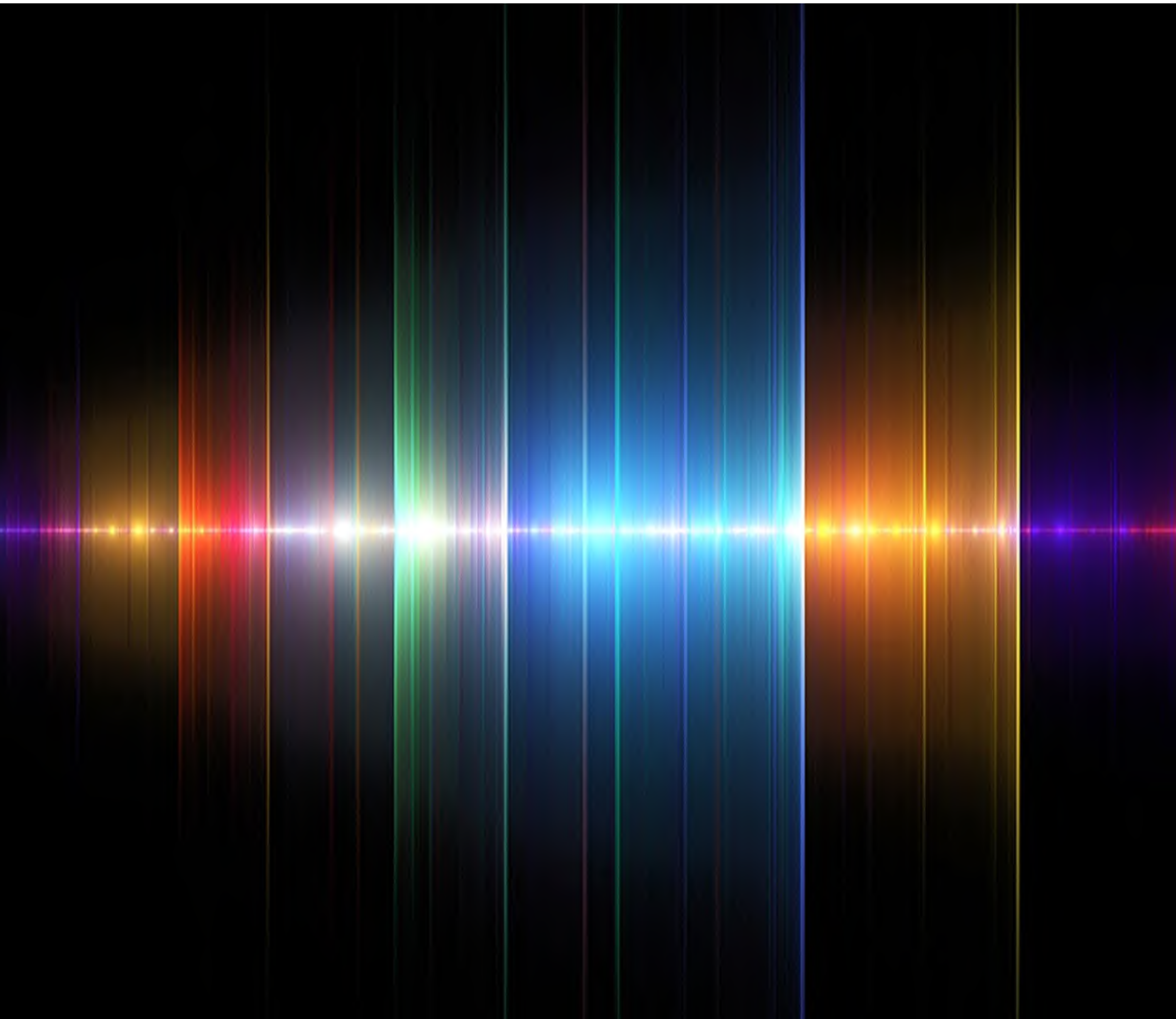
Baker McKenzie.

TMT Looking Ahead 2021

Technology, Media & Telecommunications



Return to Contents

Foreword

Raffaele Giarda
Chair
Rome
Technology, Media & Telecoms
Global Industry Group

Resilience, Recovery, Renewal

Certainly 2020 has been a year like no other. When we were issuing the 2020 edition of TMT Looking Ahead, the COVID-19 pandemic had just started, halted economies around the world and forced people to stay home. Now — almost a year later — various countries are in their second or third lockdown, many of us are working remotely as a matter of course, and while the availability of vaccines provides reason for cautious optimism, we are not yet back to normal life as we used to know it.

As TMT businesses plan for 2021 they are building on the opportunities and challenges arising from 2020. Many bold decisions were taken by the TMT players in 2020 to protect their workforces and to ensure that they continue to be able to deliver technology, connectivity and digital transformation across sectors. Responses to the pandemic were manifold, but two aspects among those that stand out and are top of mind as we enter 2021 are remote working and supply chain diversification. Technology businesses were amongst the first to announce a shift to sustained remote working models and, as they continue to implement this shift, they need to take into account the various resulting legal and tax consequences in addition to the possible impact on team culture, engagement and morale. Building even more resilient and ethical supply chains will be another priority for many TMT businesses in 2021. We look at these and other topics in our Section "The New Normal".

In 2021, we also expect important developments on the legislative and regulatory front that will impact TMT businesses. High on the agenda will be the European Commission's end of 2020 proposal for regulating the digital economy — the Digital Services Act and the Digital Markets Act. We analyse many of the proposed concepts ranging from content moderation and online advertising to data access, regulatory oversight, investigatory powers and accountability mechanisms under "Key Legislative Developments to Watch". In that section, we also dive into the volatile geopolitical environment marked by governments resorting to export controls, import restrictions, tariffs, procurement bans and foreign investment controls — often targeted at the tech sector — in pursuit of digital sovereignty and national security.

On a different note, 2020 has been the year of accelerated digital transformation. As providers of key technology and critical infrastructure such as cloud, blockchain, data centers and next generation networks, many TMT businesses have proven vital in helping to fight the virus, ensuring business continuity and keeping us all informed and connected while confined to our homes. In the "Digital Transformation & Technology" section, we cover topics including cloud, data centers, drones and 5G. We also look at how technology is changing the compliance function as compliance leaders increasingly turn to technology to balance their dual role as protectors and creators of commercial value.

Last but not least, we focus on Data — one of the top business assets in the digital economy and the subject of new regulation and ever more regulatory scrutiny across the globe, from California to Europe to Asia. We offer insights into online gaming privacy, share data transfers strategies and look at data litigation.

We hope you enjoy this publication for which sincere thanks go to all of the authors and editors. Please reach out to any of them or your usual Baker McKenzie contact on any of the content. And, most importantly, on behalf of the Baker McKenzie team, we wish all our readers good health for 2021.

Contents

Digital Transformation and Technology

The pace of digital disruption, accelerated by COVID-19, has prompted companies across all industries to re-examine and transform their business models. Smart technologies such as 5G, AI/robotics, machine learning and IoT are all becoming more interconnected and helping businesses design and execute their digital transformation plans. This year, we consider three interesting examples for the TMT sector: how technology is driving real innovation in compliance; how commercial drone services can take off with the roll out of 5G; and how continuing advances in cloud services are not only being used to drive operational efficiencies, but also new revenue streams.

At a glance

- **The currency of connection: Mobilizing technology for compliance integration.** From a regulatory perspective the race to digitalize operations brings new risks and challenges for compliance teams should they be less involved in technology decision-making processes. On the other hand, the increasing adoption of technology within the compliance function has huge potential. One example is the use of AI by compliance teams to push the right information to the right people at the right time. Going forward such technology will be deployed in more sophisticated ways, including to anticipate regulatory risks as well as enabling business innovation and growth.

- **UAS set to take off with 5G.** 5G networks have significant potential benefits for Unmanned Aircraft Systems (UAS or drones). Always connected drones operating beyond visual line of sight (and ultimately autonomously) in low altitude airspace, which relay large volumes of data in real time from on-board sensors and cameras, are on the horizon. These new generations of 5G connected drones offer significant new business opportunities — think of drones as a service which monitor equipment and facilities in remote locations for security and maintenance or drone delivery services on a much wider footprint. Realizing these new opportunities will depend on having the right balance of regulatory frameworks that enable expeditious roll out of 5G and universal UAS standards that promote safe and efficient drone operation.

- **Cloud services — The key to delivering digital transformation.** Data remains a crucial asset and its collection, storage, analysis and protection are all critical to success in the digital economy. For several years, businesses in all sectors worldwide have been investing in digitally transforming their operations and in some cases becoming more agile — a process that has been accelerated by COVID-19. One of the key enablers for such digital transformation remains cloud computing. Important questions for TMT businesses include: what does progress look like across sectors and where is the untapped potential? Which sectors are more advanced and are looking beyond operational efficiency at new revenue streams driven by the ability to process new data in the cloud?

- **Issues to consider in establishing data centers.** As digital transformation accelerates globally across all sectors with increased data capture and processing in the cloud, demand for data center services continues to steadily increase. Whilst creating data centers remains a key investment opportunity, there are a number of significant issues that must be addressed in advance. These include, for instance, conducting due diligence on suitable locations, staying focused on sustainability, and ensuring compliance with regulatory requirements.

Return to Contents

The currency of connection: Mobilizing technology for compliance integration

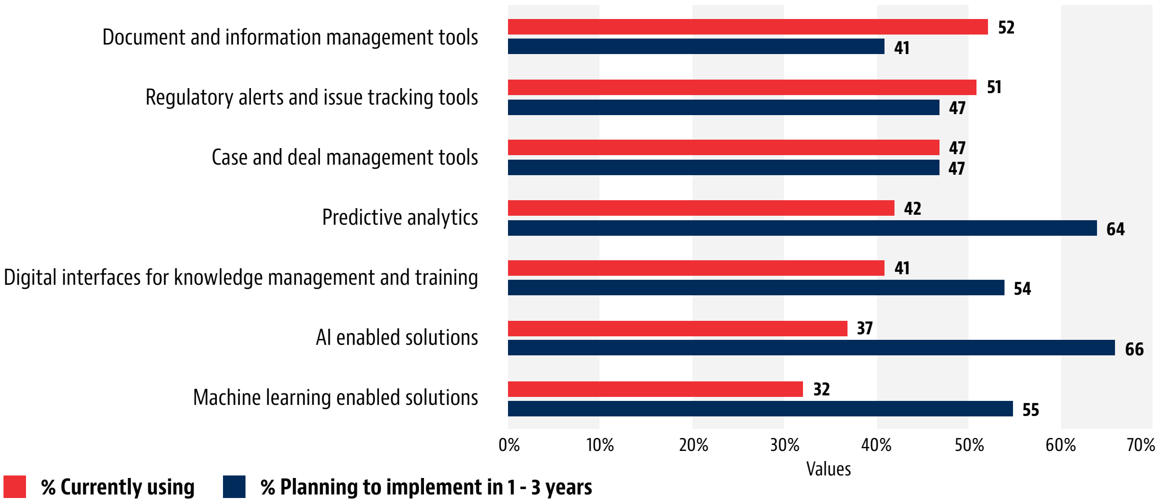
Joanna Ludlam
Partner
Co-chair Global Compliance & Investigations
London
joanna.ludlam@
bakermckenzie.com

Digitalization is not new. Organizations have been integrating technology into business models and operations consistently over the last decade, but COVID-19 has been a catalyst for them to accelerate these efforts. The dramatic shift to remote working and the imperative to quickly shore up revenue streams and supply chains have sharpened focus on the advantages of being a tech-enabled enterprise. Leaders are acting quickly to pivot entire service lines, digitalize operations and automate processes.

Technology in the compliance function

The race to digitalization is also reflected within compliance teams. Facing budget cuts and a dramatic rise in digital and data risk, compliance leaders are themselves turning to technology to balance their dual role as protectors and creators of commercial value. There is huge potential for compliance technology to deliver gains beyond efficiency. We expect to see greater use of artificial intelligence (AI) in future, to push the right information to the right people at the right time – it will be about supporting more comprehensive and connected compliance. The proliferation of new communications and collaboration technology is also an opportunity for organizations to provide next generation compliance programs, using augmented reality to improve the engagement of employees and partners with compliance policies and procedures. We are also

MAPPING THE COMPLIANCE TECHNOLOGY ADOPTION CURVE



Source: **Currency of Connection Report, Baker McKenzie** seeing an uptick in the number of organizations implementing remote-monitoring technology to ensure that employees remain productive, meet contractual obligations and refrain from high risk behavior.

The regulatory perspective

With accelerated change comes new risks and emerging challenges for compliance teams. Not only are some organizations implementing technology with little consideration for risk, but compliance is often neglected in conversations relating to critical technology decision-making. Compliance leaders say this has already resulted in enforcement investigations and predict that regulatory scrutiny will rise as a result of hurried digitalization. And this, in turn, presents an additional challenge: a lack of consistent guidance on compliance technology from regulators globally is a barrier to further tech adoption. There remains considerable room for improved clarity, consistency and guidance in relation to accepted applications of compliance technology. Preferences vary globally and, while some basic compliance technology is widely welcomed by regulators – for example, document processing systems – many of the more sophisticated tools are untested. That said, while there is no singular standard on compliance technology among regulators, compliance leaders can be assured that there is only one direction of travel when it comes to global enforcement expectations – toward digitalization. Regulators value the consistency of compliance technology for investigation reviews and analysis of outcomes – organizations that make use of digital tools are often able to provide more, better quality and timely data to enforcement. Regulators are also increasingly sophisticated users of technology and data. They are setting a high bar and have rising expectations in relation to how organizations should be deploying digital solutions to identify risk, manage issues and, ultimately, support compliance. In the US, the Securities and Exchange Commission (SEC) is leading the way on the application of technology in global enforcement, even developing proprietary tools that allow its teams to pull all trades made at a particular firm and examine data to flag possible aberrational performance and insider trading issues. From the point of view of enforcement, applying the technology that is available on the market consistently to identify, address and report on risk is key to meeting modern compliance obligations.

What's ahead?

Technology is both a new risk to be managed and an essential connector for the compliance function. COVID-19 has catalyzed a re-examination of traditional approaches and many compliance teams are on the cusp of a radical reimagining of the function – embracing technology as an enabler of compliance integration and efficiency.

For example, technology is supporting compliance teams to implement best practice and manage risk among investment partners. We are seeing a rise in the use of risk assessment tools to conduct pre-partnership due diligence as well as oversight on an ongoing basis – streamlining the process of capturing and maintaining information that enables the identification and assessment of compliance risks. This trend is likely to accelerate as new technology comes to market.
AI is particularly useful in managing third party risk. This technology mines, collates and analyzes public source information relating to investment partners to make connections that otherwise may not be made and highlight risks that may otherwise remain hidden. Used in this way, AI can provide greater insight and transparency on investment and procurement decision making processes – making it easier to assess potential hotspots.

Technology is not a panacea for managing risk. But it is a key driver of compliance integration and business growth. Compliance teams that are deploying technology in more sophisticated ways – anticipating regulatory risk, focusing on value and championing innovation – report higher performance and greater return on spend.

From AI and predictive analytics to eDiscovery and regtech (the management of regulatory matters through technology), the future of compliance is well and truly digital.

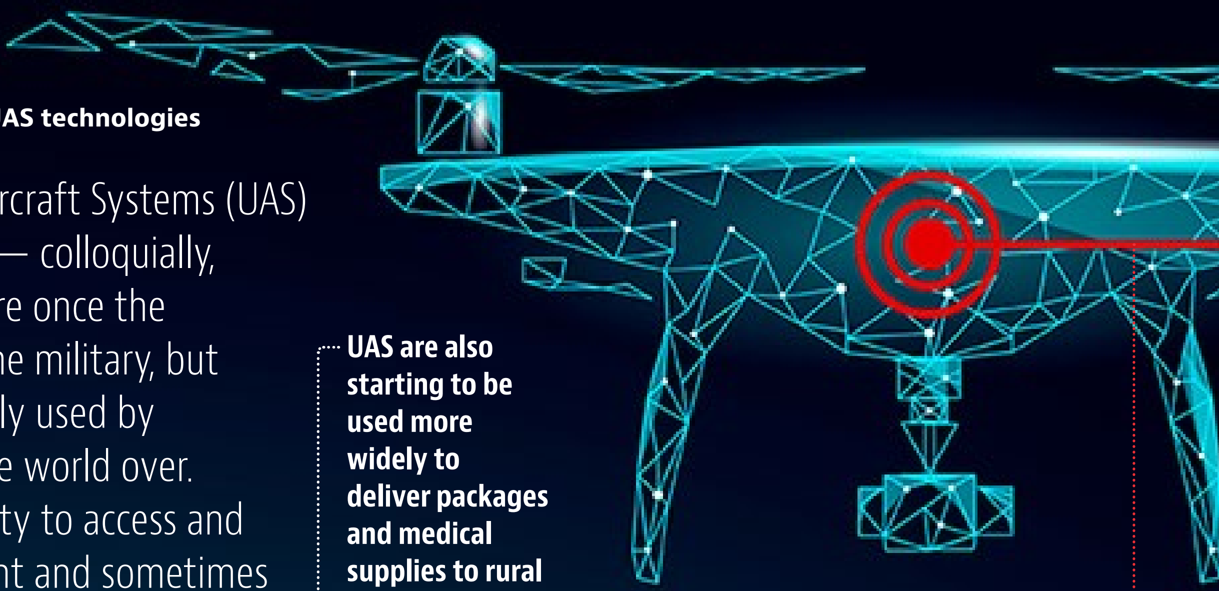
> For a more detailed analysis of the role of technology as a driver of compliance integration and business growth, please visit our Connected Compliance report **here**.

UAS set to take off with 5G

Jennifer Trock
Partner
Washington, DC
jennifer.trock@
bakermckenzie.com

Raffaele Giarda
Partner
Rome
raffaele.giarda@
bakermckenzie.com

Jay Ruan
Partner
Shanghai
zhenyu.ruan@
bakermckenziefenxun.com



Background on UAS technologies

Unmanned Aircraft Systems (UAS) technologies — colloquially, drones — were once the preserve of the military, but are now widely used by businesses the world over. With the ability to access and capture distant and sometimes previously unreachable or dangerous locations quickly and often at lower costs, UAS create myriad of possibilities for the public and the private sector. For example, UAS can be used to survey land or take aerial photos for the real estate market, to inspect remote sites or equipment at mines and other sites, to monitor events or traffic, or for emergency response and search and rescue purposes, and also recreationally or for sport.

UAS are also starting to be used more widely to deliver packages and medical supplies to rural communities.

Current legal issues and challenges in adopting UAS technologies

Businesses interested in marketing or using UAS or related technologies face a range of legal issues and other challenges, including:

- **Differing and highly prescriptive regulations:** many jurisdictions have regulatory restrictions that govern the use of UAS, and these requirements can vary significantly. Regulations of small UAS are generally risk-based, with the more dangerous operations – such as operations over people – being subject to a higher degree of regulation. Other common requirements include: pilot certification requirements, obligations to operate within the visual line of sight (VLOS), requirements to operate during daytime only, and restrictions on altitude and property density. In addition to safety-related requirements, operators must perform in compliance with applicable privacy laws regarding the use of the technology. Radio communications regulations are also implicated due to the wireless transmissions between UAS, pilots and other systems.

Return to Contents

- **Technology licensing, ownership, and liability questions:** with so many other technologies embedded in or related to UAS, companies need certainties about the rights they have and clarity around the risks they might face in adopting those technologies, with IP licensing and potential IP infringement being a key concern. There may be issues also about IP ownership of any content recorded by a drone as well as content created by any artificial intelligence (AI) and machine learning (ML) used in UAS. Counterparties to negotiations for the use and/or development of UAS technologies also have to agree on how to allocate liability arising out of the use of those technologies.
- **Security concerns:** given the wide range of use cases for UAS and the environments in which they can be deployed, security of these systems is also a key issue.

But work is underway to remove these hurdles: industry stakeholders, and harmonization organizations are working on universal UAS standards, which will be critical to related regulatory initiatives and further accelerating the harmonisation of drones; regulators are in parallel – and in consultation with stakeholders – developing improved regulatory frameworks to ensure safety and efficiency while also facilitating the industry; potential UAS customers are also gaining confidence in the technology and learning how to negotiate UAS technology deals while mitigating safety and security risks.

5G technology – a key factor in the development of UAS

Fifth generation mobile network technology (5G) offers the potential of much higher speeds, significantly lower latency and the ability to interconnect many more smart autonomous devices, including UAS. 5G, which started its commercial rollout in many countries in 2020, will be a critical technology in the years ahead as it matures and its coverage expands. It will provide a strategic part of the high-speed connectivity backbone for the increasingly data-focused global digital economy.

5G cellular networks are highly suited to connect drones in low altitude airspace where they can connect to 5G signals high above buildings and trees, away from signal obstructions on the ground. The build-out of 5G cellular technology and infrastructure now beginning to be incorporated in UAS brings the prospect of always-connected devices collecting and relaying huge amounts of data from on-board sensors and camera systems, including detailed real time video. 5G will therefore facilitate prominent technologies in UAS, including:

- Traffic management of UAS: countries including the US (through its Unmanned Aircraft Systems Traffic Management scheme) and a number of European countries (through the U-Space initiative) are currently working on global standardized technology for air traffic management of UAS to enhance safety and security of UAS flights.
- Beyond visual line of sight (BVLOS) operation: most jurisdictions currently restrict UAS to low-altitude operations within the visual line of sight of a human pilot. BVLOS remotely operated and ultimately autonomous UAS will be able to operate much farther and for longer periods.

- Sensor data transmission: 5G will provide the necessary bandwidth to broadcast to ground sites, beyond the remote control station, real time transmission of the sensor payload data and AI/ML processing needs.
- Safer flying: AI and ML – powered through 5G – will have huge potential in both the operation of UAS and counter-UAS technologies, enabling quick and effective decision-making without human intervention. For example, 5G-based AI and ML will be capable of identifying safe landing zones for UAS, developing more sophisticated and safer air traffic management systems, providing the basis for wireless network optimization or, on the contrary, enabling counter-UAS detection systems to identify and track hostile UAS.

5G Regulation

The regulatory landscape for 5G is complex and jurisdiction specific. Telecoms, privacy, real estate, tax, state aid and trade/procurement laws and regulation are all important to assess in the context of 5G. For example, the rules around the allocation and licensing of frequency spectrum, which is a highly-valuable and finite national asset, may differ widely from one jurisdiction to another. In addition, aviation laws and safety regulations are key aspects in respect of UAS.

Many jurisdictions have sought to provide a regulatory environment that fosters investment in 5G technology to incentivize the roll out of 5G commercial services – including UAS services. Crucially this includes making available the necessary spectrum – often via public auctions – on more attractive licensing terms (e.g., longer duration licences than 4G).

For example, in 2016 the European Union committed to its 5G Action Plan to roll out 5G services in a co-ordinated launch across all Member States by December 2020. Following this, in 2018, the EU approved the new European Electronic Communications Code (EECC), to be implemented in Member States by the end of 2020, which consolidates and updates the EEA regulatory framework applying to electronic communications services and networks to promote access to and take-up of very high capacity fixed and mobile connectivity across the EU. The EECC includes specific provisions on Member States making available their 5G frequency bands, co-investment in 5G networks, and regulatory predictability over a period of at least 20 years.

Whilst there have been delays in some Member States to expected timeframes for 5G roll out – all exacerbated by the COVID-19 pandemic – in September 2020, the EU reaffirmed its commitment to 5G as a key strategic pillar of the digital economy and restated its intention to invest 20% of its Recovery and Resilience Facility in digital transformation projects such as 5G. It also issued a **Recommendation** for a Union toolbox to reduce the cost and delays of roll out of 5G networks including provisions to simplify and expedite the granting of permits, improve transparency and access to information on available infrastructure and sharing best practices to ensure planning fees charged are transparent and proportionate (see our alert **here**).

In December 2020, the Body of European Regulators for Electronic Communications (BEREC) adopted its **5G Radar Guide** which covers 24 areas relevant to regulators in the coming years. These include assessing the roaming framework given the future significance of IoT devices which will require international roaming, monitoring the energy efficiency of 5G systems and a focus on ensuring the network and application security in the IoT context, where multiple connected devices provide additional entry points for possible security attacks.

In the United States, 5G deployment is led by private industry – telecommunication providers, technology companies and device makers – aiming to meet increasing demands for data from consumer and business users. These efforts are supported by Congress, which has made spectrum available for 5G use, directed the federal government to identify additional spectrum for future 5G use, and streamlined processes for deploying 5G equipment (also known as small cells) on federal land.

Within the federal government, in 2016 the Federal Communications Commission (FCC) developed the **5G FAST Plan**, a comprehensive strategy to free spectrum for 5G use and accelerate deployment of high-speed broadband in rural America. The strategy includes three key components: (1) pushing more spectrum into the marketplace; (2) updating infrastructure policy; and (3) modernizing outdated regulations.

Return to Contents

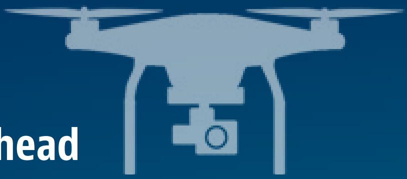
The FCC has also engaged in spectrum auctions and improvement of spectrum across high bands (**28 GHz; 24 GHz; 37 GHz; 39 GHz; and 47 GHz**), mid bands (**2.5 GHz, 3.5 GHz, and 3.7-4.2 GHz**), low bands (**600 MHz, 800 MHz**, and **900 MHz**) and unlicensed bands (**6 GHz** and **above 95 GHz** for opportunities for the next generation Wi-Fi).

In terms of infrastructure policy, the FCC has adopted **rules** that reduce federal regulatory impediments to deploying infrastructure needed for 5G and that help to expand its reach. The FCC also **reformed** rules designed decades ago to accommodate small cells. These reforms banned municipal actions that have the effect of prohibiting deployment of 5G and give states and localities a deadline to approve or disapprove small-cell siting applications.

In China, following the issuance of the formal operating license for commercial operation of 5G by the Chinese regulator to four telecommunications providers in June 2019, construction and deployment of 5G network infrastructure have been accelerated. Part of the efforts include adjustment of spectrum planning and allocation to ensure more spectrum can be used for commercial operation of 5G, as well as promotion of co-investment and sharing of network and infrastructure such as towers and auxiliary facilities.

The Chinese government has also issued policy papers to encourage and support the application and use cases of 5G technologies. Projects involving the use of 5G technologies in IoT, especially in industrial operations, are highly promoted. In addition, 5G technologies are encouraged to be applied to connected cars as a national new information infrastructure and part of the national policy on construction of smart cities and smart mobility.

At the same time, the Chinese government is stepping up the security safeguards for 5G network infrastructure and placing more and more focus on data security protection for the various applications and use cases of 5G technologies.



Looking ahead

Against that background, it is not hard to see why many are describing 5G as a game changer for the UAS industry.

As 5G technology becomes available, businesses in the UAS industry will want to develop their offerings to take advantage of the benefits of this technology. Think, for instance, of how 5G automation may improve the performance and widen the potential use cases for drones with safer and more precise object detection, collision avoidance functions and automated landing as well as utilization in agricultural or industrial settings (e.g., to spray, plant or monitor remote crops or to patrol dangerous and remote locations); or else, consider the combination of 5G and other technologies such as blockchain which offers even more potential for UAS regulators and operators. Indeed, distributed ledger technology has the potential to provide industry regulators with a reliable means of tracking and reviewing UAS operators, devices and their flight paths; the integrity of data stored in a blockchain also means that the technology is ideal to use in identifying and reliably recording non-compliant UAS activity, and to use this as the basis for secure, encrypted communications.

We therefore expect to see new products entering the market, and an upspring of new associated services.

Additionally, as more complex automated UAS solutions supported by 5G technology are developed and implemented, we can forecast an increase in the value of drones as a service, with automated inspections and surveillance as a priority area.

Finally to keep you updated please visit our additional resources below:

▶ **Baker McKenzie's UAS Insights Blog** ▶ **Baker McKenzie's UAS Capabilities Report**

Cloud services — The key to delivering digital transformation

Joyce Smith
Partner
San Francisco
joyce.smith@
bakermckenzie.com

Peter George
Partner
Chicago
peter.george@
bakermckenzie.com

Adam Aft
Partner
Chicago
adam.aft@
bakermckenzie.com

Baker McKenzie's new Digital Transformation & Cloud Survey reveals almost two thirds of businesses surveyed are currently undertaking a digital transformation program, and another quarter are planning one. Digitalization is clearly one of the leading strategic priorities for companies globally. But according to this new research, for many organizations it is also one that is proving particularly difficult to get right.

The drivers, challenges and benefits of digitalization

Just one in three companies that have been through a digital transformation process say it has actually improved operations, despite business agility being cited as the number one reason for embarking on the process. Many of those surveyed also expressed concern around increased operational confusion, and the need to imbed additional processes and technology in the wake of digitalization. However, these issues do not appear to be reducing the appetite for transformative digitalization amongst executives surveyed for the report. To the contrary, the pandemic has accelerated this activity for many as the world moves ever more quickly online, and competitive pressures increase. According to the survey of 300 executives, who as part of their roles are buyers, users and/or suppliers of cloud and digital services, other key drivers for digital transformation include the ability to attract and retain talent, to improve collaboration and internal processes, and to better understand customers.

> "Agility and innovation are uppermost in the minds of businesses when they are considering transformation. Factors such as bringing new products and services to market more quickly or using data to support new, strategic decision making as well as data monetization weigh heavily in the decision for digital transformation."
>
> **Sue McLean, IP, Data & Technology Partner**

The monetization of data and new tech appears to be one of the great untapped benefits of digitalization, with most companies still focused first and foremost on becoming more operationally efficient rather than on using digital transformation to seize new business opportunities and monetize new offerings. Those executives surveyed also remain particularly concerned about cybersecurity, with 42% of respondents citing the need to "improve cybersecurity" as one of the top-three drivers of accelerating digital transformation, due to the pandemic.

Meanwhile, trying to integrate new and legacy systems remains the leading barrier to digital transformation. Therefore, business leaders are now looking to learn from recent experiences of similar companies, cut through the tech hype, and reduce financial and operational risks.

Return to Contents

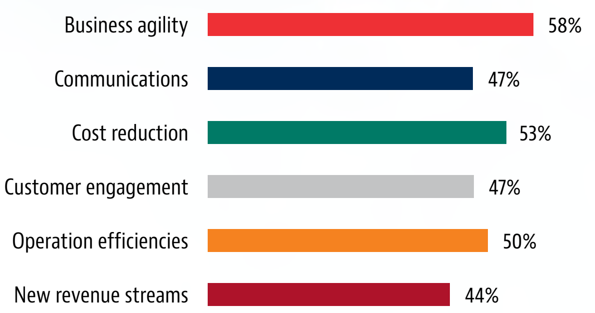
Cloud as key enabler

One of the top digital transformation enablers remains cloud computing, with the survey finding a marked increase in the reliance on private cloud services, driven in part by the promise of better data security and disaster recovery. This has been further accelerated by the adoption of remote working among businesses due to COVID-19 lockdowns.

> "Consumers are creating and acquiring digital content across multiple platforms, and the way in which they use and share that content itself creates an extensive data footprint. This means "big data" applications — quantifying, interpreting and responding to individuals', groups', companies' and governments' activities on a real-time basis — depend heavily on the availability of cloud computing services and infrastructure."
>
> **Adam Aft, Technology Partner**

Operational efficiency was a central goal when adopting cloud-based services, but this varied quite significantly across industries. Financial institutions (68%) and healthcare and life sciences companies (67%) are most likely to benefit from becoming more operationally efficient as a result of cloud-based IT, while tech, media & telecoms, and consumer goods and retail (CG&R) companies view cloud as helping to improve the company's business agility. For technology, media and telecoms companies, cost reduction, operational efficiencies, communications and customer engagement then followed to round out the top 5 perceived benefits.

IMPACT OF CLOUD ON THE TMT SECTOR



Of the industries surveyed, over 50% of CG&R companies identify building 'new revenue streams' as a potential impact of cloud; this is higher than any other industry featured. It was one of the few clear links to monetization, with most businesses rather looking at efficiencies, customer insights and colleague collaboration as key drivers.

Data remains at the center of all of these discussions and a crucial asset for business.

> "The value of data to business is undeniable. It lies at the core of a successful technology strategy, whether it is the storage, collection, protection, analysis or use of this data. Respondents from this year's survey see it as one of the most important business drivers they have."
>
> **Peter George, Partner, Technology Transactions**

Data is also a key issue when it comes to cloud deployment, with respondents citing (in this order) data privacy (confidentiality), data protection (security of data) and data sovereignty (control) as their top three concerns around cloud implementation.

WHAT ARE THE KEY CONCERNS WHEN IT COMES TO CLOUD DEPLOYMENT?

1 Data privacy (i.e. confidentiality)

2 Data protection (security of data)

3 Data sovereignty (control)

4 Cost

Cloud based solutions provide the infrastructure that supports digitization and digital transformation projects. These solutions are and will continue to be a developing trend in 2021.

The Cloud and Digital Transformation survey **here**

The TMT highlights of the Cloud survey **here**

Issues to consider in establishing data centers

Geraldine Ong
Partner
Singapore
geraldine.ong@
bakermckenzie.com

Abie Co
Lead Knowledge Lawyer
Manila
abigailnerizza.co@
bakermckenzie.com

Data center demand has steadily increased, but has received a boost with increased data use due to cloud computing, e-commerce and the availability of 5G coverage. COVID-19 has also fuelled expansion in this sector.

Here we discuss some of the major issues that must be considered in establishing a data center.

Choosing the market

Setting up a data center is complex. Just choosing where to establish one is difficult.

There have been data center projects that were not completed or for which scarcity of resources have resulted in an unexpected increase in cost. One such resource is power. Data centers use copious amounts of energy that are not always available in target sites. In some instances, the installation of additional power infrastructure is necessary and this may trigger the need to negotiate additional rights, such as rights of way. Sometimes, the difficulty lies in securing internet coverage. In some jurisdictions, owners or operators have difficulties purchasing or leasing real estate.

When choosing a location, owners and operators also need to keep security in mind, by seeking areas that are not prone to disasters (manmade or natural) and that are otherwise physically secure.

Aside from the usual permits and authorisations needed to operate a business such as planning controls and building requirements, data centers may need additional licences and approvals.

There are jurisdictions which consider data centers as a core business or critical infrastructure and so limit foreign investment or require prior approval or licensing. A number of jurisdictions also set limitations on foreigners when buying or leasing real estate. Thus, building a data center, or even just purchasing shares in a data center may trigger foreign investment restrictions.

For example, in Australia, the Australian Foreign Investment Review Board (FIRB) has imposed specific conditions with respect to acquisitions of data centres in Australia, particularly in relation to:

- the composition of the board of the controlling entity in the target group;
- the access to, and storage of, data; and
- the preparation of an audit to assess compliance with FIRB conditions.

Regulators, such as FIRB, are often concerned with the types of data held by the data center, security of the data center, accessibility of the data, connection to governmental entities and any governmental customers.

Return to Contents

Security features

Data center security is paramount to performance. Data center customers will often carefully negotiate the scope of an operator's responsibility for physical security (e.g., loss of tangible property) and electronic security (e.g., data privacy breaches). Data centers must therefore appropriately protect and secure both physical servers and electronic data.

> Data centers usually have 'layered' security to ensure continuity of service if one layer is breached. Security protocols such as 24/7 onsite monitoring and surveillance and entry and exit procedures are commonly used. They should also comply with local security requirements.

Sustainability issues

As mentioned, data centers use substantial amounts of energy. Accordingly, as businesses look for 'green' solutions, data center operators also aim at implementing green practices and sustainable power sources. The use of renewable energy will not only support clean energy goals, it also provides a steady energy source at a long-term fixed rate. Such 'green' data centers that operate with maximum energy efficiency and minimal environmental impact are attractive to investors and users with sustainability objectives.

Data privacy

International privacy concerns are a key issue amongst others. When working in foreign jurisdictions, operators must take care and make sure that international operations comply with local regulations. Additionally, customers may also be concerned about access to data by foreign governments under national security legislation in host locations. Moreover, critical infrastructure or cybersecurity laws may have direct or indirect impacts on data center owners and operators, who may be subject to reporting or other obligations to cooperate with governments.

Tax

Data center owners and operators will have to consider the tax implications of the different types of contracts that they may offer to their customers. Owning or leasing servers in another jurisdiction may constitute a permanent establishment in that other jurisdiction. In such a case, offering a hosting services agreement that does not result in the ownership or lease of a server and that expressly limits physical access might be explored to reduce the potential exposure connected to a permanent establishment and, therefore, depending on the outcome of the analysis, might be more attractive to a customer from a tax compliance perspective. Data centers will also have to identify which of the services they offer are subject to indirect taxes, such as VAT or GST.

> **Data centers are proving to be critical assets.** However, a deep understanding of the issues related to this asset class is necessary for any company wanting to expand into this business.

Key Legislative Developments to Watch

The long-mooted increased regulation of digital services and markets in Europe landed in December 2020 in the form of two draft regulations, the Digital Services Act and Digital Markets Act. In 2021, digital service providers will be focused on preparing their businesses for the changes ahead, as both proposals navigate the legislative process. The DSA and DMA will not be the only items near the top of corporate agendas in 2021. Others are likely to include monitoring the continued efforts to find international consensus on tax reforms for the digital economy and addressing the impact of any further developments in the ongoing technology-focused trade wars.

AT A GLANCE

- **The EU Digital Services Act: What does the future hold?** The European Commission has published its landmark draft new rules applicable to digital services (the Digital Services Act). The DSA shares common themes with the Digital Markets Act (see below) in particular (re) assigning liability or responsibility for possible online harms and a push for even greater transparency from market players. We examine what is actually new for TMT industry players and what lies ahead in these proposals which cover key areas, including safe harbours, notice and take down, know-your-trader requirements, reporting obligations and annual reviews of systemic risks by very large platforms (as defined in the DSA).

- **The EU Digital Markets Act: New rules for platforms.** Published alongside the proposed Digital Services Act, the proposals in the Digital Markets Act focus on the largest platforms (gatekeepers) which supply "core platform services" and seek to address what the European Commission perceives as power asymmetries between platforms, their business users and end users. Another area of focus is around general market structure — to ensure markets remain "fair and contestable". We look at the definition and role of gatekeepers and the key obligations that will apply under the DMA as well as the road ahead.

- **Trade wars and protectionism — Digital sovereignty under attack?** The TMT sector is at the center of disruptive global trade wars as geopolitics collide with new technologies and economies are increasingly driven by technological innovation. Examples include the use of export controls to protect "crown jewel" technology, import restrictions and tariffs, procurement bans and foreign investment controls which target key industry players on the basis of perceived national security concerns and in pursuit of digital sovereignty. As the concerns underlying these measures are deeply rooted and change is unlikely at the macro level in the short term, we provide an overview of the most important challenges TMT businesses are facing.

- **Taxing the digital economy: Still striving for consensus.** The longstanding effort to find international consensus on how best to tax the digital economy continues in 2021. There is however cause for optimism as the OECD's two-pillar approach has widespread support (Pillar One being focused on an agreed method of taxing digital services and Pillar Two on a minimum tax rate for multinational groups). Moreover, there is hope that the Biden administration will take a more multilateral approach to tax matters. However, agreement is not guaranteed and TMT businesses will need to watch developments carefully and prepare for the upcoming changes.

The EU Digital Services Act: What does the future hold?

Ben Allgrove
Partner & Global
Head of R&D
London
ben.allgrove@
bakermckenzie.com

Julia Dickenson
Of Counsel
London
julia.dickenson@
bakermckenzie.com

Rebecca Bland
Associate
London
rebecca.bland@
bakermckenzie.com

On 15 December 2020, the European Commission published its long awaited drafts of the "Digital Services Act" (DSA) and "Digital Markets Act" (DMA). In the run up to the drafts being released there was intense speculation about how far the Commission would go in trying to achieve its aims of *"[making] sure that we, as users, have access to a wide choice of safe products and services online. And that businesses operating in Europe can freely and fairly compete online just as they do offline"* (EU Commissioner Margrethe Vestager). Cutting through all the noise, where do the real impacts lie, and what is the road ahead for these high profile Commission proposals?

If you look back at the raft of EU legislative proposals that have come out over the last few years, you can see some common themes in the DSA and DMA, in particular (re)assigning liability or responsibility for online harms and a push for greater transparency from market players.

But what is actually new in the DSA? Some key aspects are covered below and also see the table at the end of this article. For an analysis of the DMA see **here**.

New intermediary categories

First, the DSA proposes 4 categories of online services: an *"intermediary"*, a *"hosting service"*, an *"online platform"* or a *"very large online platform"* (VLOP), with each category having increasing obligations, with the highest stakes (and fines) for VLOPs. This is new. And it comes on top of the classification that we have already in the Platform to Business Regulation (P2B), the Copyright Directive and the Audiovisual Media Services Directive (AVMS). It is going to be increasingly important that online players understand what bucket (or buckets) they fit into in order to understand what obligations they will potentially be subject to.

Liability and responsibility

Safe harbours

The well-established e-Commerce Directive safe harbours will be largely replicated in the DSA, though with the addition of a "Good Samaritan" provision for intermediaries who carry out investigations to detect illegal content or comply with the DSA. The latter is a change that has long been advocated for by the technology industry and will be welcome. However, the defences will be narrowed to exclude consumer law violations where it is reasonable for consumers to believe the intermediary is providing the information/good/service they have received. In other words, clarity as to with whom a consumer is engaging will become ever more important. This may impact product and customer contracting strategy and structures.

Notice and takedown

The DSA purports to harmonise notice and takedown mechanisms for the first time in the EU. However, the mechanisms proposed are fairly general and in practice are unlikely to materialise into significant changes for the majority of platforms and marketplaces, which mostly already have sophisticated processes in place. The big change proposed is to require a statement of reasons to be provided to explain why a host has removed or disabled content (and to make those statements publicly available). This mirrors a parallel obligation in the P2B Regulation, but with much wider potential impact. We expect to see a lot of discussion about how this might work in practice, and at scale, and how the imperative to provide a safe online experience is balanced against other fundamental freedoms in circumstances which are often highly fact dependent.

Another proposed change is the recognition of "trusted flaggers" which will be specially chosen by (also new) Digital Service Coordinators in Member States, noted for their expertise in flagging illegal content for collective interests. Given some of the current political tensions within the EU about differing Member State approaches to the rule of law, we can anticipate that there is likely to be material variance between Member State approaches to trusted flagging.

Know your trader requirements

In an effort to clamp down on illegal and harmful goods and services available online, the Commission also proposes new "know your trader" requirements, making online platforms obtain proof of trader identities and to verify actively whether they are accurate. While some of this information is already collected by platforms, the legal duty to verify it has not been seen before outside of situations where anti-money laundering requirements apply. These requirements echo proposals in other jurisdictions, including in the US, and are a bid by the Commission to make marketplaces take greater responsibility for their platform without – automatically – bearing liability for the actual listings.

VLOPs and "systemic risks"

For the largest platforms, the DSA proposes a requirement for VLOPs to carry out an annual review to identify what "systemic risks" stem from the use and provision of their services and then to take measures to address these risks. This approach invokes the spirit of self-regulation, but with sharper legal teeth, including independent audit.

Transparency/accountability

Transparency reports

One of the strongest themes emanating from the DSA is the push for more transparency. While many intermediaries already provide some, or even much, of the information the DSA is asking for, the draft requires more. All intermediaries must publish transparency reports at least once a year which include the number of orders by Member States to remove content, notice and takedown requests (and the time to remove them) and what content moderation measures they have taken. On top of this, VLOPs must publish details of any automatic means used for content moderation, and the number of disputes submitted to out-of-court dispute bodies and suspensions imposed for misuse of the notice and takedown procedure. All this must be done every 6 months under the eye of a compliance officer appointed by the VLOP, responsible for compliance with the DSA. This seems to be more than what is expected of a Data Protection Officer under the GDPR.

If these reports do not contain information the Digital Service Coordinators (experts appointed by Member States to enforce the DSA) require about VLOPs, there are new broad powers for them to request it. While this can be done already in most Member States via the courts, this is a more direct and potentially more invasive compliance tool. Importantly, there is a proviso that such information does not need to be shared if the VLOP does not have access to the data or if its release might lead to significant vulnerabilities. We expect this to be an area of much debate.

Advertising transparency

If the draft makes it through in its current form, online platforms will have to identify all advertising as such as well as who is behind the advertising and why that advertising targets certain users. In addition, VLOPs will have to set out the main parameters used in recommendation systems as well as any options for users to modify the influence these have on their use, and to compile and make publicly available information on the content of adverts, who they were aimed at and the total number of recipients reached. These obligations go materially beyond obligations that already exist in most Member States.

The path ahead

The European Parliament and Member States will now discuss the proposed DSA through the ordinary legislative procedure. Reports suggest France wants to reach an agreement during their presidency of the EU Council, which may mean a final DSA Regulation entering into force by the end of 2022.

Ultimately, the date of publication and the final form of the DSA will be dependent on how it fares as it passes through the EU legislative process. It is unlikely to be a smooth ride given some of the implications of the Commission's draft and what we saw with the earlier passage of the Copyright Directive and AVMS Directive in particular. The US Chamber of Commerce has already said it is "concerned about the direction" of the proposals, suggesting Europe seems "intent on punishing successful companies that have made deep investments in Europe's economic growth and recovery". Such comments will play in the minds of those working on the draft, especially given the wider consequences it might have on transatlantic relationships which the US has flagged "risk being undercut by burdensome and discriminatory proposals".

Key battlegrounds are likely to include the more onerous transparency requirements and additional measures proposed for VLOPs.

We'll keep you updated...

WHAT ARE YOUR OBLIGATIONS UNDER THE DIGITAL SERVICES ACT?

	Intermediary services	Hosting services	Online platforms	Very large online platforms
Transparency reporting (A13, R39)	●	●	●	●
Requirements on terms of service due account of fundamental rights (A12, R3)	●	●	●	●
Cooperation with national authorities following orders (A8 and A9; R29,30,31,32,42)	●	●	●	●
Points of contact and, where necessary, legal representative (A10, R36; A11; R37)	●	●	●	●
Notice and action/obligation to provide information to users (A14 and A15. R40-42)		●	●	●
Complaint and redress mechanism and out of court dispute settlement (A17 and A18, R44 and 45)			●	●
Trusted flaggers (A19, R46 and 47)			●	●
Measures against abusive notices and counter-notices (A20, R46 and 47)			●	●
Vetting credentials of third party suppliers ("KYBC") (A22, R49)			●	●
User-facing transparency of online advertising (A24, R52)			●	●
Reporting criminal offences (A21, R48)			●	●
Risk management obligations and compliance officer (A26, 27 and A32, R57, 59 and 65)				●
External risk auditing and public accountability (A28 and 33, R60, 61 and 65)				●
Transparency of recommender systems and user choice for access to information (A29 and A30, R62 and 63)				●
Data sharing with authorities and researchers (A31, R64)				●
Industry Standards and Codes of conduct (A35 and A36, R66-70)				●
Crisis response cooperation (A37, R71)				●

A — Refers to Articles in the proposed Digital Services Act Regulation

R — Refers to Recitals in the proposed Digital Services Act Regulation

The EU Digital Markets Act: new rules for platforms

Paul Johnson
Partner
Brussels
paul.johnson@
bakermckenzie.com

Laura Philippou
Senior Associate
London
laura.philippou@
bakermckenzie.com

After being postponed twice, the European Commission (Commission) published its draft Digital Markets Act (DMA) on 15 December 2020, in revised form — the EU's Regulatory Scrutiny Board having objected to earlier iterations. The DMA takes the form of a regulation as the Commission seeks to ensure maximum alignment among Member States. The proposed "Digital Services Act" (DSA) was published on the same day.

The proposals in the DMA focus on the largest platforms – mostly US-based at this juncture – and seek to address perceived power asymmetries between platforms, their business users and end users - as well as issues around general market structure - to ensure markets remain "fair and contestable". The Commission's concern is that existing competition law enforcement is too slow and cumbersome to rectify problems before markets "tip" irrevocably in favour of the strongest players.

Prior controversial proposals for a standalone "New Competition Tool" (NCT), akin to a market investigation power, have been "folded" into the main text of the DMA and been made more limited in scope than originally proposed.

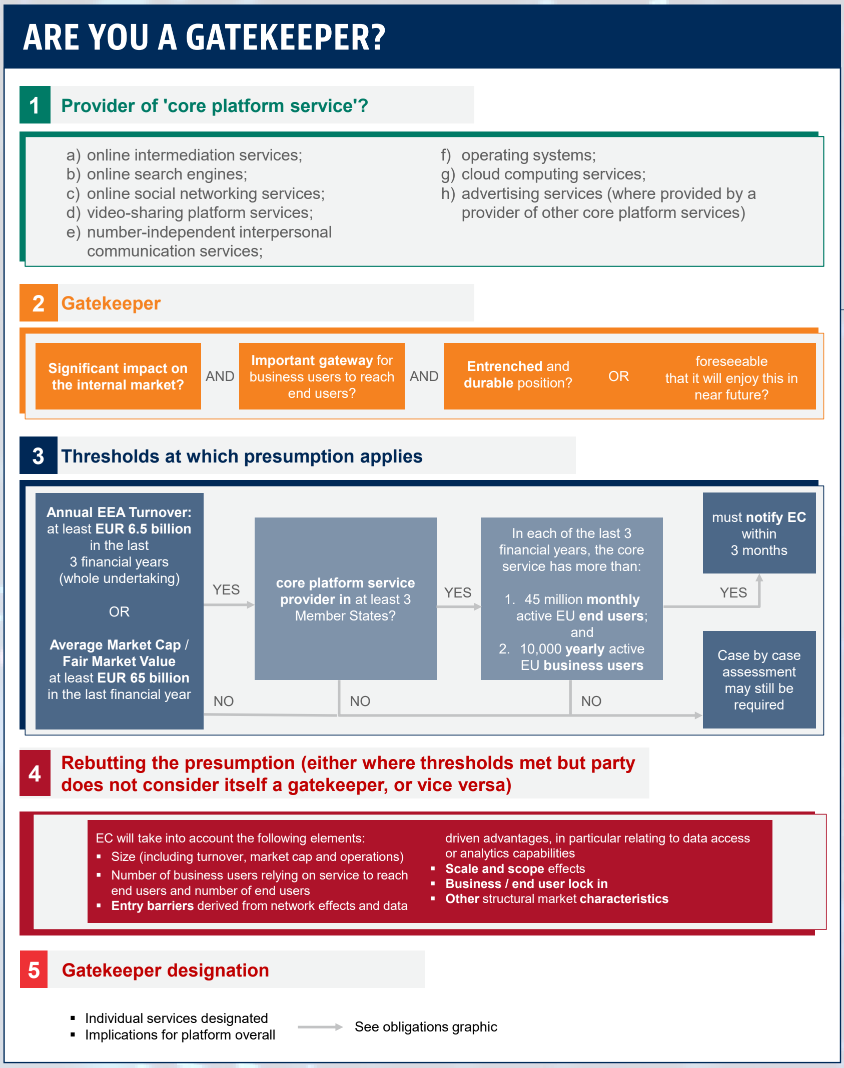
Unlike the parallel DSA, which builds on – and materially expands some – existing e-commerce rules, the DMA introduces a somewhat disparate list of obligations – largely not already present in any form in existing law. Instead, the DMA is best characterised as the Commission seeking to legislate to achieve the same outcomes as the Commission has tried to achieve via competition actions it has brought against key platforms, most of which are still unresolved or under appeal.

Scope

If passed, the DMA will apply to "gatekeepers" which provide "core platform services". Core platform services are defined to include: online intermediation, online search engines, online social networking, video-sharing platforms, number-independent interpersonal communication services, operating systems, cloud computing services, and advertising services. Most of these terms are defined in other pieces of EU legislation such as the AVMS Directive, the Copyright Directive, the new European Electronic Communications Code, or the Platform to Business Regulation. The three elements of the gatekeeper definition will be presumed satisfied where certain quantitative thresholds are met. "Emergent gatekeepers" are also caught, where it is foreseeable that a service will meet the criteria in the near future.

The presumptions are rebuttable in either direction: platforms can argue they are not gatekeepers despite meeting the thresholds; or they may be deemed gatekeepers by the Commission nonetheless. The designation applies to both the specific service and the corporate group overall (with obligations mostly applying to the specific service in question). The onus is on the platform to self-assess, but the Commission says a "market investigation" will be launched to confirm statuses in some cases.

Return to Contents



ARE YOU A GATEKEEPER?

1 Provider of 'core platform service'?

a) online intermediation services;
b) online search engines;
c) online social networking services;
d) video-sharing platform services;
e) number-independent interpersonal communication services;
f) operating systems;
g) cloud computing services;
h) advertising services (where provided by a provider of other core platform services)

2 Gatekeeper

Significant impact on the internal market? AND **Important gateway** for business users to reach end users? AND **Entrenched** and **durable position?** OR foreseeable that it will enjoy this in near future?

3 Thresholds at which presumption applies

Annual EEA Turnover: at least **EUR 6.5 billion** in the last 3 financial years (whole undertaking)

OR

Average Market Cap / Fair Market Value at least **EUR 65 billion** in the last financial year

YES → **core platform service provider** in at least 3 Member States?

YES → In each of the last 3 financial years, the core service has more than:

1. 45 million **monthly** active EU **end users**; and
2. 10,000 **yearly** active EU **business users**

YES → must **notify EC** within 3 months

NO → Case by case assessment may still be required

4 Rebutting the presumption (either where thresholds met but party does not consider itself a gatekeeper, or vice versa)

EC will take into account the following elements:

- Size (including turnover, market cap and operations)
- Number of business users relying on service to reach end users and number of end users
- **Entry barriers** derived from network effects and data driven advantages, in particular relating to data access or analytics capabilities
- **Scale and scope** effects
- **Business / end user lock in**
- **Other** structural market **characteristics**

5 Gatekeeper designation

- Individual services designated
- Implications for platform overall

→ See obligations graphic

Click to enlarge

What obligations apply under the DMA?

Gatekeepers will then be subject to new obligations in respect of how they operate specific services, with a limited number of obligations applying to the whole undertaking.

Obligations range from those seeking to:

- govern relationships between platforms and their business users – including a number intended to facilitate competition via other channels, aimed at reducing perceived exploitation by platforms, or preventing discrimination between the platform's own and competing services operating over the "gatekeeper" service;
- prevent lock in or to help promote new entry – including through promoting end user choice, data portability or interoperability, and obligations stipulating business user or third party access to data;
- address perceived issues around collation of data across ecosystems, including requiring end user consent for data to be combined across services, and an annual disclosure requirement on profiling techniques used; and
- enhance transparency between platforms and advertisers specifically.

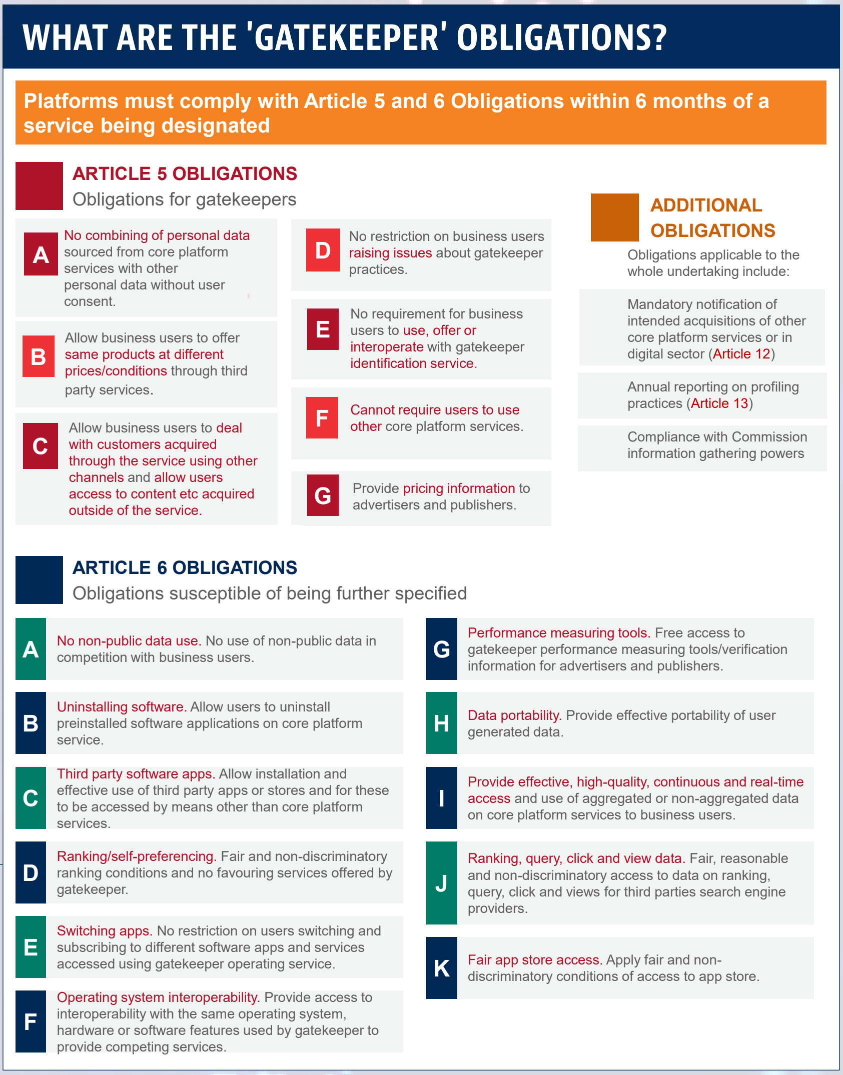
The reader will note some overlap, and expansion of, certain requirements that already exist to some extent under the GDPR and the P2B Regulation in particular.

Further, gatekeeper undertakings are required to inform the Commission of any intended merger involving another provider of core platform services or of any other services in the digital sector – irrespective of whether the normal EU Merger Regulation or national merger filing thresholds are met.

Return to Contents

This is a material new requirement, and comes on top of the UK's recently announced plans to introduce new notification requirements for several industries, including many that might also be covered by this proposed new DMA requirement in the EU.

Emergent gatekeepers will be subject to a narrower pool of obligations (i.e., only those necessary to prevent them from achieving an entrenched and durable position), and it will be possible for all gatekeepers to request suspension of obligations or exemption for public interest reasons.



WHAT ARE THE 'GATEKEEPER' OBLIGATIONS?

Platforms must comply with Article 5 and 6 Obligations within 6 months of a service being designated

ARTICLE 5 OBLIGATIONS

Obligations for gatekeepers

- **A** No combining of personal data sourced from core platform services with other personal data without user consent.
- **B** Allow business users to offer same products at different prices/conditions through third party services.
- **C** Allow business users to deal with customers acquired through the service using other channels and allow users access to content etc acquired outside of the service.
- **D** No restriction on business users raising issues about gatekeeper practices.
- **E** No requirement for business users to use, offer or interoperate with gatekeeper identification service.
- **F** Cannot require users to use other core platform services.
- **G** Provide pricing information to advertisers and publishers.

ADDITIONAL OBLIGATIONS

Obligations applicable to the whole undertaking include:

- Mandatory notification of intended acquisitions of other core platform services or in digital sector (Article 12)
- Annual reporting on profiling practices (Article 13)
- Compliance with Commission information gathering powers

ARTICLE 6 OBLIGATIONS

Obligations susceptible of being further specified

- **A** No non-public data use. No use of non-public data in competition with business users.
- **B** Uninstalling software. Allow users to uninstall preinstalled software applications on core platform service.
- **C** Third party software apps. Allow installation and effective use of third party apps or stores and for these to be accessed by means other than core platform services.
- **D** Ranking/self-preferencing. Fair and non-discriminatory ranking conditions and no favouring services offered by gatekeeper.
- **E** Switching apps. No restriction on users switching and subscribing to different software apps and services accessed using gatekeeper operating service.
- **F** Operating system interoperability. Provide access to interoperability with the same operating system, hardware or software features used by gatekeeper to provide competing services.
- **G** Performance measuring tools. Free access to gatekeeper performance measuring tools/verification information for advertisers and publishers.
- **H** Data portability. Provide effective portability of user generated data.
- **I** Provide effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data on core platform services to business users.
- **J** Ranking, query, click and view data. Fair, reasonable and non-discriminatory access to data on ranking, query, click and views for third parties search engine providers.
- **K** Fair app store access. Apply fair and non-discriminatory conditions of access to app store.

Click to enlarge

Penalties

Potential fines for non-compliance will be significant (up to 10% of worldwide total turnover), with periodic penalty payments also an option. Structural remedies (including break-up) may be available for systematic non-compliance (i.e., three incidents of non-compliance or fining decisions in the last five years) where behavioural remedies would not suffice and "where there is a substantial risk that systematic non compliance results from the very structure of the undertaking concerned". Interim measures will be possible on a prima facie finding of infringement. This is also particularly significant, with the Commission having the power to exert early pressure on target enterprises. Given the number of Commission enforcement actions overturned on appeal in recent times, this is of particular note.

Investigative powers

While the mooted concept of a standalone "NCT" market investigation tool has been axed, there is provision for various – defined in scope – "market investigations" amongst the DMA proposals: to confirm gatekeeper definition, to investigate systematic non-compliance, and to investigate new core platform services and practices (i.e., to ascertain if the regulation needs updating).

Investigative powers include the power to request information (and to mandate a response) as well as the power to carry out interviews and dawn raids.

What next?

There is likely to be at least 18-36 months before these proposals pass into law, during which time Member States, the European Parliament and other stakeholders will have a chance to feed in their views. The European Parliament's Internal Market and Consumer Protection ("IMCO") Committee has been designated as the main Parliamentary committee for both the DMA and DSA, with identity of the Rapporteur yet to be published at date of writing. Introductory materials prepared by the Commission for discussion with IMCO are available **here**. Details of relevant Council working groups were yet to be released at time of writing.

We suspect there will be significant push back on a range of issues, such as:

- **The substance itself –** whether there's a need at all for this type of regulation (given the existence of competition law, P2B Regulation, the Copyright Directive, GDPR, etc) and, even if there is, whether the regulation takes the right form (more on which below);
- **Definitional issues –** although the Commission says delegated acts will provide more detail, the gatekeeper tests and thresholds afford the Commission a wide margin of appreciation: what is the meaning of "significant" market impact where thresholds aren't met, how should one predict enduring power, and why should activities over only three Member States suffice to clinch this regime;
- **Procedural issues –** including how the mandatory merger notification will work and how much information the Commission will demand to see - in particular relating to deal "rationale";
- **Coexistence –** mapping out how this legislation will sit alongside existing sectoral rules and other legislation, in particular data privacy.

A key point of contention will be the "do's and don'ts" approach to defining obligations.

- Articles 5 and 6 currently read like a "who's who" of cases the Commission has tried to bring under Article 102. It's backwards looking and oddly specific in some respects. Obligations are not arranged thematically, according to ends sought, and appear disparate.
- In other aspects, the list appears overarching – for instance, the apparent blanket ban on various forms of self-preferencing. The Recitals point to the harm self-preferencing causes to competing business users, but do not leave space for a case by case assessment of what will often be highly complex facts. While the UK's parallel approach (in recent CMA Advice to the government on new legislation in this field) recognises the need for differentiated obligations in light of firms' differentiated business models, the EU proposal advances catch-all obligations – albeit conceding that Article 6 obligations "may be susceptible" to further refinement as between the parties and Commission.
- The proposed regulation is also premised on the idea that the Commission can define what a well-balanced market should look like. Tipping of the market in favour of one player is presumed harmful in all instances.

Further, interaction with Member States – and other wider initiatives in this sector – will be complex:

- While describing the regulation as "harmonising", the Commission notes that the DMA is "without prejudice" to Member States' ability to legislate against undertakings "other than gatekeepers" or even to impose additional obligations on gatekeepers.
- It remains to be seen how national initiatives will seek to align themselves with the new DMA, or whether Member States will press ahead with their own national solutions. Revisions to German competition law (see our alert on this **here**) contain a number of substantive overlaps with the DMA, in particular the new provisions addressed to "undertakings with paramount significance for competition across markets", which empower the German Federal Cartel Office to prohibit specific practices by such firms.
- In the meantime, the proposed new UK regime, while equivalent in many respects to the DMA, is not identical, notably introducing "high level principles" (in addition to narrowly defined rules), which may result in a divergent approach further increasing complexity around compliance issues.
- Accordingly, at this stage, there is a real prospect of different regimes applying across Europe.

However, case by case enforcement under Article 102 might be predicted to drop, as firms comply with the new regulatory regime.

As for the DSA, see our separate article in this publication **here** for an overview, and **watch this space...**

Trade wars and protectionism: Digital sovereignty under attack?

Alison Stafford Powell
Partner
Palo Alto
alison.stafford-powell@
bakermckenzie.com

The COVID-19 pandemic has provided an economic boost to many in the TMT sector. Yet, the sector has simultaneously found itself at the center of disruptive global trade wars faced with growing protectionist trade policies. Trade wars have essentially become tech wars as geopolitics collide with technological innovation amid increasingly tech-intensive economies. Governments have wielded a full panoply of tools from sanctions to export controls, from import restrictions to tariffs, from procurement bans to foreign investment controls, targeting key industry players in the name of national security and in pursuit of digital sovereignty.

The concerns underlying these measures are so deeply rooted and broadly held that we are unlikely to see a change at the macro level, certainly in the near term. While companies have become more adept at responding and adapting to disruptions in the technology supply chain, the challenge will be how to better anticipate and influence the regulatory map for the coming years to minimize the risk of a fragmented approach that would be detrimental to providers and users alike.

Know your end user and end use - who is using your products and technologies and for what purpose?

Recent years have seen growing policy concerns over the misuse of technologies in support of the expansion of civil/military fusion programs, electoral interference, cyber crime, cyber surveillance, censorship, human rights violations. Yet many of the technologies so used are commonplace and can be utilized for good aims and for ethical purposes. To tackle misuse, governments are deploying end-user and end-use based restrictions to curtail the transfer of even basic technologies to particular targeted "bad" end-users or end-uses. Examples include blacklistings by the US, EU and other governments of certain individuals, entities, and even cryptocurrency addresses involved in such activities, as well as stricter controls on exports to military end-users and military end-uses.

These measures have a proven quick and chilling effect on cutting the targets off from access to key technologies, financing and markets - particularly as they are often accompanied by the zero-risk tolerance approach of banks, lenders and insurers towards being seen as supporting such activities, even if otherwise lawful. Mitigating these compliance risks is a challenge, particularly for end-use screening which cannot readily be automated; companies will need to take a more holistic, cross-functional and connected approach to their transactional compliance screening.

Combatting fragmentation due to competing controls on technology transfers and emerging and foundational technologies

Export controls have long been a tool to protect a country's technological "crown jewels" and this is particularly so now as the US, EU, China and other countries take steps to limit outbound transfers of critical emerging and foundational technologies to prevent a dilution of their digital sovereignty.

Return to Contents

Key technologies of concern are 5G, additive manufacturing (3D printing), AI and machine learning, advanced surveillance technologies, robotics, biotechnology, advanced computing technology, quantum technology, position, navigation and timing technologies, amongst others. Enabling technologies, such as tooling, testing, and certification equipment, particularly in the semiconductor and 5G space, are also a continuing focal point for tighter export controls.

China's own recent adoption in December 2020 of a new, long-awaited Export Control Law is a game-changer for anyone producing in, and exporting from, China. This came on the heels of China's expansion of its technology import and export controls to cover broader swathes of emerging information processing technologies and represents China's first attempt at a comprehensive export control regime. It includes several familiar features drawn from EU and other multilateral export control regimes, but we may expect a unique China spin. While the implementing rules and details have yet to be published, companies need to gear up now to expand their compliance programs to address this new regulatory framework and consider the impact on their cross-border R&D and manufacturing operations so as to minimize delays and potential hurdles down the road.

Beside the increased regulatory burden, such barriers to sharing developing technologies across borders risk fragmentation across markets, with differing product standards for different markets resulting in higher costs to companies and consumers. It is incumbent upon companies to follow these export control developments closely and to provide detailed input either individually or via industry associations throughout the rule-making process to ensure that the resulting controls reflect a fair and pragmatic balance between national security concerns and commercial realities without stymying healthy technological competition and advancement.

Procurement restrictions - who and what is in your supply chain?

Digital sovereignty concerns will continue to affect the TMT supply chain. We have seen a tendency towards countries implementing restrictions to preserve the integrity of critical supply chains including in the critical infrastructure, telecommunications/5G, digital economy, bulk power supply, and critical mineral sectors, amongst others. A prime example is the US Clean Network Program, a bipartisan effort designed to combat the "long-term threat to data privacy, security, human rights and principled collaboration posed to the free world from authoritarian malign actors". These measures are designed to curb the use of certain foreign technologies in domestic critical supply chains, both public and private, and even block access to procurement opportunities for suppliers that choose to use targeted foreign technologies and equipment for their own internal business use. Companies will need to map their end-to-end supply chains to understand what parties and inputs are involved and may need to make hard choices to preserve certain business at the expense of other supplier relationships.

Foreign direct investment constraints

National security concerns over intense reliance on key technologies and data will also continue to drive a tightening of foreign investment review regimes even in countries with traditionally more open investment environments. Recent scrutiny of foreign investments in traditionally lower risk sectors, such as social media, dating apps and so forth demonstrate the reach of these concerns. Companies should expect scrutiny over broader types of cross-border transactions beyond typical M&A, such as fund investments and financings, and should plan and prepare for conditions and demands for commitments, including potentially restructuring of deals and foregoing of governance rights.

Outlook

The shifting geopolitical landscape will continue to expose vulnerabilities, particularly with respect to self-sufficiency in key technologies. Decoupling and fragmentation is not an option, but neither is the traditional form of globalization. Looking ahead, companies will need to tackle these issues proactively by engaging to shape the regulatory dialogue and also holistically through cross-functional teams to both mitigate risks and identify opportunities in the changing landscape.

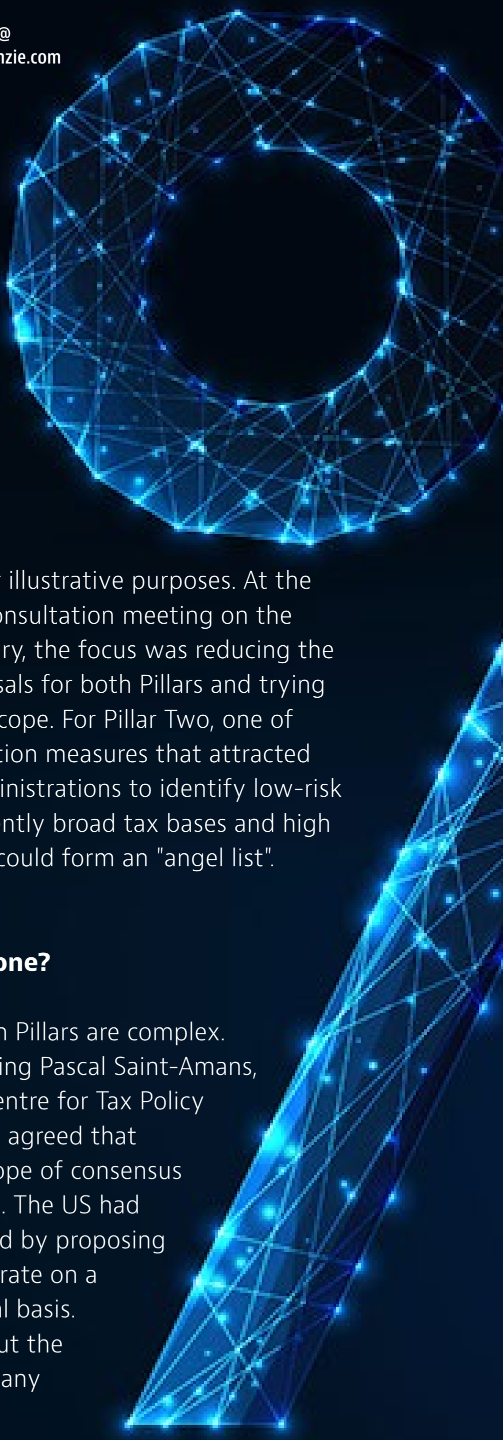
Taxing the digital economy: Still striving for consensus

Kate Alexander
Partner
London
kate.alexander@
bakermckenzie.com

Emily Maguire
Associate
London
emily.maguire@
bakermckenzie.com

Jill Hallpike
Knowledge Lawyer
London
jill.hallpike@
bakermckenzie.com

A new global regime for taxing the digital economy has still not been agreed upon. COVID-19 has caused the OECD's original deadline of the end of 2020 to slip to mid-2021. There is cause for optimism, with widespread support for the OECD's two-pillar approach and hope that the Biden administration will take a more multilateral approach to tax matters, increasing the chances of consensus. However, agreement is not guaranteed and there is still work to do, including gaining support from developing countries for the current proposals. Businesses will need to keep a close eye on developments over the next few months in order to prepare for the changes to come.



Where are we now?

The Inclusive Framework, a group of 137 countries that includes the OECD member countries and many others, had a virtual meeting in July 2020. Instead of agreeing then, as originally planned, on a framework that could be put to G20 ministers in the autumn, they committed to producing “Blueprints” for each of the two Pillars, with the aim of reaching consensus in 2021. Reaction to the delay has been mixed. The European Commission has accepted the deferral, but warned that an agreement cannot be postponed again. The Blueprints were released in October 2020. Pillar One focuses on profit allocation and nexus rules for automated digital services (ADS) and consumer-facing businesses (CFB) that both align taxation with value creation and, crucially, grant additional taxing rights to market jurisdictions. Examples of activities that are ADS for these purposes include: online advertising, search engines, gaming, cloud computing services and social media platforms. Pillar Two puts forward a Global Anti-Base Erosion (GloBE) proposal that would introduce a minimum tax rate for multinational groups (not just tech businesses) wherever they operate. The rate has not yet been agreed upon, although the Blueprint uses 10-12% for illustrative purposes. At the OECD's (virtual) public consultation meeting on the Blueprints on 14-15 January, the focus was reducing the complexity of the proposals for both Pillars and trying to agree on Pillar One's scope. For Pillar Two, one of the suggested simplification measures that attracted support was for tax administrations to identify low-risk jurisdictions with sufficiently broad tax bases and high corporate tax rates that could form an "angel list".

What remains to be done?

The proposals under both Pillars are complex. Tax policy leaders, including Pascal Saint-Amans, director of the OECD's Centre for Tax Policy and Administration, have agreed that realistically there is no hope of consensus without the US on board. The US had previously created discord by proposing that Pillar One could operate on a “safe harbour” or optional basis. This had little support, but the US has been opposed to any global system for taxing

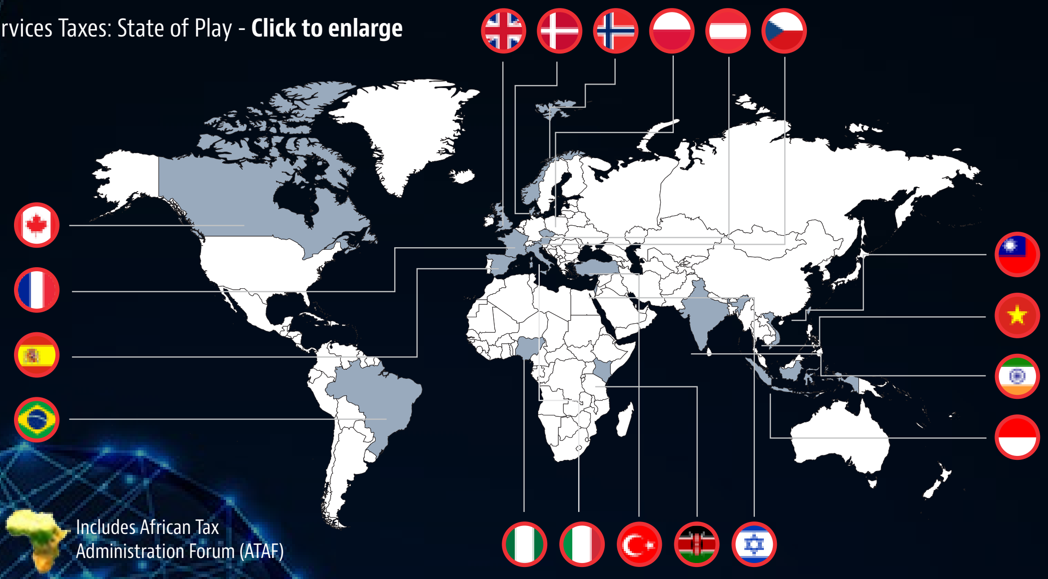
Return to Contents

the digital economy that would disproportionately affect US companies. Developing countries have expressed the view that the proposals are too complex. The UN Tax Committee has proposed an alternative route consisting of a change to its Model Tax Convention to allow a withholding tax to apply to payments in respect of automated digital services. How quickly the UN change, if approved, could be incorporated into treaties between UN member jurisdictions and third countries is not yet clear though.

WHAT ARE INDIVIDUAL COUNTRIES DOING?

Many countries have introduced their own digital services taxes (DSTs). Most of these are applied on gross income, meaning that even some loss-making companies may be liable to DSTs. Some countries have deferred implementation until the OECD reaches a consensus, but with any possible agreement delayed until mid-2021, more of the taxes are starting to take effect. France was the first to apply its own tax, introduced in July 2019 but retroactively effective from 1 January 2019. Generally, the French DST is aimed at online advertising and services companies, with some exceptions. France postponed collecting tax due for 2020 until mid-December, but has now resumed. This is despite the possibility of US trade sanctions, including tariffs on certain goods, with the US duty designed to balance the French DST paid by US companies. The UK DST came into force on 1 April 2020 and the first tax due under it is payable in February 2021. Turkey's DST is already in place, with other countries due to "go live" early in 2021. For example, Spanish DST is due to be introduced from early 2021. Although similar to the French DST, there are slight differences in terms of the definition of advertising services and transactions must be between 100% intragroup companies to be within the scope of the exemption for internal transactions. The EU is waiting to see what happens at OECD level, but is poised to introduce EU-wide measures if consensus does not materialise.

Digital Services Taxes: State of Play - **Click to enlarge**



HOW CAN BUSINESSES PREPARE?

The current uncertainty undoubtedly makes it difficult for businesses to plan and to estimate their likely exposure to new tax liabilities. With some DSTs already in force, many multinationals will already have established computational, compliance and payment systems to deal with their obligations. Without consensus, these systems will need to be expanded to deal with the growing number of DSTs around the world. Even if agreement is reached on the OECD's Blueprints, the proposals are complex and will require sophisticated processes to be set up in order to comply. Some countries have expressed optimism that the change of administration in the US might ease the path to global consensus, but that cannot be guaranteed. For the moment, businesses will need not only to watch OECD developments closely, but ensure that they have identified their exposure and liability to existing DSTs around the world. Once the picture becomes clearer, businesses will have to adapt either to a new international tax system or set up mechanisms to deal with a global array of tax and compliance obligations.

Return to Contents

The New Normal

2020 will be remembered as the year in which the global COVID-19 pandemic disrupted the world and our lives as we knew them. While we have not overcome the pandemic as yet, vaccines provide reason for hope that we will eventually put the crisis behind us. However, the impact of COVID-19 has been so profound that "normal" will look different to what we used to describe it before.

AT A GLANCE

- **Four tips for managing the transition to permanent (or temporary) remote work.** The 'work from home' experiment of the pandemic has been a success for many companies in the TMT sector and might be the new normal. Remote working brings many potential benefits, including savings in real estate, access to a wider talent pool, increased productivity and increased retention. But it also raises a variety of legal and non-legal challenges. We provide four essential tips to follow when going remote.

- **Supply chain — Building robust strategies.** In 2020, businesses across sectors experienced unprecedented shocks to their supply chains. In 2021, we expect companies in the TMT sector to focus on making their supply chains more resilient through identifying vulnerabilities, stress testing, diversification, digitalisation and contractual allocation of risk. In addition, we predict that during 2021 we will make great strides in making entire supply chains more ethical and sustainable.

- **Tech M&A post-pandemic: A return to normal (and beyond).** All of the indicators point toward 2021 being a busy year for M&A in the tech sector. At the time of writing, equity markets are at an all-time high, interest rates remain at historic lows, and an end to the deal-repressing pandemic is in sight. Looking ahead, it is reasonable to expect the leverage to move toward sellers, earnouts to be increasingly used to bridge valuation gaps, acqui-hires to remain popular, and corporate buyers to firmly embrace R&W/W&I insurance. To complete the picture, though, regulatory scrutiny of foreign investments is likely to continue, if not intensify.

- **Sustainability for tech companies — The environment and beyond.** Sustainable corporate governance will be a critical dimension of the business community's economic recovery from the impact of the COVID-19 pandemic and its response to the rapidly developing climate emergency and widespread global biodiversity loss. As high-profile global leaders in innovation, tech companies will be expected to be in the vanguard of renewal and change, as enterprises face heightened stakeholder expectations for environmentally sustainable and socially responsible business. We look at two central aspects: sustainable supply chain and circular economy policies.

- **Brexit and the telecommunications sector.** Much like other industries, the telecoms sector, considered part of the UK's critical national infrastructure, will be impacted by the Brexit trade deal which applies from 1 January 2021. We are highlighting some sector-specific issues that arise such as regulatory changes, cross-border telecom services, net neutrality and spectrum.

- **Content production — Back in action?** The pandemic has accelerated the surge in consumer demand for online content. On the flipside, during the first half of 2020, the film industry faced an almost complete shutdown. Sites were locked down and teams faced travel restrictions and quarantines. As lockdowns started to ease throughout the year, regulators allowed the filming activity to resume, subject to certain rules, protocols and guidelines. Compliance with these can be challenging as they are evolving and not always consistent. In addition, producers face various legal and practical challenges in ensuring safety during production.

Four tips for managing the transition to permanent (or temporary) remote work

Mike Brewer
Partner
San Francisco
michael.brewer@
bakermckenzie.com

Susan Eandi
Partner
Palo Alto
susan.eandi@
bakermckenzie.com

Caroline Burnett
Knowledge Lawyer
San Francisco
caroline.burnett@
bakermckenzie.com

Tech companies are using their own technology to make remote work easier and re-imagine the future of work.

Many are considering a more flexible workplace with some or all employees permitted to telecommute for some or all of the time even after the pandemic ends. These companies will maintain their physical office space (potentially with a reduced footprint) and the employees will remain tied to their current employer and office location (but gain greater flexibility). Others are looking at more radical change, minimizing or even eliminating physical office space and allowing employees to work permanently remote, whether in countries/states in which the company already has operations or anywhere else in the world.

Permanent remote working brings many potential benefits to tech employers including: savings in real estate, access to a wider talent pool, increased productivity, and increased retention. Of course, it also brings challenges, including how to maintain team culture, collaboration and engagement as well as preventing remote workers feeling isolated and digitally fatigued. Recognizing there are many interconnected legal considerations and drivers, including employee compensation and benefits, data privacy and trade secrets, corporate law, and corporate tax, here are four essential tips to follow when going remote.

Return to Contents

1

Set guardrails by choosing locations

While the simplest approach for determining locations for remote work is to limit employees to working from their primary residence only (which is often, but not always, in the same location as their office), that is rarely the reality. Even then, there will be various employment law issues to consider, including ensuring that telecommuting employees remain subject to company rules and expectations; implementing a compliant office expense reimbursement policy; clearly defining the workspace and work time to establish reasonable limits on the employer's responsibilities for accidents and illnesses that may occur; and more.

More often, however, the decisive point is whether to allow employees to relocate to states or countries where the company does not yet have a legal presence. If employees will only be allowed to work remotely from locations where the company already has a corporate presence and ability to payroll, that raises legal issues more akin to "scaling up" activities. If employees will be allowed to work remotely from locations where the company has no corporate presence or ability to payroll, then many of the legal issues raised when expanding into a new location are triggered. Consider that the mere presence of employees working remotely in a particular state or jurisdiction could constitute a presence of the employing entity in that location for corporate income tax purposes. Also, employer payroll tax and personal tax requirements are implicated. Applicable employment laws, rules on employee invention and intellectual property assignments and many other legal issues may defer to the place where an employee works as opposed to where the employer is based.

2

Design an application process with established criteria

As with any new program, it is important to set out a clear policy on the application process and eligibility criteria. A few key tips to mitigate legal risk and preserve flexibility include:

- developing template application requirements, such as minimum seniority, excluded positions, interview with management in the new location, whether a justification is required
- determining which job positions can be performed productively in a remote setting
- defining eligible locations and deciding whether to implement headcount limits per qualifying location
- establishing objective criteria for accepting and rejecting applications
- considering that once the remote work policy is implemented, it will be difficult for the company to reject remote work requests outside of the policy framework (e.g., a request to work remotely as a reasonable disability accommodation) based on business hardship
- clarifying within the communication related to this application process that the applicant is responsible for all changes in the individual's tax consequences as a result of relocations made in connection with the program

Return to Contents

3

Craft policies to support the remote model

There is a laundry list of issues to address when implementing a remote work program, all of which can be rolled into a Remote Worker Policy. For example, consider the following:

- salary/cost of living adjustments: these may be appropriate depending on the transferring employee's new location
- costs/equipment: address how the employer will provide remote workers with the equipment necessary to perform their jobs and whether the employer will cover certain costs of remote working
- timekeeping: the company might be required to track hours/overtime for remote workers under applicable local law
- rest periods: the company must provide mandatory rest breaks to remote workers under applicable local law
- business travel policies: these may need updating
- information security: remote working carries increased risks of misappropriation of confidential information and loss of trade secret status

4

Address data privacy implications head on

Privacy and security of company information is critical, particularly when you consider the sensitive information employees have access to and submit over wireless and wired networks: passwords, email addresses, personal identifying information, phone numbers, addresses, proprietary information, financial data, communication about customers and employees. The list goes on.

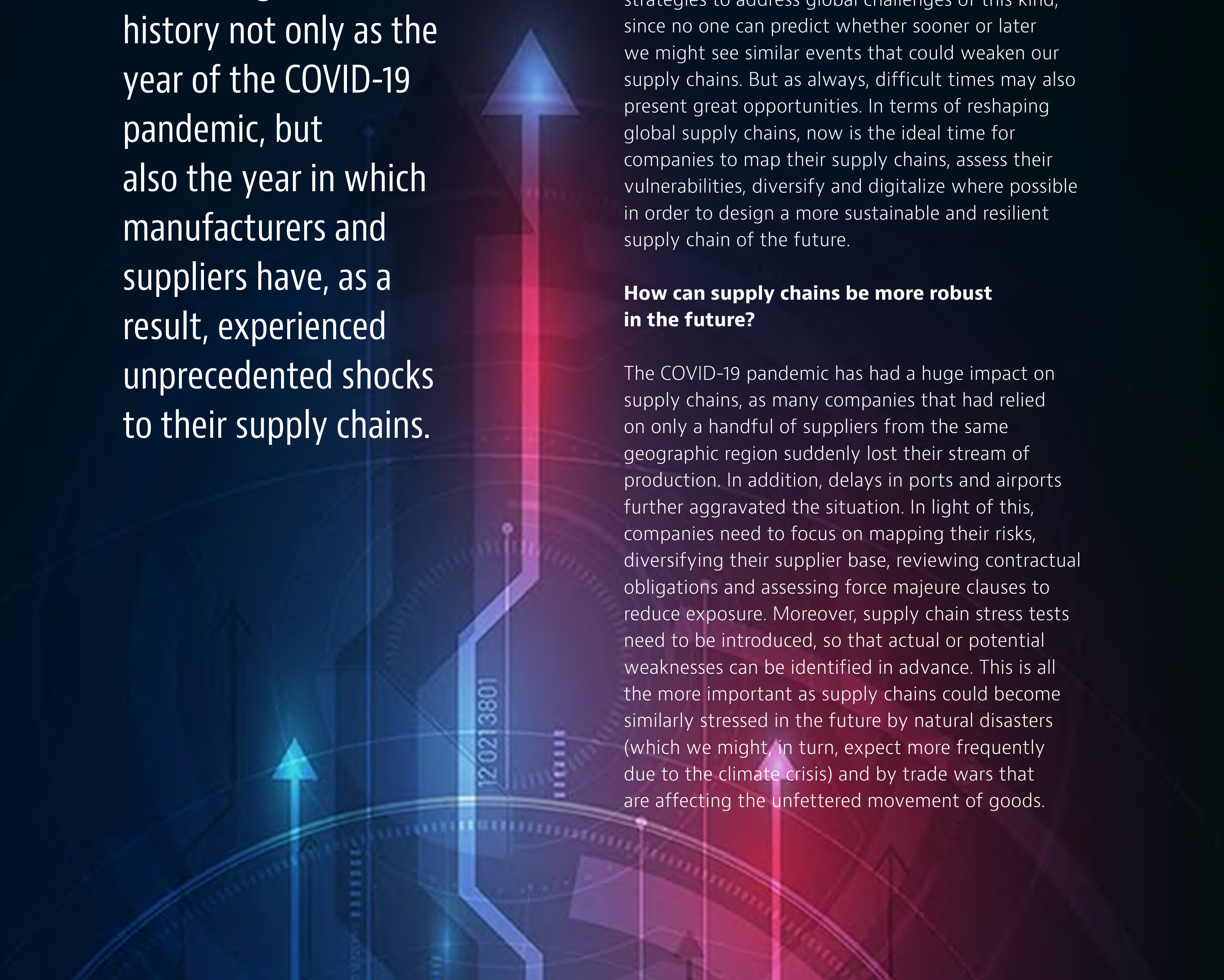
To maximize cybersecurity, we recommend companies to:

- implement appropriate telework policies to address data privacy (e.g., remote monitoring and "bring your own device" policies) and cybersecurity hygiene (e.g., no using personal accounts for company information and no using shared accounts on computers)
- restart and revamp cybersecurity training and messaging and review and update data breach response plans to address remote working related risks and scenarios, especially related to phishing attacks and cyber-hygiene possible mishaps
- document the updated policies, procedures, security controls, trainings, and mitigation measures that have been put in place; this is essential for litigation readiness
- remind employees that they have specific obligations in terms of data privacy and security, as part of their work duties
- perform an impact assessment to strike a reasonable balance between the need to protect data and information and the rights of employees, and to structure activities such as employee monitoring accordingly

Supply chain — Building robust strategies

Anahita Thoms
Partner
Dusseldorf
anahita.thoms@
bakermckenzie.com

2020 will go down in history not only as the year of the COVID-19 pandemic, but also the year in which manufacturers and suppliers have, as a result, experienced unprecedented shocks to their supply chains.



For the future, companies will need to find new strategies to address global challenges of this kind, since no one can predict whether sooner or later we might see similar events that could weaken our supply chains. But as always, difficult times may also present great opportunities. In terms of reshaping global supply chains, now is the ideal time for companies to map their supply chains, assess their vulnerabilities, diversify and digitalize where possible in order to design a more sustainable and resilient supply chain of the future.

How can supply chains be more robust in the future?

The COVID-19 pandemic has had a huge impact on supply chains, as many companies that had relied on only a handful of suppliers from the same geographic region suddenly lost their stream of production. In addition, delays in ports and airports further aggravated the situation. In light of this, companies need to focus on mapping their risks, diversifying their supplier base, reviewing contractual obligations and assessing force majeure clauses to reduce exposure. Moreover, supply chain stress tests need to be introduced, so that actual or potential weaknesses can be identified in advance. This is all the more important as supply chains could become similarly stressed in the future by natural disasters (which we might, in turn, expect more frequently due to the climate crisis) and by trade wars that are affecting the unfettered movement of goods.

Return to Contents

Implementing new technologies is a key factor

Companies can, however, influence future challenges by testing and introducing new technologies into their supply chain processes:

- IoT and blockchain can simplify and streamline the tracking of components through the supply chain including during the production process – their origin, location and quality. Smart manufacturing – which involves the aggregation and analysis of data from IoT, enterprise applications, blockchain and AI – is projected to sweep away the current processes and will create opportunities for process optimization.
- Robotics, 3D-printing and automation reduce exposure to human errors and increase efficiency. Algorithms can diagnose causes of failure before they have a negative impact. The entire operations technology is moving towards autonomous and connected manufacturing.
- The use of cloud computing solutions facilitates and helps managing supplier relationships so as to improve automation, speed and cost efficiency. Cloud computing also enables the coordination and real-time analysis of data to allow quick responses to changing demands.

Companies will need to embrace these innovations to remain competitive. On the other hand, companies also have to keep an eye on legal issues that are likely to arise, for example in the fields of data privacy, employment relationships and trade laws.

What role do human rights play in this context?

Ignoring human rights risks along the supply chain also poses a threat to companies for several reasons:

- Corruption, inhumane labor conditions and the exploitation of workers are just some of the possible human rights violations that can make the supply chain vulnerable. Thus, a human rights risk assessment is a key factor in any efforts to mitigate possible external risks to the functioning of the supply chain.
- Several national legislative bodies and the EU have implemented, or started working on, regulations to ensure that companies take their human rights responsibility even more seriously. For 2021, the EU plans to introduce legislation that requires EU companies to conduct mandatory human rights and environmental due diligence in their operations. France has passed a Law on Vigilance that prescribes comprehensive due diligence obligations with regard to human rights and ecological risks. Companies need to expect that other countries will follow and should therefore begin assessing their supply chain with regard to these topics.
- Investors are increasingly viewing a sustainable focus as a competitive advantage (rather than an additional investment or operational expenditure). Also, more and more business partners want their counterparties to not only be compliant partners, but also ethical partners. Following sustainability principles should therefore be an integral part of every company's strategy.

Outlook

Moving forward, we expect companies in the TMT sector to focus on making their supply chains more resilient through stress testing, diversification, digitalisation and contractual allocation of risk. In addition, we predict that during 2021 we will make great strides in making entire supply chains more ethical and sustainable.

Tech M&A post-pandemic: A return to normal (and beyond)

Leif King
Partner
Palo Alto
leif.king@
bakermckenzie.com

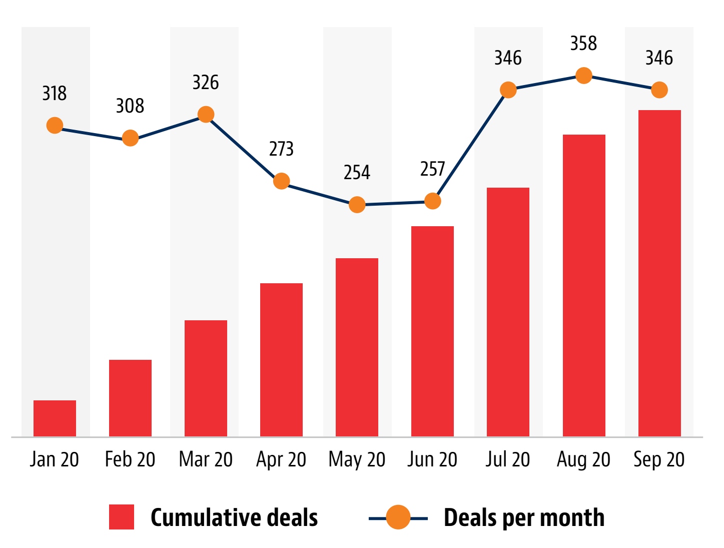
William Holder
Partner
London
william.holder@
bakermckenzie.com

Sze Shing Tan
Partner
Singapore
sze.shing.tan@
bakermckenzie.com

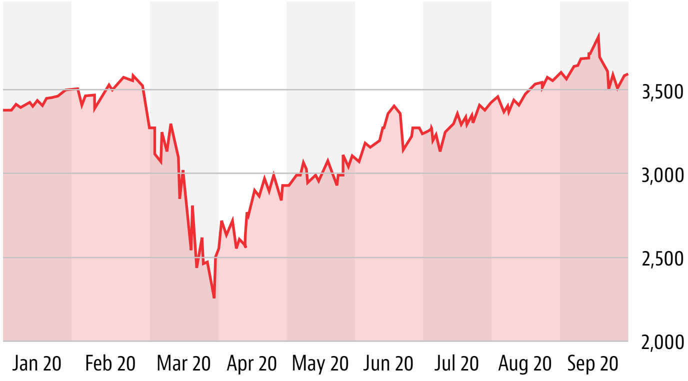
Amanda Bradley
Associate
Los Angeles
amanda.bradley@
bakermckenzie.com

Tech M&A is expected to be robust in 2021.

All of the indicators point toward 2021 being a busy year for M&A in the tech sector. At the time of writing, equity markets are at an all-time high, interest rates remain at historic lows, and an end to the deal-repressing pandemic is in sight. Global TMT M&A overall saw an impressive rebound in Q3 2020, surging by 34% in volume and 5.8x in aggregate deal value, according to KPMG. Anecdotally, we have seen an uptick in tech company hiring for M&A-related in-house functions, like M&A legal and corporate development, often a leading indicator of those businesses' intention to increase M&A as part of their overall growth strategies. And while fluctuating valuations and an uptick in regulatory scrutiny may provide something of a countervailing force, we fully expect that to be drowned out by these favorable macro trends.



Source: **KPMG, Q3'20 Global TMT M&A update**



Source: **Ycharts.com, S&P 500**

Leverage steadily moving toward sellers: At the start of the pandemic, this team had envisaged that the leverage in deal negotiations would shift heavily toward buyers, as it has in prior periods of economic distress (we were not alone!). And while that was true to some degree, we did not see a wholesale shift toward buyer-favorable terms in acquisition agreements. Why so? Sellers in the tech sector were, for the most part, not under pressure to dispose of their companies at bargain prices. Buoyed by continued access to venture capital, cheap debt and a robust IPO market, and encouraged by the belief that the pandemic-created dislocation was temporary, tech sellers could afford to be patient. As a result, we have observed that deal terms in acquisition agreements tended to be "middle of the road", striking a balance based on principles of fairness rather than the brute force of leverage. With some skepticism for any crystal ball exercise, we expect the field to tilt toward sellers after the pandemic eases and the power moves even more squarely into their hands.

Earnouts increasingly used to bridge valuation gaps: Pandemic economics have left us in a curious spot. Equity valuations are increasingly robust – even for companies with a "temporary" dip in fundamental valuation metrics like revenue or net income. Sellers are seeking high valuations, while buyers want to exercise at least some measure of discipline and restraint. Enter the earnout Fundamentally, this tool is a promise to pay for hitting milestones or projections after the transaction closes. We have observed an uptick in parties employing earnouts over the past year.

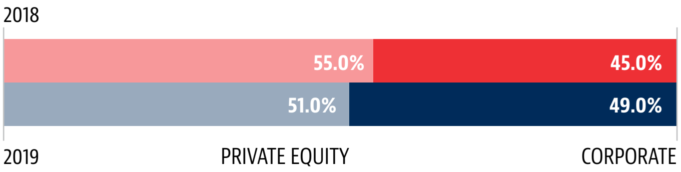
As lawyers we tend to focus on all of the "what ifs," which can be considerable when using a term that measures future performance based on a merged business. But despite the complexity and additional detailed terms to negotiate, we have seen great success in getting deals done by using earnouts to bridge the valuation gap.

Continued popularity of acqui-hires: Competition for talent remains fierce, especially in nascent tech subsectors like AI. The "acqui-hire" has proven to be an increasingly popular tool for acquiring talent, and related IP, while leaving behind legacy liabilities, customer contracts and, on occasion, redundant employees. The structure involves paying the target company in exchange for the right to hire employees and to acquire desired assets, while leaving the target with the responsibility of settling its remaining liabilities before liquidating. Buyers favor acqui-hires because they are faster and come with less risk than an outright acquisition. We have seen a burst of these transactions in 2020 and expect that trend to continue.

Corporate buyers firmly embrace R&W/W&I insurance: Once the province of PE buyers in heated auctions, representation and warranty insurance (or "warranty and indemnity insurance" to our European friends) has steadily worked its way into strategic M&A deals.

According to Marsh JLT Specialty, corporate buyers accounted for 49% of deals with R&W insurance, up from 45% in 2018, and continuing a years-long trend of strategic buyers increasingly becoming comfortable with accepting insurance in lieu of sizeable indemnification escrow accounts.

PRIVATE EQUITY VS CORPORATE



Source: **Marsh JLT Speciality, Transactional Risk Insurance 2019: Year in Review**

Return to Contents

Rise of foreign direct investment regimes

Slightly dampening this optimism has been a broad uptick in regulatory scrutiny of foreign investments, driven by trade tensions, geopolitical tailwinds and the COVID-19 pandemic exacerbating concerns about the robustness of critical supply chains. Even with the favorable macro trends discussed above, these dynamics risk threatening a de-globalization effect, particularly in relation to investment in sensitive industry sectors such as technology and telecoms. In many cases, tightening rules in this area also appear to conflate traditional national security concerns with industrial policy factors, or a strategic desire for supremacy in advanced technology areas.

In Europe, different countries have tightened their national rules, particularly in areas deemed important to pandemic response capabilities. The EU has also encouraged its Member States to take steps to protect critical assets from hostile takeovers. Meanwhile, in October an EU framework for harmonized screening of foreign direct investments became fully operational. This framework does not impose foreign investment regulations on those Member States that do not already have domestic regimes. However, it creates a coordination mechanism regarding inbound investments between the EU Commission and Member States, while – at the same time – establishing a core set of triggering areas for national Member State screening systems on grounds of security or public order.

The UK Government in November also introduced a long-awaited National Security and Investment Bill aimed at establishing a standalone investment review regime in the UK. We anticipate that this Bill will pass into law between March and May 2021.

Once enacted, the regime will significantly expand the UK Government's existing powers to review investments on national security grounds. Transactions in 17 sensitive industry sectors – including communications, data infrastructure, artificial intelligence, advanced robotics, quantum technologies, and satellite and space technologies – will for the first time be faced by a UK mandatory notification obligation, while there will also be a power for the UK Government to proactively call in for review a broad range of transactions in the wider UK economy giving rise to national security concerns.

Controversially, this call-in power will apply retrospectively to qualifying transactions entered into from 12 November 2020, to avoid a rush of M&A activity in the implementation period of the Bill falling outside the regime's scope.

Sustainability for tech companies: The environment and beyond

Graham Stuart
Partner
London
graham.stuart@
bakermckenzie.com

Renata Amaral
Partner
Sao Paulo
renata.amaral@
bakermckenzie.com

Sustainable corporate governance will be a critical dimension of the business community's economic recovery from the impact of the COVID-19 pandemic and its response to the rapidly developing climate emergency and widespread global biodiversity loss. As high-profile global leaders in innovation, tech companies will be expected to be in the vanguard of renewal and change, as enterprises face heightened stakeholder expectations for environmentally sustainable and socially responsible business.

Sustainable supply chains

In particular, tech companies are facing a future where responsible business conduct and sustainable supply chains are the norm. This is already evident in the EU, with the European Commission clearly envisaging that sustainable corporate governance and due diligence will be an essential part of the EU's recovery package and growth plan. In late October 2020, the Commission launched a widely anticipated public consultation on its Sustainable Corporate Governance Initiative, which asks how the EU can help businesses further embed sustainability into the corporate governance framework.

This consultation builds on a study of due diligence through the supply chain, published by the Commission in February 2020. The study's findings drew on submissions from 631 stakeholders including 334 business respondents coming from all sectors and of all sizes, operating in regions across the world. It found that only one-third of businesses in the EU currently undertake supply chain due diligence on human rights and environmental impacts; that the majority of those only assess first tier suppliers; and that the majority of companies take a more reactive than proactive approach to due diligence — they conduct infrequent audits and reviews, and potential risks only get raised to board level when major issues arise.

It is noteworthy that the majority of respondents in this study felt that voluntary approaches to address environmental and human rights issues in

Return to Contents

supply chains have failed to change, sufficiently for the better, the way in which businesses manage their responsibilities. In fact, the study's respondents were largely in favour of mandatory, enforceable, cross-sectoral EU due diligence laws to ensure legal certainty, a level playing field and a single harmonised standard for business relationships throughout the supply chain.

It appears certain that this consultation will lead to an EU legislative proposal in 2021 that will likely require companies across sectors in the EU to undertake mandatory environmental and human rights due diligence of their supply chains. This fits with a broader trend toward purpose-led corporate governance that takes into account environmental, social and governance concerns as a matter of transparency and diligence. It will sit alongside similar regimes in other regions, such as the California Transparency in Supply Chains Act and the Australian Modern Slavery Act 2018. Similar action is expected in Hong Kong (Modern Slavery Bill) and Switzerland (Initiative for Responsible Business Conduct). Alongside the growing number of these focused laws, there has been a shift in corporate governance standards mandated by company law to account for matters of corporate social responsibility.

Circular economy policies

Another certain challenge for tech companies is the implementation of circular economy policies that aim to ensure that resources which enter the economy remain part of manufacturing and consumption processes for as long as possible. These policies emphasize the reuse of natural resources, keeping products in the hands of the consumer for longer, enabling the restoration of ecosystems.

Currently, the planet produces around 50 million tons of e-waste every year, 80% of which ends up in unknown locations (see UN report: Time to seize opportunity, tackle challenge of e-waste: **here**).

There is growing pressure globally for this scenario to change. Countries around the world that used to accept electrical and electronic waste streams from other countries are no longer doing so and recently the United Nations has been very clear that countries need to develop clear policies on how to deal with e-waste. Accordingly, obligations to recycle or recover electrical and electronic devices are going to increase substantially as more and more countries look to repurpose valuable metals and other elements from electronic devices that are no longer fit for purpose — part of so-called "urban mining" initiatives. According to experts, around 50% to 60% of the world's tungsten is found in our devices and 26% of the world's tin is found in our laptops and other similar equipment.

Shifting from voluntary to mandatory standards

Many tech companies already see value in reinventing their processes in accordance with a purpose-led approach because it delivers growth, lower costs, boosts consumer engagement, supports consistency in demand and price, reduces risk in the supply chain, and builds trust with employees, consumers, investors, regulators and other stakeholders. Nonetheless, the expectation for sustainability initiatives is that governments move increasingly from voluntary adherence to mandatory compliance and, from there, to the potential for enforcement either by regulators or in civil litigation. Those companies that have not already made the shift and incorporated these considerations into their systems, controls, compliance and diligence should now consider the drivers to do so as the market moves toward wholesale change.

Brexit and the telecommunications sector

Jennifer Revis
Partner
London
jenny.revis@
bakermckenzie.com

Ian Walden
Of Counsel
London
ian.walden@
bakermckenzie.com

As the availability of telecoms infrastructure and services underpins much of today's economic (and social) activity across sectors, the UK considers the telecoms sector part of the UK's critical national infrastructure. Much like other sectors, the telecoms industry will be impacted by the Brexit trade deal, more formally the new Trade and Cooperation Agreement (TCA), which applies from 1 January 2021. In the following, we are highlighting some sector-specific issues that arise.

For a more detailed analysis of what Brexit means for the Technology, Media and Telecommunications sector, please click **here**.

Regulatory

The sector is regulated with the UK telecom regulatory framework mainly contained within domestic UK legislation (which implements the EU Directives that make up the "EU Regulatory Framework" on telecoms) and the enabling measures to support applicable EU Regulations. The EU Regulatory Framework regulates a wide range of issues, including mandating telecommunications network access, radio spectrum management, use of electronic communications data, number portability and consumer access to emergency services. It aims to harmonise national telecoms regulatory rules across EU Member States, to promote the liberalisation and competitiveness of telecommunications markets, and to protect customer and end user rights.

Return to Contents

Notably, the existing EU Regulatory Framework is currently being replaced by Directive (EU) 2018/1972 which establishes the European Electronic Communications Code (EECC). The EECC - to be implemented into national law by 21 December 2020 - addresses critical issues such as access to network infrastructure, regulation of new services and technologies (including over the top services) and spectrum management and assignment.

The UK government has transposed the EU Regulatory Framework (including the substantial provisions of the EECC) into UK law through national legislation. As a result, there will be no immediate consequences of Brexit on the general telecoms framework that applies in the UK. The existing national legislation will continue to be valid and applicable. However, telecoms businesses should monitor future developments for any divergence of the UK telecommunication regime from the EU regulatory framework which may develop over time. For example, the UK's transposition of the EECC excludes number-independent interpersonal communications services from the regime.

Cross-border telecom services

As of 1 January 2021, the UK is trading services with the EU on the basis of the WTO's General Agreement on Trade in Services (GATS). Accordingly, whilst a UK-established company will continue to be able to provide cross-border telecom services into the EU on the basis of GATS, some EU Member States require telecom service providers to have a legal presence in an EU Member State – either through a subsidiary or a branch / representative office – in order to obtain the necessary telecom authorisations. From now, a UK based entity would no longer fulfil this requirement and, if it intends to provide telecom services into countries in the EU / EEA, should check whether they would be subject to any such local laws.

Net neutrality

As of 1 January 2021, Regulation (EU) 2015/2120 which provides for open internet access and establishes common rules on equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights (so-called "Net Neutrality") will continue to apply to the UK, although in an amended form (see The Open Internet Access (Amendment etc.)(EU Exit) Regulations 2018). Accordingly, electronic communications service providers that continue to provide internet access services in the UK will need to remain compliant with Net Neutrality rules.

Spectrum

Following Brexit, the UK will no longer be subject to European Commission decisions and initiatives regarding the harmonisation of spectrum allocations and use across the EU. As a result, we could see the UK position on spectrum management and assignment deviate from the EU position. However, we consider major divergence unlikely as a harmonised framework is in the interest of UK operators and the UK will continue to be a member of the International Telecommunications Union, which harmonises certain uses of spectrum at a global level.

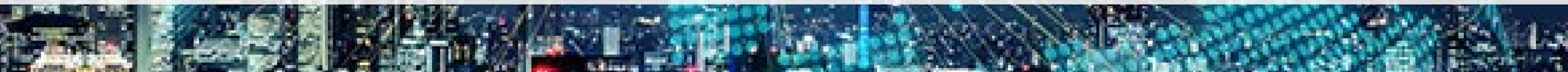
Funding schemes

Businesses active in the telecommunications sector may lose access to key funding schemes such as the Investment Plan for Europe which is intended to boost investment in digital infrastructure and, in particular, broadband.

Data roaming

Moving forward, UK consumers (including employees of UK companies) will no longer be able to rely on the EU Roaming Regulation which guarantees surcharge-free roaming when travelling throughout the EU and EEA countries. Whilst surcharge-free roaming will not be guaranteed from a legal perspective, the major mobile operators in the UK have stated that they have no current plans to change their mobile roaming policies (though this may to some extent depend upon how the roaming arrangements that UK MNOs enter into with MNOs around the EU develop).

While many businesses in the telecommunications sector have started preparing for Brexit long ago, this work will continue in 2021, now that we finally know the terms of this deal and begin to understand how it will be implemented in practice.



Content production: Back in action?

Carolina Pardo
Partner
Bogota
carolina.pardo@
bakermckenzie.com

In 2020, governments around the world adopted lockdowns and social distancing measures as a result of the COVID-19 pandemic, which almost completely neutralized outdoor "social distractors" and any competition that these could exert on digital, online and broadcasted content. Digital access compensated social distance for users in developed countries and in some developing geographies.

Yet, humankind craves the return to normality, and the "new normal" is an elusive moving target. Despite announcements on the availability of vaccines, it will take a while for them to reach many of us. Consequently, consumers can expect to continue to spend much of their leisure time watching digital and streamed content.

During 2020, United States consumers **increased their online activity by 25% on average**, which use was already quite significant pre-pandemic at almost seven hours a day. As a comparison, according to **Ofcom**, internet users in the UK spent **an average of four hours and two minutes online each day in April 2020**.

The Digital Economy and Society Index of the European Commission (DESI 2020) reported that during 2019, **85% of individuals in the EU used the internet at least once a week, with the most common online activities including listening to music, playing games and watching videos**. And this time spent online increased sharply during the pandemic.

The heavy reliance on digital products and internet use during the pandemic has increased the appetite for online content. This incremental surge for content demand has amounted to huge opportunities for film producers in a pre-COVID-19 world.

At the same time, the pandemic has challenged the film industry by forcing the reduction, postponement and even termination of many initiatives for new content production. Indeed, during the start of the pandemic in 2020, the film industry halted to an almost complete stop. Production sites were locked down and teams faced travel restrictions and quarantines.

These abrupt changes gave rise to a number of legal claims including breach of contractual clauses, disputes over force majeure allegations and conflicts related to cast and production insurance. This scenario also created new and material risks for those continuing on-site activity, such as talent, crew and casts, that have intensified pressures on content producers to properly handle health and safety concerns and data protection issues. All of this has contributed to increased costs for production activities.

Fortunately, as with most crisis situations, with challenges come opportunities. As a result, the film industry has seen creative new initiatives and different ways of working.

Production protocols — not one size

As lockdowns started to ease throughout the year, regulators allowed production activity to resume, subject to certain binding rules and protocols. In some cases, in addition to new laws at various levels of government, industry groups and trade organizations have developed their own non-mandatory guidelines. This means that the industry has had to adapt to applying countless sets of different rules to pursue production during the pandemic. Some of these guidelines have continued to evolve with the pandemic:

- In the United States, the Director's Guild of America together with **SAG-AFTRA**, **IATSE** and the **Teamsters** engaged in a joint effort from the production stakeholders and **published guidelines** on the protocols that are intended to unify the different rules. These guidelines include suggestions for producers to provide a safe working environment to the cast and crew for the resumption of film production during the pandemic. The guidelines include protocols regarding mandatory testing, personal protective equipment, department specific procedures and others.
- Similarly, the British Film Commission, published non mandatory Guidelines on Working Safely During COVID-19 in Film and High-end TV Drama Production. The Guidelines were updated on January 6, 2021, as a consequence of the national lockdown declared in England at the very beginning of the year.
- The Spanish Film Commission also prepared **distinct practice guidelines** to be used when shooting films within the Spanish territory after May 25, 2020.
- The European Film Commissions Network published the **links to guidelines** and protocols for film production in the European countries during the pandemic.
- The Australian Screen Sector Task Force issued **Guidelines** to be used by screen productions as guidance to develop their own COVID-Safe risk mitigation plan prior to recommencing work.

Thus, the industry, while prolific in creating recommendations and guidelines to allow content production to continue globally, has also become quite complicated as a web of requirements worldwide must now be considered prior to resuming the type of development enjoyed pre-pandemic.

Employment and data protection requirements

In order to resume filming activities, production companies need to be mindful of the health and safety challenges that in-person shooting presents during the pandemic.

Many of the guidelines issued by different governmental and industry bodies prefer continuous health screening as the best practice to avoid COVID-19 outbreaks during film production. In implementing such testing, production companies face challenges such as (i) deciding how to roll out the screening and testing procedures in the most efficient manner; (ii) determining which tests to use and how often to use them; (iii) understanding the laws applicable to the collection, processing and storage of sensitive personal data such as the data related to the screening and health of the cast and crew; (iv) implementing rules for off-site and distant collection of data; (v) anticipating what to do in case of a positive test result; and (vi) planning the ways in which to implement tracking and localization of employees, cast and crew after screening.

Insurance

Prior to the pandemic, insurance was already a major factor in all content production activities. Such coverage would insure production companies against risks related to property damages, bodily injuries and even death of cast and crew members. Financing of big production projects was unthinkable without adequate insurance. However, during the pandemic, traditional insurers have refused to cover losses resulting from COVID-19 or are requiring significantly increased premiums to provide coverage. This has pushed some film makers to adopt new forms of risk management and to self-insure. This may be an area in which crowdfunding and other disruptive ideas may start to proliferate to allow the show to continue.

In summary... the pandemic has created many, multi-faceted challenges for the content production industry from a legal perspective. These include risks relating to compliance efforts, contractual relationships, employee health and safety and insurance coverage, among others. But the production industry is a creative, innovative and evolving one that is well-positioned to invent new way of addressing the challenges. Accordingly, the post-pandemic content production industry will be one of the best-positioned to recover fully from COVID-19 obstacles and demonstrate new and better ways of working and creating.

Return to Contents

Data

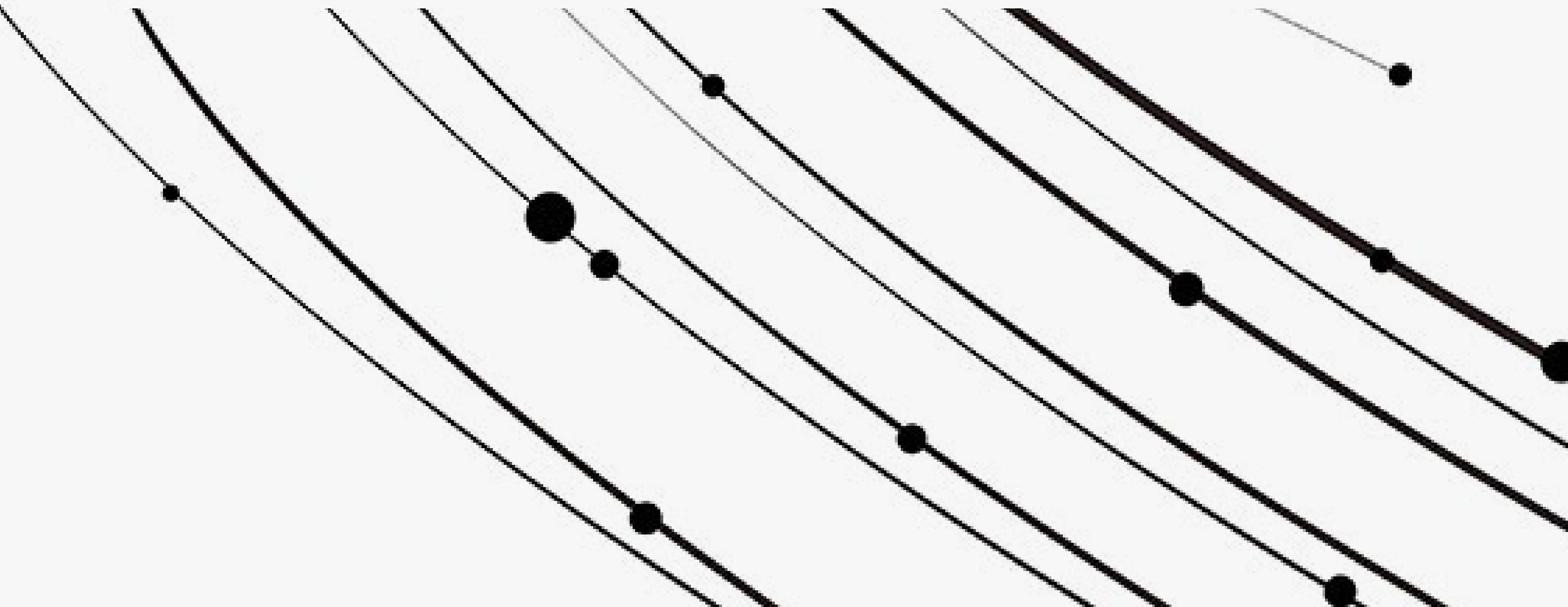
Data is an asset and underpins the digital economy. Businesses are looking to monetize data, privacy regulators are scrutinizing personal data processing, competition authorities are viewing data as a source of market power and governments are aiming for data sovereignty. There will be many developments in 2021 to watch. We cover a few key ones here.

AT A GLANCE

- **Data transfers: Survival strategies after CCPA, CPRA and Schrems II.** How do you solve a problem like Schrems II, the CCPA and CPRA? And how about other key challenges in 2021 such as potentially increased data residency requirements and more requests for encryption backdoors? We provide some practical suggestions on how business can manage this global complexity as they brace for what we term ABCD-type data regulation around the world — additional, broad, conflicting and diverse.

- **Online gaming privacy.** The global pandemic has accelerated growth in the video game industry with the games market estimated to have generated around USD $160 billion in 2020 (an increase of over 9% on 2019) and forecasters predicting similarly rapid growth for 2021. As they collect larger volumes of personal data and process such data in novel ways, developers are shifting focus on data privacy compliance. We take a look at some key privacy compliance concepts within the gaming context, including privacy by design, protection of minors, privacy issues surrounding the digital advertising industry, and data subject requests.

- **The rise of data class actions in the EU.** While the data class action map in the EU and UK is still fragmented and not yet comparable to what we see in the US, the volume of class actions relating to data breaches and misuse is on a steady rise in the EU and a trend to watch. Some EU jurisdictions already permit group actions outside the GDPR. There are also a number of recent legislative changes in relation to group actions which may significantly change the risk profile within certain jurisdictions depending on how they are applied. Businesses which may be exposed to potential group actions in Europe should, on an ongoing basis, identify their key jurisdictions and monitor developments pro-actively as the law changes.



Data transfers: Survival strategies after CCPA, CPRA and Schrems II

Lothar Determann
Partner
Palo Alto
lothar.determann@
bakermckenzie.com

In the near and mid-term future, businesses have to brace for ABCD-type data regulation: additional, broad, conflicting and diverse new laws around the world. As predicted in last year's looking ahead report (see page 7 **here**), the EU (with the **Schrems II decision, EDPB guidance** and new **SCC proposals**) and California (with its CPRA — see our client alert **here**) are outpacing each other in restricting data transfers in the interest of privacy and data protection.

At the same time, antitrust authorities are pressuring larger companies to make their data and platforms more accessible while the EU Commission launched a **new data access framework.** Also, several jurisdictions are eying data residency requirements and encryption backdoors to ease government access to data (including in a new EU draft resolution on encryption and India's new Personal Data Protection Law), despite the adverse impact on privacy and data protection (see author's World Economic Forum article on data residency **here**). The global economy needs a modernized, coherent framework for global data transfers (the WEF set out a road map **here**). Yet, companies have to comply with more and more diverse, complex, conflicting, and national or state-by-state regulations that pull and push them in various opposite directions. Every country seeks to protect the privacy of its residents from other governments and foreign companies, secure better access to data for itself and local companies, and protect its local industries from global competition.

Return to Contents

How do TMT businesses navigate this global complexity?

Recognizing the problem is half the battle. As a starting point, TMT companies should:

- **Assess the potential impact on their various business lines** and consider what markets they can and want to compete in, and with what offerings. Companies that want to develop or deploy cutting-edge machine learning, autonomous driving, personalized medicine, blockchain or customized advertising may have to adapt significantly if they want to be able to operate in California or the EU — at least they should consider operating in a different way compared to what they can do in other jurisdictions;
- **Distinguish between data regulation as a compliance area and a sales topic.** Customers and prospects worry about legal impediments and risks associated with using cloud storage, mobile apps, software-as-a-service, managed security, call centers, business process outsourcing, and a variety of other services that they are using for employee and customer data. Not only providers of information technology services are affected; more and more products come with connectivity, remote access for tech support, and other data processing features. Also, within affiliated groups, companies provide services to subsidiaries and parent companies. To succeed at selling data processing services and features, companies have to help their customers overcome compliance concerns. Thus, companies not only have to address their own compliance obligations. They also have to help customers and subsidiaries or affiliates address their concerns;
- **Offer their business customers contractual commitments that meet local compliance requirements** where the customers are based, as well as offer evidence and details regarding technological, administrative and organizational measures that TMT product and service providers are capable and permitted to supply under laws where providers are based to comply with contracts. To succeed at this task, providers have to upgrade and document their procedures and compile information that can be of comfort to their customers.

In this endeavor, TMT providers need to be positive to generate and preserve trust, but they cannot and do not have to be perfect. Realistically, few companies in the EU (or elsewhere) have sufficient resources to fully assess other countries' data protection law regimes, surveillance practices or compliance realities. Local or national data protection authorities are also hardly in a position to provide complete information or guidance when even the European Commission itself inevitably struggles with such assessments. The European Commission's **current list of "adequate" jurisdictions** contains a selection of only twelve countries after more than 25 years of assessments, and the Court of Justice of the European Union (CJEU) has invalided the Commission's adequacy decision regarding the United States twice in five years. In fact, the CJEU itself only addressed a few provisions of U.S. law, did not even begin to examine or compare data protection standards in actual practice within and outside the EU, and formulated due process requirements regarding national security programs that few countries outside or within the European Union can meet (on war and peace in cyberspace, see **here**).

In conclusion... providers should consider offering alternative products, including "on premise" solutions, as were common only 20 years ago. Companies around the world feel an increased pressure to keep personal data locally. This is already the case in countries with stringent data residency laws (including China and Russia) and in some of the EU Member States. Companies will likely have to brace for further disruptions if governments in the United States and other countries take a tit for tat approach with trade protectionism of their own, despite the generally positive potential of knowledge and information-sharing for economies and societies.

Return to Contents

Online gaming privacy

Sebastian Schwiddessen
Senior Associate
Berlin
sebastian.schwiddessen@
bakermckenzie.com

Ayako Suga
Senior Associate
Tokyo
ayako.suga@
bakermckenzie.com

Jonathan Tam
Associate
San Francisco
jonathan.tam@
bakermckenzie.com

The COVID-19 era has accelerated growth in the video game industry with the games market estimated to have generated around USD $160 billion in 2020 (an increase of over 9% on 2019) and forecasters predicting similarly rapid growth for 2021. Many video game companies are welcoming the opportunity to engage with gamers around the world who are spending more time at home and interacting with others virtually. But global privacy developments have also prompted video game companies to address heightened compliance obligations that apply to collecting greater amounts of data and processing it in novel ways.

Designing Privacy into Games

Video game developers are increasingly asking privacy advisors to sit at the table during the game design process, as the concepts of "privacy by design" and "privacy by default" become more commonplace. Some laws such as the European Union General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (Lei Geral de Proteção de Dados - LGPD) expressly require compliance with these principles, while other privacy laws, such as the California Consumer Privacy Act (CCPA), incentivize developers to think about privacy early on and often by codifying other general privacy principles that affect a game's functionality.

Integrating Technologies and Platforms

We anticipate that video game companies will continue to offer and engage in new data collection and sharing activities to give gamers more immersive experiences while tapping into additional revenue channels. This includes using cameras, sensors, microphones and other hardware, tracking technologies such as cookies, beacons, and geolocation monitoring, and enhanced features that allow users to stream content, socialize, mix realities, and link gaming and social media accounts.

> **As the online gaming data ecosystem grows more complex, it will become even more important for companies to be transparent about their privacy practices.**

Return to Contents

Protecting Minors

Children's privacy protection laws exist in every region and are typically actively enforced given the widely shared goal of shielding children from unsafe content and situations. Video game companies often have to make strategic decisions about whether to let children play their games, and then comply with all applicable children's privacy requirements, or use technical measures to block children from playing, and then limit the universal appeal of their games. These decisions are made more complicated by the fact that different jurisdictions define children's age thresholds differently and the online nature of many games makes it possible for children anywhere to play.

Advertising Conscientiously

Advertising through mobile games has been commonplace for some time, but now even console games that require an Internet connection are beginning to embrace dynamic digital advertising. We expect this trend to increase as more consumers spend more of their leisure time playing games than perhaps watching TV. At the same time, data protection laws and regulators are paying close attention to the privacy issues surrounding the digital advertising industry, with new laws — such as the California Privacy Rights Act and potentially the European Union ePrivacy Regulation — governing the use of cookies, profiling and other cross-context behavioral advertising techniques (our alert **here**). In Europe, there has been a spotlight on adtech practices for some time now with different regulators taking a close look at the adtech industry's data monetization practices and making it clear that they expect the industry to step up their data privacy efforts.

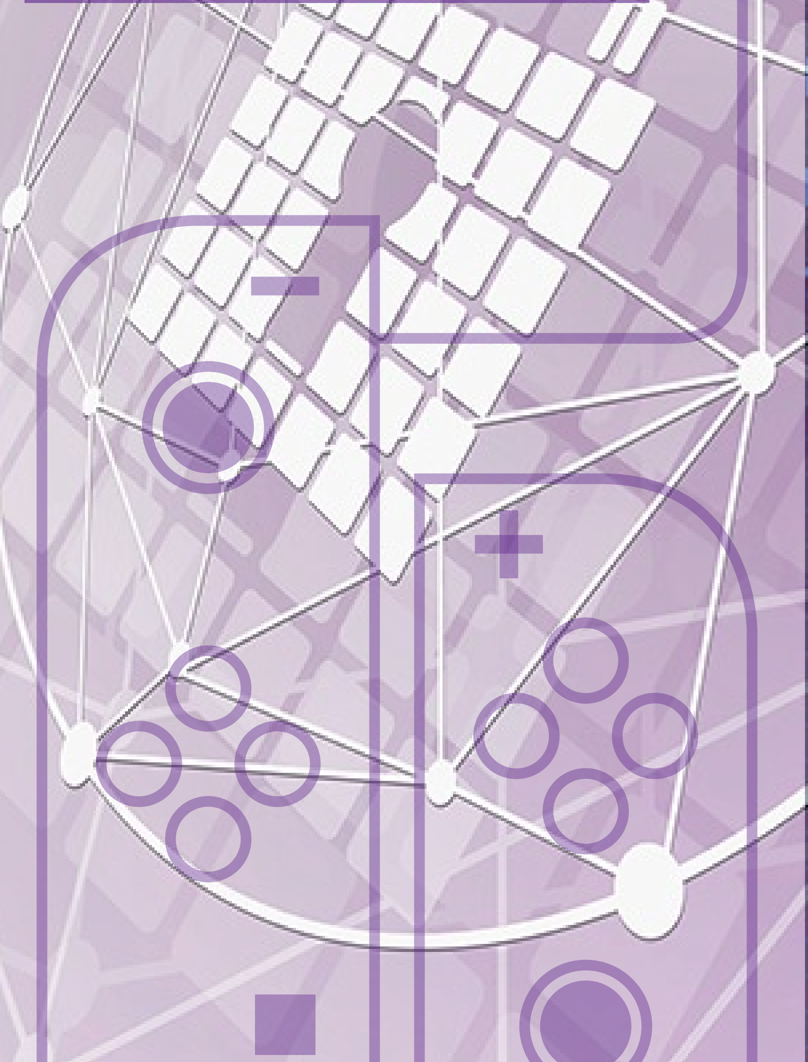
Responding to Data Subject Requests

Privacy laws around the world are giving data subjects new or expanded rights, with recent or upcoming developments in China, India, Brazil and Canada, to name a few. Video game companies should expect to receive higher volumes of data subject requests, including requests for access to copies of their personal information and data to be forgotten. Video game companies must navigate the sometimes inconsistent goals of comprehensively responding to requests while not disclosing information about how their internal algorithms and anti-cheating measures work so as to preserve the integrity and security of their games.

Getting on the Leaderboard

While the ever-shifting global landscape of privacy laws can be daunting for any video game business, there are tremendous incentives to getting privacy compliance right. Implementing a holistic compliance program that demonstrates to gamers that their personal information will be handled responsibly and securely will earn and keep their trust.

Better resourced regulators, ever more vigilant consumers and the public at large increasingly expect business to handle personal data in a trustworthy and transparent manner, and this trend is set to intensify.



The rise of data class actions in the EU

Paul Glass
Partner
London
paul.glass@
bakermckenzie.com

The volume of class actions relating to data breaches and misuse is on a steady rise in the EU. At the same time, there is a trend of individuals' rights relating to data being strengthened, with the rise of broad rights of action for individuals if their personal data is not processed in compliance with data privacy legislation. The data management chain is becoming ever more complex, usually involving the deployment of technologies supplied by multiple third (and beyond) parties, particularly as businesses rush to digitally transform and adopt new ways of working during COVID-19. As the compliance and litigation risk to data controllers increases, we expect to see more disputes between controllers and technology suppliers, data processors and sub-processors as to which entity was 'responsible' for a breach go to court or arbitration proceedings, rather than settling pre-action.

Claims for almost any breach of EU data protection legislation?

GDPR grants a right to receive compensation to "any person who has suffered material or non-material damage as a result of an infringement of this Regulation... from the controller or processor for the damage suffered." What that means in practice is the subject of several class action claims which have been commenced recently, so we are still waiting for precedent on key issues, at least in the EU. Many recent updates to privacy legislation around the world are based on GDPR, and contain similar - on their face broad - rights.

In Europe and the UK, despite the intention that GDPR would promote harmonisation, the data class action map is currently very patchy. While GDPR permits group actions to be brought by consumer associations, in practice this option has not been used at all in some jurisdictions (such as the UK), but is being used much more in other jurisdictions (such as Belgium, Italy and to some extent France). Some jurisdictions permit group actions outside the GDPR consumer mechanism, whereas others do not. Where such group actions can be brought, they are opt-in in some jurisdictions, opt-out (i.e., similar to U.S. class actions) in others, and some jurisdictions permit both but by different legal mechanisms. Such legal mechanisms include group litigation orders, which are opt-in, and representative actions, which are opt-out - both available before the English courts and both being used in a number of claims at the moment. There are also a number of recent legislative changes (such as the expansion of opt-in class actions in Italy in November 2020, and legislation to allow representative class actions for

Return to Contents

monetary damages in the Netherlands in early 2020), which may significantly change the risk profile within certain jurisdictions depending on how they are applied. Businesses which may be exposed to potential group actions in Europe should, on an ongoing basis, identify their key jurisdictions and monitor developments pro-actively as the law changes.

While data breach claims are on the rise and a real business threat, several of the recent class actions filed in EU jurisdictions focus on data misuse, rather than data breach. Data misuse claims do not involve the loss or theft of personal data, but instead focus on issues such as use of data without valid consent or use of data outside the scope of the consent obtained. Like data breach claims, data misuse actions are usually brought with the backing of litigation funders, who are looking for a return on their investment by way of damages. While there is very little useful case law to assist with quantifying damages for these claims, on their face these claims pose a significant risk - they are often quantified at hundreds of millions, or billions, of Euros / dollars. Faced with such potentially significant liability, controllers are likely to start looking harder at whether they can pass on some of that liability to third parties whose technology solutions they use.

Who is really responsible - or liable?

As an example, most e-commerce websites operate using a range of solutions purchased from third parties, which are then integrated into the overall website build. If a website is then the subject of a cyber-attack and customer data is compromised, this may raise complex technical issues such as: How did the attack happen? What was the root cause of the vulnerability which enabled the unlawful access? Was third party code deployed as intended, or was it used in a way which the third party had not intended, and did that unexpected use create the vulnerability?

When obtaining consent for use of personal data, given the level of technical complexity, data controllers may operate on the basis of certain assumptions as to how third party technology which they use or incorporate processes that data. If that understanding is incorrect, in some circumstances there might be claims that consent was not validly obtained and that the processing by the controller took place (in whole or in part) without valid consent.

In that situation: Did the controller misunderstand how the third party technology worked? Did the vendor mis-describe it? Or was the product deployed in a non-standard way which might change the position? It might be a combination of some or all of these issues. Sometimes, when new features are deployed, the way a product operates could change, or data could be inadvertently sent to new servers hosted in a jurisdiction not covered by existing consents or legitimate transfer mechanisms.

The scope of potential claims under GDPR is very broad, and the boundaries are likely to be pushed in the coming years, particularly in jurisdictions with aggressive consumer associations or where claimant law firms and litigation funders drive the market.

Outlook and takeaways

Claims for breaches of GDPR and similar laws around the world are still in their infancy, but the scope of rights of action granted to individuals is, on its face, extremely broad. Where local law allows for class actions, the quantum of such claims could potentially be very significant.

Understanding in detail how third party technology works, the risks of deploying it, defining carefully how it is going to be used and making sure that such use matches the contractual allocation of risk between the parties is going to be ever more important. This should also not be a one-off exercise when contracting. Technology stacks change, data is frequently put to uses which were not necessarily originally envisaged, and legal requirements and guidance evolve over time. **Having a holistic, detailed understanding of the technology the business uses, the risks it creates, how that technology relates to the data you collect and hold, with an up-to-date overlay of the legal position, and reflecting that risk where possible in contractual limitations is essential to effectively managing data liability.**

Return to Contents

Technology, Media & Telecommunications Industry Group

Key Contacts

Raffaele Giarda
Partner, Chair Global TMT
Rome

raffaele.giarda@
bakermckenzie.com

Kate Alexander
Partner, Tax
London

kate.alexander@
bakermckenzie.com

Lothar Determann
Partner, International
Commercial
Palo Alto

lothar.determann@
bakermckenzie.com

Adrian Lawrence
Partner, Technology & Media
Sydney

adrian.lawrence@
bakermckenzie.com

Carolina Pardo
Partner, Antitrust & Competition
Bogotá

carolina.pardo@
bakermckenzie.com

Zhenyu Ruan
Partner, Mergers & Acquisitions
Shanghai

zhenyu.ruan@
bakermckenziefenxun.com

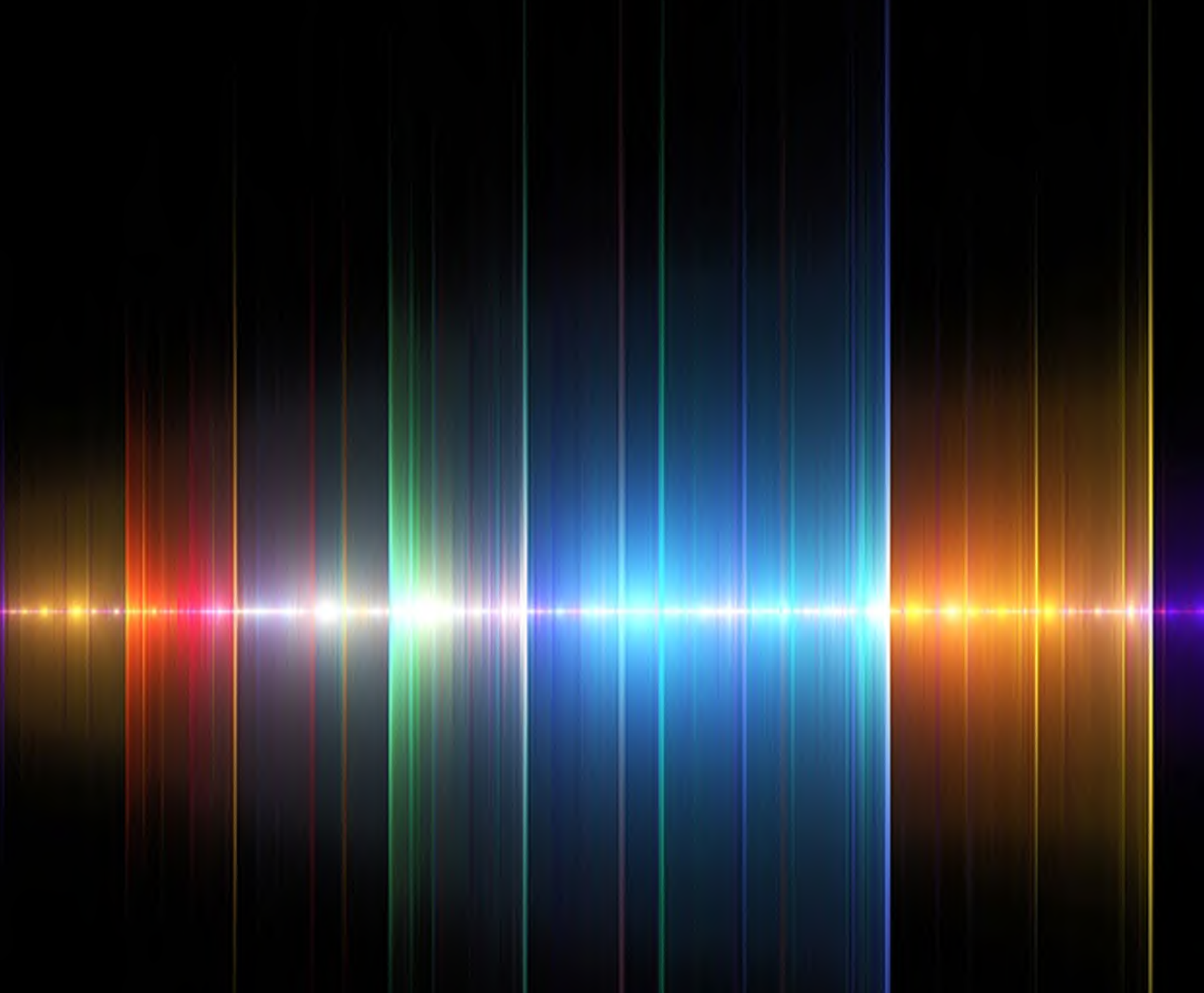
Editors

Anna von Dietze
Director of Knowledge,
Global Industry Groups
Dusseldorf

anna.vondietze@
bakermckenzie.com

Jason Irvine-Geddis
Knowledge Lawyer
Belfast

jason.irvineGeddis@
bakermckenzie.com



Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

bakermckenzie.com