. 2020 proved that technology has much more to offer consumers and businesses and the EU is keen to create a competitive market for digital finance while mitigating any potential risks to investors and market integrity.

Read more: FSB lays out global agenda on stablecoins and cross-border payments (October 2020)

A digital single market for finance

The Commission's solution is to create an EU digital single market for finance to rival the UK, U.S. and Asia. Specifically, a proposed Regulation on Markets in Crypto Assets (MiCA) aims to set an ambitious, stable and credible framework for cryptoasset and stable coin regulation, directly applicable in all 26 EU member states. It also seeks to bring a broad range of cryptoasset service providers within scope and to facilitate market entry by enabling passporting across the single market.

A specific crypto taxonomy calibrated to risk

The Commission proposes three broad categories of cryptoasset, each representing different investment opportunities and regulatory issues. The term "stablecoins" is not used, it being considered a misleading marketing term given to these types of cryptoassets that may be neither stable, nor coins. Instead, it distinguishes between "e-money tokens" (broadly, tokens that reference a single fiat currency), and "asset referenced tokens" (broadly, tokens that reference other assets). MiCA also distinguishes between smaller, less risky digital assets, which can be supervised nationally, and more "significant" tokens with cross-border implications (and a higher risk profile), warranting supervision at a federal level by the European Central Bank.

> "The EU's proposed new rules are going to make waves in a number of ways – not least by raising the prospect of a more unified market for digital finance than currently exists in the U.S. or Asia."
>
> **Joshua Ashley Klayman** – Global Tech Sector Leader, Senior Counsel, New York

Direct contrast to the U.S. approach

The EU considers that there are too many cryptoassets coming onto market that do not clearly fall within existing securities law and that a specific regime – borrowing many of the same principles, but recalibrating them for digital assets – is required to bring cryptoassets out of any regulatory grey areas. MiCA only covers cryptoassets which are *not* securities (i.e. *not* already financial instruments for the purposes of EU financial regulation).

This cryptoasset classification approach is in direct contrast to the principles-based approach taken by the U.S., where the so-called *Howey* test looks at the facts and circumstances to determine whether the offer and sale of a cryptoasset can be considered the offer and sale of an investment contract (and hence, "security"). In the U.S., the question of whether a transaction involving a particular digital asset – or such digital asset itself – is regulated is complex, as numerous regulators (including, among others, the SEC, the CFTC, FinCEN, the DOJ and the OCC), at both the federal and state level, may have jurisdiction and such jurisdiction frequently may overlap. It will be interesting to see if regulators in the U.S., and elsewhere, will be inspired by the EU to take a fresh look at their approach to crypto, particularly given ongoing requests from market participants for greater legal clarity and certainty concerning the regulatory treatment of digital assets.

A three-year trajectory

There are three core proposals under the Digital Finance Package now going through the EU's ordinary legislative procedure: (1) MiCA, (2) a Digital Operational Resilience Act (imposing prescriptive requirements on the management of IT risks for all EU financial entities and a new oversight regime for critical third party technology providers) and (3) a Pilot EU-wide DLT sandbox (testing ways to trade and settle transactions in digital assets that qualify as financial instruments). The aim is to have all three in full effect by 2024.

Implications for member states

In contrast to the U.S. legislative process where many proposals get blocked, the majority of legislative proposals submitted by the European Commission are adopted. However, the single market approach inevitably raises questions for some national regulators on the transition process and the treatment of entities approved under existing regimes. There will also be a question of whether the rules will be enforced evenly across all member states.

In the UK, the government has committed to consult on the UK's own approach to cryptoasset regulation, including stablecoins. It remains to be seen to what extent the UK's approach will follow the EU's post Brexit. Non-EU crypto providers should also be aware that the EU regime may have extra-territorial effect, in that issuers or service providers whose assets or services are available in the EU may be caught by the new regime.

Read more: The EU's proposal to regulate the crypto industry: what, how and when? (October 2020)

Impact on DeFi

The move towards concrete regulation of digital finance could have a major impact on the burgeoning DeFi industry, which encompasses a wide range of quasi-financial activities, such as decentralised stablecoin networks, exchanges and lending platforms.

DeFi has been experiencing exponential growth akin to the ICO boom, with many players in the space operating on the assumption that they are unregulated. In reality, the regulatory landscape is complex and a number of arrangements are likely to have implications under existing frameworks. The European proposals will extend the regulatory perimeter further, and are likely to sweep up many more previously unregulated arrangements.

Read more: Decentralised Finance: Navigating the rugged regulatory landscape (October 2020)

Read more in our Fintech Year in Review 2020 Year to Come 2021 (available from 9 December)

Contacts

Christian Ahlborn
Global Tech Sector Leader,
Competition Partner, London
Tel: +44 20 7456 3570
christian.ahlborn@linklaters.com

Christoph Barth
Competition Partner, Düsseldorf
Tel: +49 211 22 977 306
christoph.barth@linklaters.com

Harriet Ellis
Dispute Resolution Partner, London
Tel: +44 20 7456 5515
harriet.ellis@linklaters.com

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

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

Laure de Panafieu
Head of Employment and Incentives Asia,
Employment Partner, Singapore
Tel: +65 6692 5791
laure.de_panafieu@linklaters.com

Niranjan Arasaratnam
Global Tech Sector Leader,
Corporate Partner, Singapore
Tel: +65 6692 5858
niranjan.arasaratnam@linklaters.com

Richard Cumbley
Global Head of TMT/IP,
TMT Partner, London
Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

Stuart Bedford
Global Tech Sector Leader,
Corporate Partner, London
Tel: +44 20 7456 3322
stuart.bedford@linklaters.com

Vanessa Havard-Williams
Global Head of Environment & Climate Change, Corporate Partner, London
Tel: +44 20 7456 4280
vanessa.havard-williams@linklaters.com

Contributing authors

Alex Roberts
Corporate and TMT Counsel, Shanghai
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

Bella Spring
Competition Senior PSL, London
Tel: +44 20 7456 5864
bella.spring@linklaters.com

Clare Murray
Tech Strategy Consultant, Global
Tel: +44 20 7456 2126
clare.murray@linklaters.com

Jack Colthurst
Dispute Resolution Managing Associate, London
Tel: +44 20 7456 4826
jack.colthurst@linklaters.com

Jennifer Calver
Tech Sector Senior PSL, Global
Tel: +44 20 7456 2417
jennifer.calver@linklaters.com

Rachel Barrett
ESG Corporate Partner, London
Tel: +44 20 7456 5414
rachel.barrett@linklaters.com

Ruth Knox
ESG Corporate Managing Associate, London
Tel: +44 20 7456 4413
ruth.knox@linklaters.com

Simon Kerr-Davis
Employment Counsel, London
Tel: +44 20 7456 5411
simon.kerr-davis@linklaters.com

Tim Castorina
Competition Counsel PSL, London
Tel: +44 20 7456 5673
tim.castorina@linklaters.com

linklaters.com

2020-584