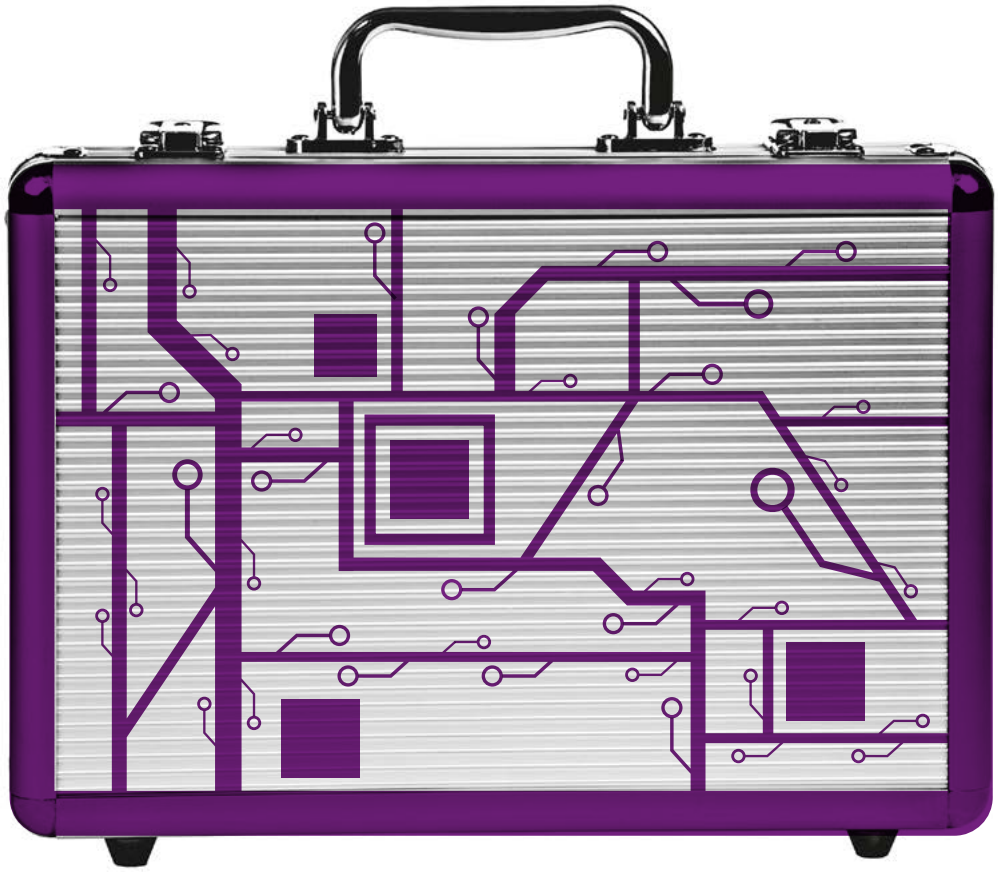
EVERSHEDS SUTHERLAND

TELESCOPE

TMT 2021 outlook

The shape of things to come

What will impact the TMT industry in 2021



Contents

Helping ensure your business moves forward

Contents

Click the below links to read the following articles

Nasser Ali Khasawneh
International TMT Sector Leader

We all thought that 2020 was an extraordinary year and a once-in-a-century moment. But 2021 is now promising to be equally exceptional.

We all thought that 2020 was an extraordinary year and a once-in-a-century moment. But 2021 is now promising to be equally exceptional. Sadly, the pandemic rages on all over the world, and the suffering continues on so many fronts. Yes, we can celebrate some good news, as vaccination takes hold across the globe. The speed with which vaccines were developed stands out as one of humanity's and science's greatest moments.

In the world of our sector (technology, media and telecoms), this moment of crisis is proving to be a pivotal moment. Technology is at the heart of almost every aspect of the response to the pandemic, whether it's in treatment, vaccine development, new working methods, proliferation of video calls and a lot more.

In such extraordinary times, horizon scanning is especially difficult. Nonetheless, our team of legal experts from around the world provide in this report their thoughts and predictions on a number of trends in the TMT sector as well as the legal issues and challenges around them. I co-authored an article about one of those trends that will only intensify in the coming period: social media regulation!

With the US election and many other events, the intersection of freedom of speech and social media could not be more on our minds. How legislative bodies react in this space will be one to watch in the coming months and I expect a great deal of activity.

We have many other articles in this report that I am sure you will find interesting. The digital tax debate rages on and the coming period will prove critical here. The way we work, and the mobile office, will be a subject close to all our hearts and there are some interesting technology and legal issues in this regard. Cutting edge issues such as defamation in an AI context, and deep fakes are also addressed.

These trends will all be affected by many factors in the coming months. For example, how the Biden administration deals with many of these issues will be something closely monitored by all concerned. We will be sure to address that in detail in upcoming reports.

It's fascinating to be part of this conversation. Like all of you, I feel blessed to be part of a sector that lies at the heart of everything in this perilous moment for the world. I am sure technology will help us make it through these challenging times and come out stronger. Inshallah as we say.

Contents

Digital economy tax reform: 2021 – "make or break"?

2021 could be the year in which international agreement is reached on one of the most fundamental and widescale rewrites of international tax law in over 100 years, with the potential to impact all businesses engaged in the digital economy. Alternatively 2021 could be the year in which the OECD concedes defeat in its efforts to seek broad international consensus, leading to tax chaos as countries pursue individual and different tax policies for the digital economy and digital businesses are required to comply with a plethora of potentially conflicting and overlapping digital tax regimes. The pressure is on for the OECD in early 2021 and digital businesses should follow developments closely.

OECD reforms

The OECD is currently attempting to achieve international consensus on proposed tax reform measures for businesses operating digitally. These reforms seek to reflect the global reach and scale available to businesses through digitalization. Fundamentally, these reforms propose a reallocation of taxable profits from the "home" jurisdiction of digital businesses to customer or market jurisdictions. This represents a radical shift in international tax rights that will expose consumer-facing businesses to taxation in many more countries, increasing tax and administration costs and potentially requiring the reorganization of current corporate structures and supply chains.

Unilateral digital tax measures

The OECD negotiations on digital tax reform have been ongoing for nearly a decade and during this period many countries have become concerned that international consensus will not be reached. Therefore, to address lost tax revenue and local political imperatives, many countries have or are in the process of introducing, their own digital tax measures such as digital services taxes (DSTs), withholding taxes (for example, on digital advertising revenues) and VAT/sales-type taxes on digital services. These take many different forms but often seek to tax the same income producing activity, giving rise to potential double taxation in some cases as well as significant additional tax payment and compliance burdens for digital businesses.

Many of these measures (either in force or prospective) are expressed to be subject to the implementation of an OECD approved, internationally agreed system for the taxation of the digital economy. If this can be agreed, many of these inconsistent and often conflicting unilateral taxes will fall away to be replaced by what is hoped to be a coherent international system that is easier for businesses to operate and designed to prevent double taxation.

Contents

Spotlight on 2021

2020 was supposed to be the year in which consensus was reached on an OECD proposal. While good progress was made (despite the pandemic) and detailed proposals have been developed, international agreement on a final proposal was not achieved and is now targeted for 2021. 2021 is also likely to be the "make or break" year – sufficient progress has already been made on proposals such that it does not seem likely that finalizing these proposals will extend beyond 2021, so the key issue is whether international consensus and agreement can be reached.

If consensus can be reached, there could be huge global change to international business taxation in 2021. If consensus is not reached, 2021 is likely to see the rapid expansion of unilateral digital tax measures that are anticipated to create significant confusion and tax cost for businesses operating globally. For regular updates throughout 2021 on this developing area, please subscribe to our weekly **Digital Tax Bytes.**

Ben Jones
Partner
benjones@eversheds-sutherland.com

Robb Chase
Partner
robbchase@eversheds-sutherland.com

TeleScope TMT 2021 outlook

Contents

The agile workplace: the new blended working environment

As we approach the anniversary of the start of the world's greatest mass work from home experiment, it is time to take stock. After countless debates in the market over the last year, the general consensus is that the office is not a thing of the past - but metamorphosing. The new world of work will be a blurred blended working environment on a global scale. "Agility" once a buzz word, touted by workplace strategists is now the mantra in the accelerated working from home trend. This new workplace will need to reconcile employees' demand for a better quality of life, freedom and flexibility with the deeply human need for interaction, motivation and a safe space which is not their living room. The answer emerging is clear - an agile combination of virtual, home working, serviced space and a reinvigorated traditional office working environment with people passing seamlessly between them all.

Consolidation and cost efficiencies

We are receiving increasing requests to review our clients' global real estate portfolios. Some occupiers want to reduce their office exposure and release cash via disposals, off-market sale and leasebacks and corporate deals. It is important to note that the headache of how to manage the agile world falls at the doors of a few people within a business. It is clear that the way in which the largest of businesses respond to this crisis will set the template for those businesses that look up to them.

Consolidation is the order of the day. Empty space or under-utilized space is a corporate sin. Business leaders are focused on the cost efficiencies which can be achieved through reducing their office footprint under rack rent leases and consolidating into prime high quality HQ space together with space that offers quick flexibility as the business expands and contracts.

Getting out of a rack rent lease is not straight forward. Absent of any negotiated surrender with the landlord; a rolling break right; or a fixed break right just when it is needed, the only way to offload excess space is via an assignment of the lease or subletting it. Working on the assumption that finding an assignee for premises may be difficult in these challenging times and it is also worth noting that, if one is found, landlord's consent is usually required and finding an assignee which meets the covenant strength tests acceptable to the landlord maybe harder still. Many occupiers will see the solution as being to underlet excess space. But this is not without its difficulties; if underletting is permitted then it most likely will only be permitted with the landlord's consent, but there can be extensive conditions on the rent level, the term, security of tenure rights, the replication of service charge, and insurance rent obligations.

Quality and efficiency of office space

How is the new working environment to be different? Occupiers' relationship with the space they occupy is shifting – the function of the office will be different. Richard Pickering, Chief Strategy Officer of Cushman and Wakefield in his new "The Future of Work"article comments that this new environment "needs to combine space for thinking, making and interacting with others."

Office space has to be the highest quality and in the right location which entices employees to attend. The post-COVID office has to offer more than just a desk which employees now have at home without the tiresome and costly commute. Collaboration spaces, break out rooms, contemplation rooms, cafes and gyms will take center stage to facilitate innovation, interaction, team-work and learning.

When reconfiguring office space with the blended office model in mind, occupiers have various options for providing desk space without the need to provide a desk per employee. Hot desking, desk sharing and desk hoteling may suit different businesses, and ultimately different teams within such enterprises, depending on culture, industry, head count, talent, team dynamics and strategy.

Technology to enable working from home has become critical to business operation – pipeline workstreams for digital and technology products and new applications have been accelerated. A year into the new COVID-world, customers are less forgiving – they expect a slick service, and will not accept the fact that it is just possible to work from home. The new HQ buildings now, more than ever before, need to deliver on these technological requirements and facilitate the new hybrid working environment to enable people to work anywhere whilst maintaining security and data confidentially. As mentioned in JLL's recent article "5 reasons why businesses will embrace hybrid workplaces" Lee Daniels, Global Product Manager Workplace & Occupancy Strategy & EMEA Experience Lead at JLL states: "offering this choice and flexibility will be the key differentiator for businesses to attract talent in the coming years".

Agility – flexibility and the role of serviced offices

With a reduced foot-print, flexibility is key – especially for TMT occupiers. When taking a HQ, having a keen eye on swing space in the building, part floors and options over such space is one solution. But this can take time. A quicker solution is serviced offices offering flexible office space. Finding a trusted serviced office provider which might be in the proposed building or immediate locality is vital, and building a partnering relationship with them and understanding their offering is key.

When acquiring small start-ups, having the ability to expand and contract the HQ to embed them in the culture of your business is essential to accelerate successful integration. Having a flex office provider in the building from whom you can swiftly take more space from will really help with onboarding. With the great home-working project led teams will need to all come together on mass potentially for limited periods to deliver the project. These requirements will disappear, however, as quickly as they arrived and as such a swing space can be a great asset in a businesses' space armory.

The variety of serviced offices available is vast including renting communal "co-working" desks on a day by day basis to outsourced bespoke serviced offices. Safety and privacy requirements are key concerns for any TMT occupier. Therefore, "flexible leasing" is of increasing interest and market demand by big corporate occupiers who are drawn to their shorter terms and capped total occupancy costs, whilst they deliver the atmosphere of co-working alongside security of space.

Serviced office providers are not just the answer to the practical somewhat functional requirement to increase or decrease space responding to dynamic business needs. They tick another box – that of beautiful design-led buildings. They have the bells and whistles, top barista offerings, gyms, contemplation rooms and front of house staff to meet and greet employees as clients – and the offering need not be off the peg. Working alongside providers to create a space that delivers for the occupier's business needs, project needs, and how their people like to work offers the best of both worlds for a bespoke flex space.

Blended working environment in 2021

2020 accelerated trends already afoot. The Agile workforce is now ready for the Agile workplace – in 2021 it now just needs to be delivered.

Tom Goldsmith
Partner
tomgoldsmith@eversheds-sutherland.com

Natasha O'Neill
Senior Associate
natashao'neill@eversheds-sutherland.com

Data privacy and cybersecurity: maintaining legal and operational resilience

2020 made clear the importance of developing and maintaining a proactive, holistic and strategic approach to data privacy and cybersecurity.

It was a busy year for data protection, with the pandemic and remote-working pushing many organizations to focus on internal resilience and increased security in IT infrastructure and processes. In several jurisdictions we saw a move towards increased regulatory oversight: Brazil's new data breach notification requirements came into force in September and on 1 December New Zealand followed suit. In Europe, December saw the implementation deadline pass for the new European Electronic Communications Code, bringing over-the-top (OTT) communications service providers into the scope of the ePrivacy Directive's 24 hour breach reporting regime, in several member states.

While ransomware may have impacted many companies in 2020, the year will be known for the massive and systemic SolarWinds hack, which demonstrates that private companies (and governments) must redouble efforts to engage in robust, timely and meaningful information sharing—even when personal data may not be involved. Recognizing this, for example, the New York State Department of Financial Services, released an alert on 18 December requiring all NY DFS regulated entities to immediately report whether they have been affected in any way by the security state-sponsored hack. Others have followed suit showing the serious concern that the SolarWinds hack is "active and ongoing," and will pose significant systemic risks to the financial system beyond what is currently known. The alerts emphasize the importance of a public-private partnership of enhanced information sharing in the face of these advanced, state-sponsored threats.

Whilst now is a good time for organizations to take stock of these recent developments, 2021 promises to be a year that brings further cyber challenges to the TMT sector, with several new laws coming into play that particularly affect the sector.

In Europe, these include:

- NIS 2 Directive - the new Commission proposal for a NIS 2 is aimed at fixing the deficiencies of the previous NIS Directive by clarifying that all medium and large sized companies in specific sectors will be captured. It also provides a greater focus on security in supply chains and cybersecurity and the harmonization of sanctions
- Digital Services Act and Digital Markets Act – the final proposals reveal new transparency obligations for deep consumer profiling, intermediary services, hosting services and online platforms
- 'DORA' - The Regulation on Digital Operational Resilience for the Financial Sector, looks at ICT risk, and how it will be managed by institutions and their ICT service providers alike. A key feature is the active monitoring of ICT service providers being deemed critical, with a centralized oversight framework proposed

Contents

In addition to cybersecurity, the issue of data sovereignty is something which companies will increasingly have to navigate in 2021. Spurred on by Schrems II and Brexit, uncertainty over the validity of international transfer mechanisms will likely lead to an increased shift towards data localization. As a reaction to Schrems II, the market is already seeing many US-based companies resorting to localization of European data in European datacenters, so as to avoid the hurdles of entering into model clauses. In terms of Brexit, currently personal data can still flow freely from the EU and EEA to the UK for a period of six months until an adequacy decision is reached. However, if an adequacy decision is not achieved, EU based businesses will need to consider (if they have not already) alternative transfer mechanisms, and/or localization of European data.

The global privacy landscape will also continue to evolve throughout the year, posing increasing compliance obligations on multinational TMT companies and presenting the potential for escalating costs of non-compliance. In June, Thailand's Personal Data Protection Act is due to come into effect and South Africa's long-awaited Protection of Personal Information Act (POPI) finally comes into force in July. Also in the privacy pipeline: the implementation of new laws for Canada, Switzerland and Peru, and the expected passage of new privacy bills for India, Indonesia and Israel, amongst others. With some jurisdictions imposing breach notification requirements and direct culpability on service providers, we are seeing a trend towards increased regulation in this sector.

The United States has also not escaped the GDPR's gravitational pull. A number of the more advanced state legislative proposals are based on the GDPR - like Washington's, and the California Privacy Rights Act, which California voters passed as a ballot initiative in November - made sweeping changes to California's landmark privacy law, the California Consumer Privacy Act (CCPA), mere months after the CCPA went into effect and after a year's worth of regulatory changes. The CPRA moves the CCPA closer to the GDPR.

From pandemics, to hacks, to major privacy judicial decisions, this year tested operational resilience to its core; and a key lesson is that many shocks, while hopefully preventable, can no longer be considered exogenous. They are part of the cybersecurity and data privacy landscape, necessitating a proactive data strategy that combines legal and operational resilience.

With the pace of change not letting up, organizations should look now to recognize the changes that will impact them most, develop a holistic strategy to address those changes where possible, but remain flexible in the knowledge that other challenges will arise further down the line.

Paula Barrett
Global Co-Head of Cybersecurity
paulabarrett@eversheds-sutherland.com

Michael Bahar
Global Co-Head of Cybersecurity
michaelbahar@eversheds-sutherland.com

Jonathan Palmer
Associate
jonathanpalmer@eversheds-sutherland.com

Rhoda Bryans
Associate
rhodabryans@eversheds-sutherland.com

Brexit – implications of the new points-based immigration system: the good... and the bad

On 1 December 2020, the UK Government introduced a new points-based immigration system to encourage flexibility and equality for skilled workers outside of the UK and Ireland and to manage migration to the UK from Europe following Brexit. With the right infrastructure in place, UK based employers can now take advantage of the increased flexibility the new Skilled Worker system offers for the recruitment of EU and non-EU nationals in the UK. However, whilst there is some relaxation under the new rules as compared to its predecessor, Tier 2 (General), there are several red flags that UK businesses should factor into their business and recruitment processes.

Resident Labor Market Test (RLMT)

The resident labor market test (RLMT) was a key part of Tier 2 (General) requiring employers to show that no settled worker in the UK was suitable for the role before applying to sponsor a migrant worker. The RLMT does not form part of the Skilled Worker route and its absence eliminates the administrative burden and time constraints from the global recruitment processes that previously added many weeks, and sometimes months, to the process. However sponsors need to be aware that the sponsor is still required to evidence the recruitment process. It is unclear as to what a now, 'RLMT-free', global recruitment campaign should look like. Similarly, sponsors need to consider how they evidence that the individual in mind is the most appropriate candidate for the role. Is there any need to evidence an attempt to recruit within the UK? Many businesses are left unsure on how to proceed creating some flaws under the new system and a degree of confusion for recruiters.

Document retention is one part of the sponsor's compliance obligation - there are many others – and these obligations should be carefully considered before embarking on using the Skilled Worker route.

HR and budget planning

Businesses will now need to secure a Sponsor License in order to recruit candidates who are not settled in the UK. This covers EU and non-EU nationals but not EU nationals who benefit from Withdrawal Agreement protection as they were resident in the UK before the end of 2020.

The use of the Skilled Worker route for first time sponsors will require a significant degree of planning in terms of the visa process itself, managing race discrimination risk, sponsor compliance and costs.

The 'cap' on applications that was an important part of Tier 2 (General) has been removed under the new system meaning businesses can sponsor unlimited numbers of individuals for a wider range of roles if they are the best people for the job.

The ease with which this recruitment can take place is added to by relaxation in the skill level and salary levels capable of sponsorship.

As with all visa applications however, there is a cost implication. For a medium-large organization to sponsor an individual for five years, the sponsorship costs are in the region of £10,000 (£7,000 for smaller organizations) making it much more expensive to recruit an international workforce than it used to be when free movement allowed visa free employment. There are costs for the employer and the employee: for the employee the Immigration Health Surcharge (IHS) has continued to increase and is now £624 per annum, furthering the financial burden.

Contents

Sponsor obligations

As mentioned above, complying with sponsor obligations is an essential part of being a sponsor and businesses will face punishments – including the loss of Sponsor License, a fine or even imprisonment for their mistakes.

There is a compliance burden making it important for sponsors to understand their duties and obligations. This raises a particular risk for those who have not previously held a Sponsor License and are new to the process. It can be tricky to ensure all boxes are ticked given that the new worker guidance is over 200 pages long and separated into five documents. Businesses new to sponsorship must invest in training and management of their sponsor license to avoid any risks of illegal working/loss of sponsorship.

It is clear that the new system comes with the good and the bad. However, thorough planning in all respects is required where businesses intend to start (or continue) sponsoring workers.

Top tips:

1. identify EU national employees (and their dependents) who are eligible for status under the EU Settlement Scheme and offer assistance with securing Pre-settled/ Settled Status before the end of June 2021
2. prepare new recruitment strategies where global mobility may be required
3. apply for a Sponsor License for recruitment of non-UK nationals
4. plan and arrange comprehensive training for HR employees and recruitment and management teams (including individuals responsible for the management of Sponsor Licenses)

Audrey Elliot
Partner
audreyelliott@eversheds-sutherland.com

Artificial Intelligence regulation: global update

New laws, industry guidance, white papers and policy-making is set to increase as regulators and governments across the world compete to 'set the standard' for Artificial Intelligence (AI) regulation.

Over the last few years, it has been rare for a month to go by without some new government or industry issuing draft regulations or laws, guidance documentation, whitepapers and/or policy around AI. We did see a slowdown in 2020 as a result of Covid-19, and some anticipated legislation has now been pushed to 2021. The pandemic may even have shifted the thinking of legislators as they suddenly woke up to the importance (at times) of sharing data across governments and countries in fighting joint threats such as global pandemics.

The European Union (EU), who no doubt influenced by the success of GDPR in shaping global privacy debates, looks set to continue down the path towards AI specific legislation. The Commission's white paper on AI – A European approach to excellence and trust in early 2020 set out the roadmap for ethical AI innovation. In October 2020, an EU-wide regime for the regulation of AI came one step closer when the European Parliament adopted proposal on the regulation of AI which will now be sent to the Commission. Legislative proposals are expected in early 2021 but innovation friendly countries are increasingly articulating their objection to heavy-handed regulation. In October 2020, 14 EU countries (including innovation hubs like Estonia, Sweden, Denmark and Ireland) published an open position paper urging the EU to take a balanced approach to future regulation and to focus on 'soft law solutions'. It remains to be seen if internal dissent can soften the EU approach to AI legislation.

In the United Kingdom (UK), the ICO published its final guidance on AI in July 2020. The guidance is intended to help organisation mitigate the risk of AI from a data protection perspective and it provides a framework for auditing AI systems based on a proportionate and risk based approach. Notwithstanding the new guidance, the UK approach appears at least a tacit acknowledgement that existing data protection laws are sufficient (at least for now) to deal with privacy concerns around AI. The UK is also looking more generally at AI law and what is right for the UK and this is an area we have been looking at with the CBI and others.

The United States of America (US), has been off to a relatively slow start in terms of AI regulation but in the second half of 2020 a number of new bipartisan bills were passed in the House of Representatives to develop a national AI strategy and adopt measures for the ethical use of AI and broader consumer protection measures. We have also been following carefully as NIST and others focus more and more on AI.

Contents

Meanwhile regulators in Asia have been looking at these issues for some time and producing guidance. For example in Hong Kong, the Monetary Authority and Privacy Commissioner for Personal Data, and in Singapore, the Personal Data Commissions Model Artificial Intelligence Governance Framework (updated in 2020). At the heart of the Singapore PDPC Model Framework are two high-level guiding principles: (i) organisations using AI in decision-making should ensure that the decision-making process is explainable, transparent and fair; and (ii) AI solutions should be human-centric.

The Singapore PDPC framework illustrates the strong thematic gaze, we are seeing from a cross spectrum of countries, sectors, and regulators on transparency, which is set to continue and intensify. In particular transparency is viewed as a critical foundation if there are to be means provided by which to counter-balance the potential detriments of automated decision-making.

Notwithstanding the state of global AI regulation, from a more practical perspective, we are starting to seeing how the increased regulatory scrutiny is starting to have an impact on consumers of AI. Compliance conscious corporate consumers are increasingly demanding assurances and design/audit documentation as part of the AI procurement process.

We are also seeing the Court's and existing data laws used to shape developments. In the Netherlands, the District Court of The Hague held that the System Risk Indication (SyRI) algorithm system, a legal instrument that the Dutch government uses to detect fraud in areas such as benefits, allowances, and taxes, violates article 8 of the European Convention on Human Rights (ECHR) (right to respect for private and family life). In the view of the Court, the principle of transparency was not observed, because there was no insight into the risk indicators and the operation of the risk model. Absent that transparency they couldn't assess and rule out that the deployment of the SyRI in "problem areas" would discriminate and stigmatize people in such areas.

There is enough traction in this area that designing an AI strategy for your business which considers the above areas in a manner that is able to be flexible enough for much of what is coming is now realistic and many companies are doing that. Customers are also expecting to see statements on how AI is being used by the vendors they buy from (both B2B and B2C) and also have a huge focus around ethics, transparency, non-bias, compliance with regulations and governance themselves and therefore are looking to place some obligations on their suppliers in these areas.

We have been fortunate enough to work with some of the leading companies focused on using AI within their businesses in the last year in a number of ways (both on supplier and customer side), including in relation to how to adopt AI legally, how to embed AI ethically, statements to the market on use of AI, how to ensure good governance and requisite transparency when building and/or when utilising AI, how to ensure privacy law compliance, intellectual property and ownership implications, security implications around AI, writing templates for use of AI, training on use of AI and more.

We have advised a number of clients (both supplier and customer side) and written a number of templates and articles which focus on AI and intellectual property aspects including ownership and use of data (including, inputs, outputs and models and how this fits in with confidentiality too.

Crucially, WIPO, the European Parliament and various other governments have been and are looking at whether there need to be changes in the law around AI and IP – some countries current laws work better for AI than others. A particular focus in Europe, for example, has been around patentability. This is an area where more change is expected. For those suppliers and customers putting in place deals now, it is really important to future-proof these areas as far as possible contractually and there are a number of useful ways to do this.

Another key area to watch around AI in 2021 will be the debate around AI and its potential to disrupt employment. There is an immense about of positive change AI can bring but there is no doubt (as with outsourcing) going to be an increased focus on what that means for employees, re-skilling and potential redundancies. Getting in front of those issues when looking at deployments of significant AI solutions is key to customers and therefore also key for suppliers to be cognisant of, especially in countries with stronger employment rights. In many ways, use of AI and robotics is akin to certain outsourcings and it will be interesting to see how employment law develops in this area – something which we are (and particularly our employment teams) are already working with clients on. Having a people-led approach will become increasingly important to a number of customers.

Charlotte Walker-Osborn
International Head of Artificial Intelligence, and Technology Sector
charlottewalker-osborn@eversheds-sutherland.com

Paula Barrett
Global Co-Head of Cybersecurity
paulabarrett@eversheds-sutherland.com

Erica Werneman Root
Senior Associate
ericawernemanroot@eversheds-sutherland.com

Technology M&A: trends and outlook in Europe

As Europe started to lock down in March last year, the prospects for the M&A market were considered to be gloomy. At the start of 2021, and despite the unprecedented disruption to the economy caused by the pandemic, things look very different in the technology M&A space.

Tech M&A activity is strong and expected to accelerate

Despite the gloomy predictions at the start of the pandemic, technology M&A activity saw a strong performance in 2020 and is expected to accelerate into 2021. According to Mergermarket, European technology M&A reached its highest annual value in 2020 and numerous analysts and surveys see good prospects for further growth in 2021. It has been reported that UK tech companies have raised $14 billion in 2020. The increased reliance on, and activity in, technology solutions arising from lockdown restrictions (from payments services and retail through to data center and cybersecurity) have clearly also had a knock on impact into the M&A space.

Remote working has led to new ways of doing deals

As the world was forced into a new work environment, the discussion around flexible working was accelerated and the way of doing M&A deals has been no exception to this. Many deals were done in 2020 without the parties ever physically meeting, and the option of "getting everyone into a room" to resolve issues has not been available. Whilst not without its challenges, by and large the new way of working seems to have been more successful than anyone would have imagined 12 months ago and, to an extent, it is likely to remain with us beyond the pandemic.

Private equity expected to play a key role in tech M&A in 2021

Private equity investors are increasingly looking at targets in the technology sector and are expected to play a more central role in the M&A market generally, and in technology M&A specifically, in 2021. Analysis from EY indicates that the tech sector was already the leading sector for private equity deals in 2020 in Germany, Europe's largest economy. Given the diversity of private equity investors, their activity will be a key factor in the market at all levels, ranging from possible multi-billion deals to investments in start-ups.

Risks and opportunities arising from politics and regulation

As ever, developments on a political and regulatory level have the potential to affect M&A activity in 2021 and beyond. The EU's unprecedented €1.8 trillion recovery plan for Europe has the so-called digital transition as a key aspect. Regulation of the digital economy and the concept of digital sovereignty are also increasingly a focus of debate in the political sphere, with the EU Commission recently proposing a new regulation aiming to curb the power of big tech companies ("gatekeepers"), with proposed fines between 6-10% of global annual turnover.

Brexit starts to have an effect on the ground

As elsewhere, the long-term effects of Brexit on the technology sector in general and technology M&A in particular will only become clear as time progresses. However, one immediate consequence is that UK acquirers of EU-based targets will need to be increasingly conscious of foreign investment regulation in EU member states, which often covers not only obvious areas such as defense-related technologies but also, for example, investment in so-called critical infrastructure such as data centers. This could potentially put UK bidders at a disadvantage in some processes, but in many instances can be navigated and, ensuring appropriate advice is taken at an early stage, will be critical.

Contents

Antony Cross
Principal Associate
antonycross@eversheds-sutherland.com

Elizabeth Blackwell
Senior Associate
elizabethblackwell@eversheds-sutherland.com

Fiona Ling
Trainee
fionaling@eversheds-sutherland.com

Contents

Social media:how is it being regulated?

Social media has a major impact on our lives. One major concern for users and legislators alike is to ensure that we create a balance where freedom of speech is protected as well as people's privacy. Social media is a double-edged sword, representing both the positive and harmful aspects of communication on the internet. There is no doubt that social media can and has been a great platform to give voice to the voiceless and expand participation in media, but it can also be used as a platform for bullying, terrorism and other nefarious activity.

Therefore, the debate rages on as to how we should go about regulating social media. There have been numerous developments on that front around the world, and we provide below a summary of some of these:

Middle East

When addressing the social media challenge in the Middle East, the impact and influence of politics will always be front of mind. The balance between government control, national security concerns and free speech is highly marked in this region.

This is especially the case as the rise in social media coincided with major sociopolitical movements. This has in turn led to stricter curbs on the use of social media under some laws in the Middle East.

Egypt

Egypt issued the following:

- Law No. 180 of 2018 regulating Press and Media; and
- the Decision of the Chairman of the Supreme Media Council No. 92 of 2020 dated 31 Dec 2020

(together the "SCMR Law").

The SCMR Law prevents media outlets, or websites from publishing or broadcasting false news, content that violates the Egyptian Constitution, professional ethics, and public order or morals; or calls for breaking the law; or incites discrimination, violence, racism, hatred, or extremism. The SCMR allows regulators to prevent a publication from being issued or distributed from abroad if there are national security concerns.

Turkey

In a recent development to control social media platforms, Turkey issued a new law that requires technology companies with more than 1m daily users in Turkey to store user data in the country and appoint a local representative who would be accountable to the authorities, or else face punitive measures.

The law became effective by end of October 2020. Due to noncompliance, for failing to appoint a representative to the country as required by the new law, Turkey has fined key social media platforms, $1.18 million each. In order to avoid heavy sanctions and interruption of business in Turkey, many major media platforms were compelled to abide by the provisions of the law.

European Union

In July 2020, the European Commission has launched two public consultations regarding the Digital Services Act and Digital Markets Act known as the "Digital Services Act Package".

What does the Digital Services Act provide?

The current liability framework for online intermediaries is governed by the E-commerce Directive the foundational legal framework for online services in the Internal Market (EU states) which was issued in 2000. According to the Directive, internet service providers and intermediaries are not liable for illegal and/or harmful content, provided they fulfil certain conditions:

- service providers hosting illegal content need to remove it or disable access to it as fast as possible once they are aware of the illegal nature it
- only services who play a neutral, merely technical and passive role towards the hosted content are covered by the liability exemption

The illegal use of the network (i.e. terrorism for example, with the Christchurch shooting being the most infamous incident) created a necessity to review the existing law and forced the EU to launch the two public consultations.

To put it simply, the Digital Service Act aims at tackling two main issues which have been associated with large social media platforms:

- the spread of hate speech and associated harms for society
- the dominance of gatekeeper platforms in certain markets. The EU is proposing to introduce a new regulation to ensure that markets characterized by large platforms acting as digital gatekeepers remain fair and competitive for innovators, businesses, and new market entrants

The fate of these consultations is definitely one to watch very closely in the coming months.

US

The US is the source of major global internet platforms that host content and make this content available to users. US law integrates substantial protection for such online intermediaries in cases where third parties seek to hold them liable for the conduct of their users.

US law provides robust protection for free speech. The major provisions of federal law in this context are: Digital Millennium Copyright Act ("DMCA"), and Communications Decency Act ("CDA") that govern liability and immunity of online intermediaries in the United States.

DMCA's Safe Harbor

The DMCA provides four separate sets of circumstances in which a "online service provider" shall not be liable for monetary relief. This shield from liability is known as the DMCA's "safe harbor", and these four circumstances are:

- acting as a conduit for transmitting material through its system or network
- temporarily storing material for transmission (caching)
- storing material at a user's direction.
- providing links or other tools for locating material online

Communications Decency Act

Section 230 is a landmark U.S. law that shields social media companies from liability for content that their users post and provides internet companies with broad protections. According to Electronic Frontier Foundation, an international non-profit digital rights group based in San Francisco, these are the"most valuable tools for protecting freedom of expression and innovation on the internet. This essentially allows social media companies to take actions voluntarily in "good faith" to moderate content.

Former president Trump has called repeatedly to repeal Section 230 and signed on May 28, 2020 an executive order attempting to restrain some of its protections. Despite Trump's numerous attempts to repeal the law, the executive order was challenged in court over its constitutionality and the law remains in place."

Nasser ali Khasawneh
International TMT Sector Leader
nasseralikhasawneh@eversheds-sutherland.com

Christine Khoury
Principal Associate
christinekhoury@eversheds-sutherland.com

Digital markets: new UK competition framework on the horizon

On 8 December 2020, the Digital Market Taskforce ("DMT") of the Competition and Markets Authority ("CMA") published its advice to government on the adoption of a new "pro-competition framework" for digital markets. This includes a specific regime to regulate the most powerful digital firms in the market, and seeks to establish a dedicated Digital Markets Unit ("DMU") to adopt, monitor and enforce these new rules.

In March 2020, the government requested the CMA to lead the DMT, working with the Office of Communications ("Ofcom") and the Information Commissioner's Office ("ICO"), and to recommend new pro-competition measures in digital markets.

The DMT's advice follows two recent reviews of the performance of the existing UK competition law framework in the context of digital markets. In March 2019, the Digital Competition Expert Panel, led by Professor Jason Furman, (the "Furman Review") set out its proposals for improvement. For details of the recommendations of the Furman Review, please see our earlier briefing (available here).

Subsequently, the CMA commenced a market study into online platforms and digital advertising. Please see our previous briefing for an overview of the CMA's resulting report, which was published in July 2020 (available here).

Recommendations

DMT concluded that current UK competition law is not sufficient to address the novel challenges presented by powerful digital firms, and made the following key recommendations:

- establishment of a dedicated DMU, which will be a "center of expertise" for digital markets, and seek to further the interests of consumers through promoting competition and innovation. DMU will have the power to monitor digital markets, and make proposals to strengthen existing competition and consumer laws in the UK
- creation of a new regulatory framework directed at the most powerful digital companies, which are designated by DMT to have "Strategic Market Status" ("SMS") i.e. firms that have substantial entrenched market power in one or more digital activities, the effects of which are likely to be significant and widespread. DMT recommends that the new SMS regime be targeted, proactive and forward-looking, focused on preventing harm rather than enforcing the rules after the fact

The regime would have three pillars:

1. a Code of Conduct, which would set out clear objectives and principles for SMS firms to follow, supplemented by guidance with examples and limited exemptions. SMS firms would be legally obliged to follow this Code of Conduct, and the DMU would have the power to both monitor conduct and impose tough penalties for non-compliance

2. power for the DMU to take pre-competitive interventions, which would seek to address the root cause of problems in digital markets and the reasons behind digital firms' substantial market power. Such remedies would be transformational in nature, and could include data-related interventions, interoperability and common standards, consumer choice interventions or separation remedies

Contents

3. new merger control rules for SMS firms obliging them to report all transactions to the CMA and making notifications mandatory for all transactions above a certain threshold, putting transactions on hold until clearance is obtained. In the event of a phase 2 review, the CMA would use a lower standard of proof of a "realistic prospect" of a substantial lessening of competition, rather than such a result being "more likely than not".

- enhanced cooperation and information-sharing with UK regulators, including Ofcom and the Financial Conduct Authority, to ensure a coherent regulatory landscape across the UK. As many powerful digital firms operate globally, DMT also proposes to establish a network of agencies that would facilitate coordination and concerted action with regulators across other countries

Next steps

The government recently gave the CMA the green light to adopt a new pro-competitive regime for digital markets in its response to the CMA's earlier report on online platforms and digital advertising. Consultations on the proposed regime for digital markets will take place in early 2021, and it is expected that the DMU will be established within the CMA from April 2021. For further information on the government's response, please see our earlier briefing (available here).

Comment

DMT's advice follows the recommendations provided in both the Furman Review and the CMA's report by seeking to place significantly greater regulatory checks on powerful digital firms that have SMS status. While it remains to be seen what the precise test for designating the activities of a particular company with SMS status will be, DMT has indicated that it would likely involve a 12 month evidence-based investigation into market power, which would be broadly consistent with the CMA's existing approach to merger assessments.

As the regime is only aimed at those powerful digital firms with strategic market power, it is expected that the activities of only a small number of firms will meet the criteria. Such firms may be subject to additional monitoring by the DMU, face penalties for non-compliance with additional legal obligations under the Code of Conduct, and will encounter a higher regulatory burden in notifying the CMA of all transactions, despite size. Companies active in digital markets should engage with the upcoming consultations and carefully assess compliance with any new rules that may come into play.

Annabel Borg
Principal Associate
annabelborg@eversheds-sutherland.com

Eleanne Hussey
Trainee
eleannehussey@eversheds-sutherland.com

TeleScope TMT 2021 outlook

Contents

Internet of Things: increasing regulations

It is often helpful to reflect on the past year before offering predictions about the direction of the one to come. In the 2020 edition of Telescope, the Internet of Things (IoT) article was very much focused on how the recent and vast increases in IoT adoption was driving legislators around the world to focus on security guidance.

As we start 2021, and with the benefit of hindsight, we can safely say that the focus on cybersecurity is here to stay. Indeed, much of the 'guidance' issued by legislators in the past year is already showing signs of soft-regulatory influence beyond its original sphere of application and a trend towards certain voluntary guidance becoming mandatory.

For 2021, we expect an increase in both the volume and complexity of IoT regulation and guidance with different approaches being adopted in different sectors together with an increasing divergence across jurisdictions as different legislators opt for country specific measures.

Some of the recent cybersecurity developments to take note of include:

- in the USA, the Internet of Things (IoT) Cybersecurity Improvement Act was passed by the House in September 2020 and unanimously approved by the Senate. The Act focuses on the need for government to procure IoT devices with greater security. Although the legislation is intended for the public sector, it is likely standards will flow down to private sector as companies are expected to incorporate higher security standards across the board
- the UK Department for Digital Culture Media and Sport ran a consultation on the options for legislation in this area in May 2019. The results were published in early 2020 and include a clear desire from the industry and other stakeholders for legislation on connected devices focused around making some of the principles in the UK code of practice mandatory (consumer focused)
- the European Commission announced the launch of an antitrust competition inquiry into the market for consumer products and services linked to IoT in 16 July 2020, something which we assisted clients with and which – based on work to date – we expect will result in changes for the IoT market to require more dominant IoT players to be even more cooperative with the ecosystem. A preliminary report on the replies for consultation is expected in the spring of 2021 with the final report to follow in the summer of 2022

Cybersecurity is of course not the only legislative area of focus for those working in IoT and with more and more sophisticated players exploring ways of utilising the underlying data generated by an interconnected ecosystem, privacy and data protection will continue to play a major role in shaping IoT product design and businesses policies. As more and more sectors move to digitalise and adopt technologies like IoT, companies with traditional B2B models are finding themselves fall under the wide scope of data protection laws and the burden of applying these even if limited personal data is involved. Retrofitting technologies to account for data protection laws is a painful exercise and early adopters would be well advised to consider data protection challenges at an early design phase with a strong focus on how the product set and solutions may expand capture and use of personal data going forwards.

Echoing the predictions in the cybersecurity space, this is an area of increasing regulatory and legal complexity, rendered more so by underlying political and economic drivers. A web of requirements continues to develop. Not least of which is emerging from the growth in appetite from Courts and Governments for data sovereignty in various guises. Witnessed most recently in relation to Brexit, the recent Schrems II decision. These changes will continue, so adaptability and resilience to swift legal change, as well as to protecting against incidents such as ransomware, is critical to cybersecurity.

Many IoT products and solutions increasingly include AI or complex machine learning within them and, in such a case, companies will have to grapple with the fast-changing gaze of the laws and guidance in this area and, in particular, the strong focus on ethical and transparent AI, we are seeing a small but growing segment of companies take charge of their data strategy. Regulatory compliance programs are increasingly being coupled with blue-sky thinking and proactive regulatory engagement designed to pre-empt and futureproof data strategies together with a re-analysis of terms and conditions (both sales and customer side / in-bound and out-bound) to ensure they are future proofed and fair – which, whilst challenging to do (and something we are more and more helping suppliers and customers with) is achievable and we consider will pay dividends in the future as creating solutions and products and doing business with customers and vendors becomes more efficient as a result.

Charlotte Walker-Osborn
International Head of Artificial Intelligence, and Technology Sector
charlottewalker-osborn@eversheds-sutherland.com

Paula Barrett
Global Co-Head of Cybersecurity
paulabarrett@eversheds-sutherland.com

Erica Werneman Root
Senior Associate
ericawernemanroot@eversheds-sutherland.com

The Year of the Ox: a "bullish" year for digitalization in Asia

2020 was a year that few could have predicted. However, as Asia tentatively looks beyond COVID-19, there is a sharp focus on digitalization as businesses and the public sector take stock of the learnings from the last year. In 2021, Asia is set to play host to some of the most important developments that will drive the digitalization narrative in the region, and beyond, for years to come.

As the impact of the pandemic unfolded around the world last year, organizations were forced to quickly adapt and repeatedly turned to technology to digitalize their business operations. Nowhere is this more evident than in Asia, a region that was first to adapt to the effects of COVID-19 and is home to some of the largest technology companies in the world. As Asia looks beyond COVID-19 in 2021, there are set to be a number of key developments that will drive the digitalization narrative in the region and across the globe for years to come.

Central Bank Digital Currencies

In China, an area of key focus is in Central Bank Digital Currencies ("CBDCs"). CBDCs are digital equivalents of fiat currency which are being developed or investigated by various central banks. They are typically based on Blockchain technology, but differ from cryptocurrency in that they would be issued by state monetary authorities with legal tender status.

Trials of China's own CBDC, known as the Digital Currency/Electronic Payments ("DCEP"), are well underway, with large-scale testing undertaken in Shenzhen, Suzhou, Chengdu and Xiong'an. In mid-October 2020, Shenzhen's week-long trial of the DCEP generated over 62,000 transactions and RMB8.8 million being spent. 2021 will be a significant year for the development of the DCEP as China looks to showcase it as part of the 2022 Beijing Winter Olympics. In Hong Kong, the Hong Kong Monetary Authority announced that it and the People's Bank of China ("PBOC") were preparing to trial the use of the DCEP for cross-border payments.

The development of CBDC is likely to continue to drive the reduction in the use of cash. In recent years, merchants in China have been increasingly reluctant to accept physical banknotes and coins, with that trend being exacerbated as a result of the pandemic. This practice has led to the PBOC issuing a notice on 15 December 2020 stating that the Renminbi remains legal tender and setting out a set of practices on cash-acceptance which merchants in various sectors are expected to comply.

Whilst China is certainly at the forefront of CBDC development, other nations in Asia have reported that they are considering the introduction of CBDCs, including Cambodia, Japan and South Korea. In particular, the Bank of Korea has announced that it will undertake a pilot program to test CBDCs throughout 2021.

Regulation of virtual asset exchanges

The Financial Services and Treasury Bureau in Hong Kong has issued a consultation paper seeking submissions on a proposed licensing regime that will apply to all virtual asset exchanges. The proposed regime extends the current "opt-in" regime of the Securities and Futures Commission ("SFC") whereby virtual asset trading platforms can seek to be regulated by offering the trading of at least one virtual asset that qualifies as a "security". If introduced, the regime will apply to all virtual asset exchanges actively marketed in Hong Kong, including those trading in cryptocurrencies.

Contents

The proposed regime will empower the SFC to impose a number of licensing requirements. Importantly, at the initial stage, licensed exchanges will only be permitted to deal with customers that qualify as "professional investors". Virtual asset exchanges will also need to satisfy a fit-and-proper test and be required to comply with the AML/CTF under Hong Kong's AML legislation. It will be a criminal offence to operate a virtual asset exchange without such license. Such offence is punishable with a fine of up to HKD5 million (roughly USD645,000) and imprisonment of seven years (with additional fines for continuing offences).

Similar developments are taking place in Singapore with the introduction of the Payment Services (Amendment) Bill which seeks to expand the regulatory scope of the Monetary Authority of Singapore to service providers of wallet services for digital payment tokens and exchanges of digital payment tokens (without possession of moneys/digital payment tokens). Exchanges with possession of moneys/digital payment tokens are already regulated under Singapore's existing regime introduced in early 2020.

New Chinese Personal Data Protection Law

On 21 October 2020, China's National People's Congress published a draft Personal Data Protection Law ("PDPL") for public consultation. Once formally promulgated, the PDPL will have significant impact on data privacy practices in China, particularly as there has not been a single comprehensive data protection legislation in the jurisdiction to date.

It is clear that the PDPL adopts some of its fundamental concepts from the European Union's GDPR. One key feature of the PDPL is that it will have extraterritorial application to the processing of personal data of Chinese data subjects: (1) for the purposes of providing products and/or services to data subjects in China; (2) for analyzing or assessing the behavior of data subjects in China; or (3) as otherwise prescribed. The draft PDPL also extends the localization requirements under the China Cybersecurity Law to require both "critical information infrastructure operators", and those "personal data processors" (more akin to "data controllers" under GDPR) processing over a certain "threshold" of personal data, to retain personal data in China unless they have passed the security assessment prescribed by Cyberspace Administration of China. The exact "threshold" is also to be prescribed by the Cyberspace Administration of China.

A serious breach of the PDPL can result in an order to suspend related business operations and a fine of up to RMB50 million or up to 5% of the preceding year's revenue. At this stage, it remains unclear how the revenue would be calculated, particularly whether it is calculated based on revenue derived in China only or global revenue. Personnel directly involved in the breach may be fined up to RMB1 million.

The Year of the Ox is set to be a milestone year for digitalization. As organizations in Asia look to implement digitalization strategies that build on last year's learnings, they will be doing so in a region that will see significant developments in the areas of CBDCs, virtual assets and data privacy. These developments are set to have wide-ranging implications for 2021 and beyond.

Philip Chow
Associate
philipchow@eversheds-sutherland.com

At your fingertips?: the use of biometric technology in the workplace

The dramatic innovations in biometric technologies have seen their use increase exponentially, and many businesses have seen advantages to rolling out this technology. Fingerprint scanners are the most widely-used type of biometric data technology used currently by employers (for example for unlocking company devices, allowing access to restricted areas or time attendance), but other systems collect and verify other biometric data types, including voice, eye scans, gait, facial recognition and even keystrokes. The definition of "biometric" varies across jurisdictions, but in general terms relate to any identifier that is derived from a physical, physiological or behavioural attributes.

While there are significant benefits to the use of biometric technology, there are legal and compliance risks that employers must consider before implementing biometric technology. Whilst providers may consider themselves relatively unregulated, employers must ensure that they comply with requirements of biometric and data protection regulations across the globe.

Key considerations

Biometric technology can seem to be a "quick-fix" modern security or fraud prevention solution, given that biometric solutions are regarded as difficult to fool (although this is not always the case!). In addition, the increased use of biometric data for personal use (e.g. on smartphones) seems to have increased the perceived acceptance of the use of biometric data by employees. However, one of the key challenges regarding the introduction of biometrics technology is the impact on employees from a privacy perspective.

In the UK and EU, where biometric data is used to uniquely identify (or confirm the identity) of an individual, it becomes a special category of personal data under the UK and EU GDPR (the data protection laws). This means that it benefits from additional protections. Most importantly, the employer should consider whether the use of biometric data is appropriate and proportionate to achieve the envisaged objective, but in addition, they must identify an appropriate "lawful basis" (set out specifically in the legislation) that can be relied on for its use.

Contents

Explicit consent from the individual is one such lawful basis, and it's the one most relied on in consumer uses of biometrics, such as when you use your fingerprint to unlock your phone. However, in the UK and EU, it is difficult to rely on consent as a lawful ground for the processing of biometric data in an employment context, as it is generally difficult to obtain valid (freely given) consent in an employment relationship because of the power imbalance between the employer and the employee – particularly if they are given no other option in order to do their job. In addition, employees must be provided with sufficiently detailed information about the use of biometrics so that they fully understand the consequences of providing their consent – and to make that consent explicit, by having it expressly confirmed in words which are demonstrated to have been accepted by the employee (such as by signing a statement).

Finding an alternative lawful basis to consent can also be challenging. In limited circumstances, for example, security requirements may enable an employer to demonstrate that the processing is necessary for reasons of substantial public interest, or facial recognition may be the most proportionate response to the employer's legal obligations in relation to employment, for example, right to work, in each case where this has been allowed for or required by the UK or EU member state's law. However, reliance on these other bases for processing would need to be assessed very carefully on a case by case basis.

In the absence of an alternative legal basis, consent may seem the only remaining option for employers to roll out such a system. If this is truly the case, and the employer has satisfied themselves that such a system is the least privacy intrusive manner of achieving their legitimate objective, in limited cases the employer may be able to rely on an explicit consent, provided that the employer can offer the employees alternatives and demonstrate that there will be no adverse consequence if the employee refuses to consent. If employees feels in any way forced to consent, consent will not be valid and consequently the processing will be unlawful.

In the US, consent, informed consent and notice also feature in the various pieces of legislation which govern the use of biometrics; but this presumption against consent in an employment context is not present, so in Illinois, for example, consent requirements can be satisfied in the employment context by obtaining a written release as a condition of employment. However, this doesn't mean that the use of biometrics is therefore an easier consideration - the legislation imposes additional obligations including restrictions against selling or otherwise profiting from an individual's biometric data, and specific retention periods, and employers must ensure that they are able to comply with all such requirements in each jurisdiction they are active. For more information on these requirements, please see our white paper on

> *Implications of US laws on collection, storage, and use of biometric information.*

Employers may also face possible resistance from employees. Employees can often feel this is more intrusive than giving biometric data to a bank, or even to their personal smartphones. Generally this is because employees are concerned that the data recorded for one purpose in the workplace is in fact being used for another. There have also been instances in some jurisdictions where the use of biometrics technology in the workplace has given rise to discrimination claims. For example, in the United States, an employee successfully argued that the use of fingerprints by his employer contravened his religious beliefs.

In the UK and EU, employees may have the opportunity to bring claims for compensation directly against employers if their rights have been infringed. Regulators can also bring enforcement action against any employer in breach, either issuing monetary penalties or requiring destruction of data collected. Enforcement action has, however, been limited, to date. In the US, the remedies available vary from state to state, but again individual claims (and class actions), as well as penalties issued by the relevant Attorney General may well arise – Illinois, in particular, now has a surprisingly rich case law in this area, with complaints under its Biometric Information Privacy Act increasing.

As well as complying with data protection law requirements, employers also need to ensure that they take all necessary steps to correctly engage with employee representative bodies and the required consultation obligations are complied with, including obtaining the necessary approvals from such bodies (in applicable jurisdictions) prior to the implementation of the biometric technology.

Recommendations and steps that employers should take

- assessment: employers should consider carefully whether a biometric solution is the most appropriate – and proportionate - solution. Are there any alternatives which would be less intrusive? In the UK and EU, a data protection impact assessment may be mandatory to balance the objectives of the company and the rights of the individuals. The fast-moving technological and legal developments should continue to be monitored during the life of the project, as well as any "scope creep" in the projects which might prejudice their use
- alternatives: can an alternative solution be used instead, or as well, as the proposed solution, in particular for those employees who either object to the use of their biometric data or who may otherwise be able to raise a claim of discrimination based on protected attributes such as disability or religious beliefs
- engagement: employers should be mindful to engage early with employee representatives to properly address and accommodate any concerns. The setting up of working parties on new biometric technologies can make the employee consultation processes much smoother and employees and their representatives gain a better understanding of how such technologies will impact them. Setting up a cross-jurisdictional team where necessary who can devote the necessary time and management commitment, to interrogate the business case underlying the proposal to implement biometric backed technology, as well as an understanding of the legal and practical issues in each jurisdiction, including in relation to consultation obligations with employee representatives, is likely to be critical to the successful implementation of biometric technologies and reduce the risk of future claims from employees or their representatives.
- think global: the rules relating to the use of biometrics vary from country to country and, in the case of the US, from state to state. Employers should be clear on the relevant biometric privacy and data protection obligations in all operational jurisdictions. Without such protections in place, employers are at risk of significant fines, loss of reputation and even class actions from their employees
- documentation: issuing written notices of the employer's intent to introduce a biometric system should be provided. Written policies should also be developed to cover the collection, storage, processing of biometric data as well as establishing strategies in the event of improper disclosure to not only ensure that employers are consistent with their privacy obligations, but that they are adequately safeguarding their workers

Gayle McFarlane
Partner
gaylemcfarlane@eversheds-sutherland.com

Kat Rosen
Senior Associate
kathrynrosen@eversheds-sutherland.com

Contents

The evolving front line: cyber and data privacy litigation in 2021

All organizations are on a digital transformation journey and the pandemic supercharged it. Home working exploded and organizations moved quickly to adapt to the new normal, deploying new employee and customer apps and services to protect and drive growth.

At the same time, hackers adapted to exploit the increased attack surface that remote working provided, as well as the distraction the pandemic induced. Litigants and regulators also showed scant mercy, especially as new cyber and privacy laws came into force, new private rights of action became available, and new regulatory bodies stood up.

The attack surface expands and evolves

The rapid deployment of home working, new apps and services to employees and customers, is to be applauded; but it came with increased vulnerability. We have seen a large increase in the number and effectiveness of cyber-attacks, most commonly involving ransomware and most dangerously involving the SolarWinds hack. The lessons learned in 2020 will be even more applicable in 2021. Essential procedures will be holistic, systematic, and risk-based assessments, continuous monitoring, training and testing, as well as the formulation of up-to-date, concise incident response plans, which take into account the realities of remote working and the latest regulatory guidance (including warnings about paying ransoms in violations of sanctions).

Where do you stop and start?

Security begins and ends with knowledge, both of your own systems and of anything that touches your networks or integrates in your systems. Accordingly, an important element to understand prior to an incident is where provider and customer stop and start, in terms of the provision, management and configuration of security-related hardware, software and services. This matters not only day to day, as to what each party should be doing and whether they are doing it, but also when the worst happens. We see a lack of clarity as to: who has responsibility for what in the estate; what software is deployed and where; and whose responsibility it is to configure it correctly. Contract clarity is the obvious one to check, but there is often a divergence between the contract and reality, especially over long-term contracts and distributed systems, making regular detailed audits necessary (for all parties). Identifying the gaps is critical too. These should all be high on the agenda in 2021.

These issues will almost certainly be high on the regulatory agenda this year – for example with incoming regulations in the EU (DORA) and the UK (Operational Resilience rules and guidelines from the PRA and FCA) which will focus on the resilience of digital and technological services in the financial services sector, and how well financial institutions are set up to withstand and manage disruption to those services. Focus on these issues will inevitably lead to much greater scrutiny of the arrangements with third party technology service providers to determine whether they are fit for purpose in light of the incoming rules.

Contents

Claims and enforcement action continues to increase

In 2020, we saw a continued increase in individual claims for compensation, whether one-off claims or group/class actions arising from larger breaches or other infringements of privacy law. In the UK, we saw the Courts and regulators take action. As for the Courts, they sought to further define the bounds of liability, first by paring back the exposure of organizations being vicariously liable for an employee's wrongful acts in relation to data and, secondly, granting permission to appeal in Lloyd v Google. Accordingly, a key question to be answered in 2021 is how broad the right to compensation truly is. In Lloyd v Google, the Court of Appeal found that in some circumstances a right to compensation can arise from the "loss of control" of a person's data (i.e. the mere fact that data was processed in breach of data protection legislation), even any evidence is absent (or indeed any allegation) that the claimant has suffered financial loss. The UK Supreme Court's decision in 2021 could reduce the volume of claims or open the floodgates further. As for the UK's ICO, it handed two significant fines to BA and Marriott, with group litigation progressing.

In the US, the rate of growth in the costs of non-compliance far outstripped the rate of growth in compliance costs, due to the creation of a private right of action for data breaches within the California Consumer Privacy Act (CCPA), the start of the California Attorney General enforcement of the CCPA, and the hugely expensive biometrics class actions under Illinois law. The lesson here is to proactively invest in compliance, particularly in ways that help future proof against continued evolution in privacy and cybersecurity requirements.

2021 will be another significant year for cyber and data privacy litigation and enforcement. Tech providers continue to be uniquely placed to help customers succeed in the new normal but are a particular target for threat actors. The cost of data security compliance is increasing, but the cost of non-compliance can be far higher: fines, business interruption and system outages, remedial costs, compensation claims (whether corporate customers, consumers or employees) and a more fundamental loss of trust, can be critical to short-term and long-term success.

James Hyde
TMT Disputes Lead
jameshyde@eversheds-sutherland.com

Michael Bahar
Global Co-Head of Cybersecurity
michaelbahar@eversheds-sutherland.com

Jake McQuitty
Partner
jakemcquitty@eversheds-sutherland.com

Matthew Chapman
Senior Associate
matthewchapman@eversheds-sutherland.com

Richard Bacon
Senior Associate
richardbacon@eversheds-sutherland.com

Zach Ward
Associate
zachward@eversheds-sutherland.com

Cloud computing: how it is being regulated in the Kingdom of Saudi Arabia

Cloud computing

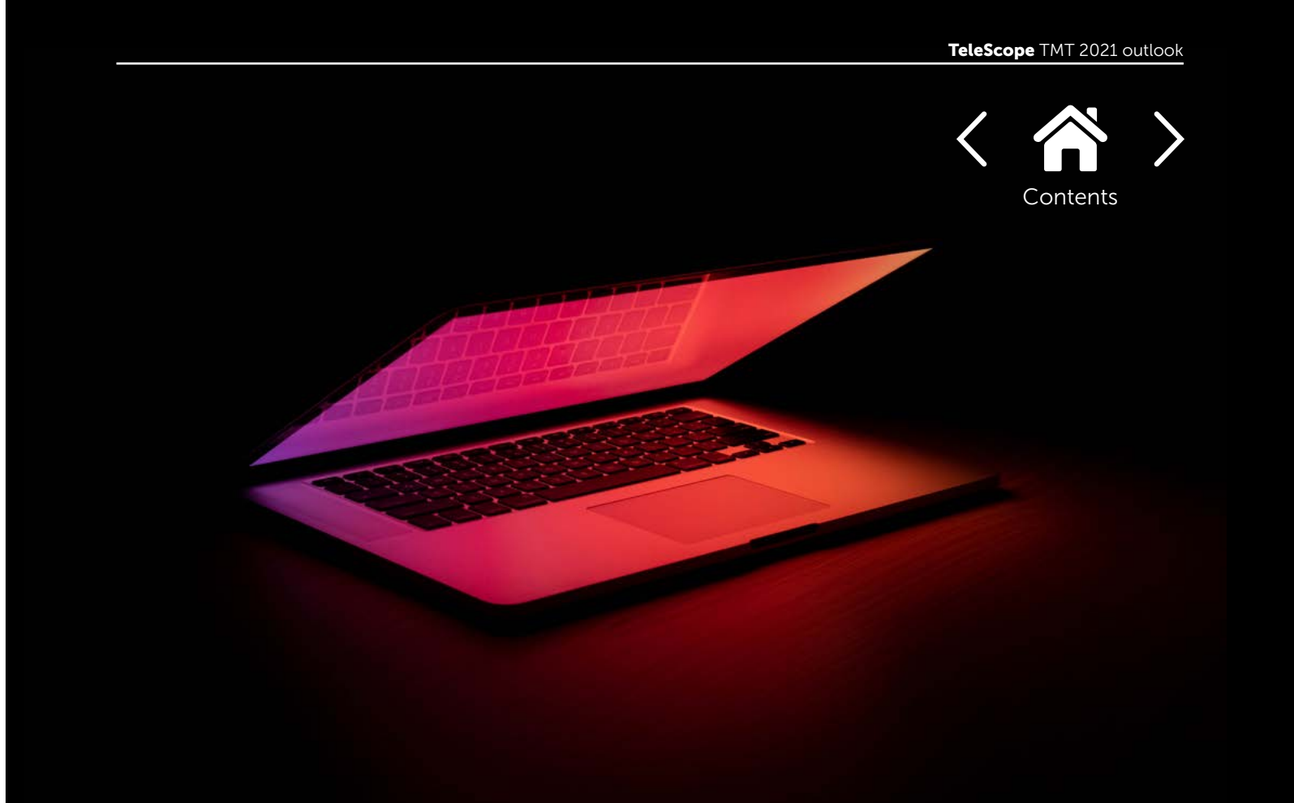
Cloud adoption has grown on a global scale in recent years due to key benefits such as cost savings, scalability, security and ease of deployment. However, this growth also brings its own set of challenges like data privacy and security, particularly in the Kingdom of Saudi Arabia (the "Kingdom" or "KSA"), where the Communication and Information Technology Commission ("CITC") and the Ministry of Communications and Information Technology (MCIT) have taken timely measures in bringing the cloud services under the regulatory ambit. CITC's Cloud Computing Regulatory Framework (CCRF) that was published in February 2018 touches upon several key cloud regulatory areas on the registration of cloud service providers. The CCRF was updated and republished in December 2020 and the revised version shows an even greater enabling environment for cloud service providers by rearranging the cloud service provider's registration levels, aligning with data and cybersecurity requirements, and creating a special track for providers classified as SMEs. For example, the CCRF clearly outlines the data classes for customer data, regulations for the protection of customer data, customer protection, content filtering, and commissioning of powers. The usage of cloud services in the public sector is directly governed by the 'Cloud First Policy' published by MCIT in October 2020. These measures have put the Kingdom ahead of a number of developing markets.

Government data

Government data represents a national asset that can enhance performance and productivity and facilitate public services delivery. This can be achieved by instituting effective data management practices, establishing the highest levels of data accountability and transparency, and leveraging data to extract insights and support strategic decision making. Nations around the world are harnessing the value of data as a vital economic resource for unlocking innovation, driving economic growth and transformation, and improving national competitiveness.

Government entities in KSA collect and process vast amounts of data that can contribute to the national economic prosperity and leadership among global data-driven economies. To drive full value realization from national data assets, data sharing is a foundational principle to establish synergies across government entities and avoid data duplication, inconsistencies, and multiple sources in absence of clarity regarding the single source of truth. This requires data classification against defined levels of confidentiality for balancing between the benefits and risks associated with data sharing among entities in the public, private, or third sector. Data classification is a pre-requisite for identifying and publishing open data, making publicly classified information available, and exchanging protected data that includes personal data. This increases the level of public scrutiny standards against the performance of public entities, enhances transparency and fosters integrity.

Contents



Personal data protection

With the technological advancement and ease of access and sharing of data, personal data protection is becoming more critical which has instigated most countries around the world to release laws and regulations for collecting, processing, and sharing of personal data to protect and to govern national data sovereignty.

The Kingdom is moving towards a new era under the National Vision 2030, enhancing government effectiveness and transparency, fostering economic diversification powered by digital and data, playing a larger role in the global economy, founded on public trust and international partnerships.

On October 20, the Saudi Data and Artificial Intelligence Authority (SDAIA) published the National Data Governance Interim Regulations to govern the collection, use, processing, and management of data in the Kingdom. The regulations cover five topics: data classification by public entities, protection of personal data, data sharing between public entities, freedom of information requests, and open data. Much of the document, including the regulation on the protection of personal data, draws significantly from international regulations such as the EU's General Data Protection Regulation (GDPR).

The publication of these regulations comes during a period of significant development for the regulatory landscape around data and digital activities in the Kingdom. SDAIA was only recently established in August 2019 and has spent much of the time since then developing the entities under its umbrella, including the National Data Management Office (NDMO), which authored these regulations. The past few months have seen increased activity from SDAIA as a policy authority, including the development of a national strategy for data and AI that was unveiled during the Kingdom's Global AI Summit on October 21 and 22, 2020.

It signals that SDAIA is now ready to take on a more active and public role in defining the Kingdom's regulation of data and AI. The decision to release these as "interim" regulations indicates that the regulation of data will continue to evolve as SDAIA and NDMO grow more established in their roles. Suppliers to customers in the Kingdom will need to be cognizant of these changes.

Anum Saleem
Principal Associate
anumsaleem@aldhabaan-es.com

Digital business transformation: the role of M&A transactions

As technology continues to transform the way businesses operate, and the products and services they offer, strategic acquisitions and investments can be key to achieving digital transformation strategies.

Companies across all sectors have prioritized the digitalization of their business as part of their transformation strategies, particularly in the aftermath of COVID-19. In terms of global deal volumes, the technology sector is booming as compared with other traditional business sectors. Whilst consolidation in the tech market remains prevalent, there has been a major shift in the last five years in the proportion of acquisitions of tech assets by the non-tech sector, with more deals now being done by non-tech companies than by tech companies. This deal volume is driven by strategic acquisitions being made by large corporates to achieve their digital transformation goals.

An enabler of transformation

Whilst companies continue to invest significant proportions of their operating capital in technology-driven transformation, this can be a challenge for incumbent organizations. It is expensive and often companies do not have the capabilities or structure to support technological innovation. Instead, many see acquisitions as the best, or at least fastest, way for a company to accelerate its digitization strategy, by acquiring the entire capability, technologies and skills of an established tech business or start-up. It is however not just full acquisitions which can achieve this, and companies may also look to pursue minority investments, joint ventures (to co-innovate) and/or corporate venture investments (to incubate and invest in growth areas).

From deal to integration

To ensure the deal realizes value, the acquisition or investment has to be taken effectively from inception stage through to post-completion integration, with importance given to thinking about life for the business beyond 'doing the deal' and beyond the challenges of technological integration.

The legal aspects can help deliver this successfully, with a key part of managing risk being the legal due diligence review of the business. Tech businesses carry complexities due to their fast growth and the types of assets involved. This requires a focused approach to diligence looking at areas such as intellectual property, people, data privacy, regulatory and cyber security.

The potential cultural challenges which arise with integrating a business into a large company are elevated further with tech and non-tech integrations. There can be a culture shock between the independence, speed and creativity to which the targets are accustomed and the traditional models of large non-tech companies, which needs to be considered and mitigated.

A key deal point will be the continued motivation of founders who are to become employees post-completion, and who may typically achieve significant returns on the deal. Earn out arrangements as part of the consideration structuring, based on the future performance of the business, are one method of achieving this.

Contents

Corporate venturing

A challenge for established companies can be confinement to a business model which lacks the agility to meet the rapid progression of digitalization. As a result, corporate venturing is a growing route to efficiently achieve transformation strategies.

Corporate venture capital (CVC) allows companies to invest in and collaborate with start-ups, rather than seeking to acquire and integrate the business into their own. The benefit to start-ups is that they can secure both the capital and a partnership. An effective governance model is key, to enable appropriate decision making whilst giving the start-up enough autonomy to operate.

CVC investments are often long-term, as compared with traditional VC, and enable access to expertise, business models and technologies. But there are also financial objectives to the investment, with participation in the financial upside of a high growth business, and ultimately monetization of the investment through exit options such as a sale of equity to third parties, initial public offering (IPO) or integration of the business.

Giles Dennison
Partner
gilesdennison@eversheds-sutherland.com

Tom Jackson
Senior Associate
tomjackson@eversheds-sutherland.com

Defamation by AI: libelous robots?

AI journalism and automated journalism are shaking up the industry, and are bringing about changes within the profession – and it is likely that software will play an increasing role in journalism and media. But what are the legal implications of a pen wielding robot?

What is the recourse against a libelous bot? One that perhaps generates a news article which contains a libelous sting that an individual is a fraudster? Even if the article isn't entirely wide of the mark what if the target of the bot's AI generated exposé - (the "target") - is threatening to sue.

The necessary elements of a claim in libel are present: publication of words to third parties containing an untrue imputation that harms the reputation of a claimant. An imputation that someone is a fraudster is likely to meet the "serious harm" test under section 1 of the 2013 Defamation Act. With those elements met, Target crosses the evidential threshold for bringing a libel claim. But who is Target going to sue? The author bot? Target wouldn't get very far – in order to be classed as an author under English law you need to be both the originator of the statement and a legal person. The year is 2021 and robots haven't yet had their legal status or human rights recognized.

If the bot isn't the author, who is? Easy, you may be thinking – Target will sue the news organization. Not so fast, it remains to be seen whether the courts (under UK law) will treat a defendant company, such as a news organization, as an "author" of AI generated material on the basis that its employees developed the underlying algorithm or tool (same problem with driverless cars). This is particularly so where there is machine learning, the end-product of which is undetermined. To do so would be some leap from traditional authorship and it would be quite a radical extension of the law as it is currently understood.

If no one is identifiably the author, who else can Target sue? Target is undeterred and knows that in libel law, you can sue anyone who is involved in the dissemination of a defamatory statement – down to the postman who delivers it, provided there is knowing involvement. That means Target can sue the news organization as the publisher (if not as the author) of the statement. What of "knowing involvement" however? If the content is generated automatically, is there knowing involvement? The answer is yes. The knowing involvement requirement here is in the act of publication. Intent is traced back to the development process and the decision to set the AI into operation. It is no defense to plead ignorance of the defamatory content. Motive is irrelevant to a claim in defamation. It does not matter that there was no intention to refer to, embarrass or defame Target.

Assuming Target can bring a claim against the Frankenstein publisher of this monstrous allegation therefore, what defenses might be available to the publisher?

Contents

What if there really are grounds to think Target is a fraudster? Section 3 of the Defamation Act 2013 provides a defense for a statement of "honest opinion" – i.e. an opinion which an honest person could hold based on true facts. That would normally get the author and publisher off the hook – provided that they can point to facts which support the holding of such an opinion – perhaps conduct which has been made public. But under subsections 5 and 6 – the defense is defeated if the defendant didn't hold the opinion or if the defendant knew or ought to have known that the author didn't hold the opinion.

If the defendant here is the publisher, it will have a job to claim that the bot it created is either honest or capable of holding any opinions, no matter how opinionated it seems to be from its content production. That suggests the publisher would not be able to rely on Section 3 of the Defamation Act 2013.

What of the public interest defense under Section 4 of the Defamation Act 2013? That provides a defense where there is a publication on a matter of public interest. If Target is a public figure, and there are grounds to say that he is a fraudster, surely it is in the public interest to publish? Here again the sub-sections throw up obstacles. Sub-section 1(b) of Section 4 requires a mental element: reasonable belief that publication is in the public interest. Again, the bot can have no beliefs and where the publisher unleashed the robot, without reviewing its output, it can have had no belief either as to the public importance of the statement (assessed at the point of publication).

So what can the Defendant stuck with the consequences of the bot's outburst do? A quick offer of amends under Section 2 of the Defamation Act 1996 looks like the only option.

What is the take-away from this? It is that those engaging with robo-journalists may find themselves liable for their defamatory statements and if an operator wishes to have in its arsenal the full array of defenses to a libel claim, careful human review before publication is advised. This is what prudent media companies do for their human authors and in this sense robo-journalists need no less supervision. In any event, there is no doubt the law is changing and will change to take account of AI and robo-law, so do watch this space.

Eileen Weinert
Senior Associate
eileenweinert@eversheds-sutherland.com

Content liability : a comparative view to the draft Digital Services Act from Ireland, France and Germany

The regulatory landscape applicable to online content is being updated in a number of ways and is set to bring much needed consistency, harmonization and pragmatism in an area that has been rather difficult to navigate especially as one of the founding EU legal instruments (the E-Commerce Directive (2000/31/EC)) became more and more obsolete. The publication of the draft Digital Services Act ("DSA") Regulation has come a long way and lays the foundations for a regime that will be easier to use across Member States and more in line with the technical reality of the Internet. The draft DSA has drawn upon some of the specific mechanisms at Member State level and this is also an opportunity to look at the current regime in Ireland, Germany and France from this perspective.

The premise to the DSA

Currently, liability for the hosting and transmission of online content in the EU is determined by the regime transposed into national laws pursuant to the Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000/31/EC) (E-Commerce Directive).

Focusing on the E-Commerce Directive which the DSA will come to supplement, and looking in particular at the status of hosting provider which the E-Commerce Directive introduced, Member States have had to grapple with the scope of this new role. The exact perimeter of the hosting provider status has been a pivotal question because in practice it can be easier and more straightforward to go after a hosting provider than after each individual content publisher.

The E-Commerce Directive has quickly shown its limits in this respect and national courts have had to step in to provide guidance on a number of practical aspects such as: who could be considered a hosting provider?; what content would be considered as manifestly illegal?; when would a hosting provider be deemed to have knowledge of such content (and thus have an obligation to take it down)?; how expeditiously should such content be taken down?; is there a requirement to ensure that content taken down does not reappear?

A number of these questions have been clarified quite clearly by national courts whilst some have not. Significant help along the way came from a number of important ruling from the CJEU (for instance in decisions CJEU, 23 March 2010, Google "Adwords", C-236/08 to C-238/08 and CJEU, 12 July 2011, L'Oréal v. eBay, C-324/09 which helped shape the definition of hosting provider and the line between the active and passive roles).

However, these joint efforts have their limits and the updating of the E-Commerce Directive is long overdue. This is because technologies and business models have evolved in the last 20 years and the EU framework is lagging behind and does not reflect the new landscape and the rise of new actors, such as social networks and other types of platforms. Also, societal changes have impacted the nature and scale of content liability, with the increasing use of platforms to disseminate illegal and harmful content. The differences that currently exist between the Member States make it harder to navigate this issue and to seek protection against illicit and harmful content.

A view from Ireland, Germany and France

Regulation of Online Content in Ireland

Currently online services are not legally liable for material that they transmit or host as long as they expeditiously remove illegal material once it is brought to their attention.

On 9 January 2020, the Irish Government approved the general scheme of the Online Safety and Media Regulation Bill (the "Bill") which will transpose the Audio-visual Media Directive 2018/1808 into Irish legislation. The General Scheme of the Bill has considered the legal liability regime for online services established by the E-Commerce Directive. It is envisaged that the proposed Online Safety Commissioner will have regard to this liability regime in creating binding online safety codes, assessing compliance of designated online services with said codes and in directing compliance through notices.

The general scheme of the Bill provides for the establishment of the Media Commission which will be equipped to deal with enforcement and sanction powers to ensure compliance, including the power to seek the imposition of administrative sanctions of up to €20,000,000 or, up to 10% of relevant turnover of the preceding financial year, whichever is higher.

The Defamation Act 2009 applies to online content published in Ireland, providing remedies with respect to defamatory statements. Online intermediaries continue to rely on the "notice and takedown" exemption under the E-Commerce directive.

Regulation of online content in germany

In Germany, the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) which aims at combating agitation and fake news in social networks, has been in force since 1 October 2017. The NetzDG aims to more effectively combat hate crime, criminal false news and other criminal content on social networking platforms. Therefore, it obliges social network providers ("Providers") to set up user-friendly mechanisms for reporting critical posts, to check reported posts for their illegality at short notice and with trained staff, and if necessary to delete or block access to such illegal content. Illegal content must be deleted or blocked within a specific timeframe (with regard to obviously illegal content it is 24 hours of receipt of the complaint, for other (not-obviously) illegal content it within seven days of receipt of the complaint. In order to make it easier for Providers to assess what illegal content is, the NetzDG provides a respective definition.

To monitor implementation, there are accompanying reporting obligations that force Providers to give account of their internal handling of complaints under the NetzDG every six months. The NetzDG provides for an internal complaints procedure and an out-of-court arbitration procedure. However, there is no general monitoring or active fact-finding obligation imposed on Providers. Providers who do not set up an effective complaints management system at all or do not do so properly are committing an administrative offence which can be punished with a fine of up to five million euros against a person responsible for the complaints procedure. Against the company itself, the fine can be up to 50 million euros. A fine can also be imposed if the Provider does not (fully) comply with its reporting obligation.

What is important to note is that under the NetzDG, Providers are not liable the moment users upload illegal content onto their platform, with liability only occurring if the Provider doesn´t remove it after the upload occurred. Anyone whose moral rights are violated within the scope of application of the NetzDG can, in principle, demand information from the Provider as to who committed the violation. The NetzDG contains provisions to ensure that such information right can be enforced.

Regulation of online content in france

In France, there are a number of legal instruments to tackle illegal online content, including the Law on the Freedom of the Press of 29 July 1881 which is still used for instance to tackle defamatory content. There is also the law implementing the E-Commerce Directive (Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy – "LCEN") which has introduced into French law the notion of "hosting provider" and the associated safe harbour liability applicable to them. More recently, the Avia Law was enacted to tackle hate speech online and to fill a gap in this respect. It has not. In its initial version, the Avia Law was quite ambitious and contained provisions that were inspired by the German NetzDG including a 24-hour take down obligation and a one-hour take down obligation for specific content such as terrorist related content and child sexual abuse content. This law was enacted on 24 June 2020 and stripped of most of its substance by the French Constitutional Court so that it is now quite limited in the changes that it introduces. The French Constitutional Court essentially considered that the draft law was a disproportionate limitation on freedom of speech. In addition, there are a number of other legal instruments relating to specific types of illegal content such as content infringing intellectual property rights.

What is next?

– DSM Directive

The Copyright and Related Rights in the Digital Single Market Directive ((EU) 2019/790) ("DSM Directive") which was published on 17 May 2019 and is due to be transposed by Member States by June 2021, will radically alter the liability regime for online content sharing platforms ("OCSSPs"). The implementation of the DSM Directive, specifically Article 17, will mean a transition from a "notice and takedown" regime, as established under the E-Commerce Directive towards a "notice and staydown" regime for infringing content, but may also necessitate the use of filtering technologies to prevent the upload of infringing content to such platforms.

– Digital Services Act

The European Commission (the "Commission") unveiled a proposal for the highly anticipated Digital Services Act on 15 December 2020, which seeks to tackle illegal content online with heightened obligations for platforms with more than 45 million users ("Big Techs"). While introduced to address shortcomings associated with the E-Commerce Directive, the DSA specifically states that it is without prejudice to this Directive.

The DSA largely reproduces the exemptions from liability for the transmission of storage of illegal content set out in Articles 12 to 15 of the E-Commerce Directive. Providers of mere conduit, caching and hosting services are exempt from liability for third-party information they transmit and store. For example, unless a hosting service has actual knowledge of illegal activity or content and is not aware of the facts/circumstances from which the illegal activity/content is apparent or on obtaining knowledge or awareness of those facts/circumstances, acts expeditiously (emphasis added) to remove or disable access to it, an Online Intermediary Service Provider ("OIP") shall not be liable. However, a court or administrative authority may still require the hosting service provider to terminate or disable access to the illegal content.

The DSA maintains the current position under the E-Commerce Directive in confirming that there is no general obligation on OIPs to monitor information they transmit or store, nor does it require OIPs to actively seek facts or circumstances indicating illegal activity. However, online platforms and other providers of hosting services must put mechanisms in place to allow any individual or entity to notify them of the presence on their service which the individual or entity considers to be illegal content. These mechanisms must be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.

The DSA obliges Big Techs to treat notices submitted by "trusted flaggers" with priority and they are required under the DSA to provide an internal complaint-handling system in respect of decisions on alleged illegal content or information incompatible with their T&Cs. Big Techs must also inform competent enforcement authorities in the event the platform becomes aware of any information giving rise to a suspicion of serious criminal offences involving a threat to life or the safety of persons. Like in the GDPR, the DSA has introduced certain elements of accountability.

In summary, the DSA seems to be a quite reasonable approach to harmonize and optimize legal and regulatory provisions already implemented in different EU Member States. This even applies for countries which already have high standards in this respect, e.g. Germany. For instance, the DSA sets out to create a central authority to monitor compliance with the DSA, whereas the German NetzDG does not offer a central authority to oversee compliance with its provisions. On the other hand, the EU may consider the country specific provisions already implemented in Member States which – like the German NetzDG – provide for more details regarding the definition of illegal content and the timeline during which illegal content needs to be deleted or blocked.

The DSA has a long path to travel before becoming effective, with commencement of the final form of the Act not likely until 2023 at the earliest. When it is in place and after that it will be interesting to see whether the DSA will act as a bit of a standard-setter in a way the GDPR has.

Contents

Vincent Denoyelle
European TMT Lead
vincentdenoyelle@eversheds-sutherland.com

Lutz Schreiber
Partner
lutzschreiber@eversheds-sutherland.com

Marie McGinley
Partner
mariemcginley@eversheds-sutherland.ie

Sara Ghoroghy
Associate
saraghoroghy@eversheds-sutherland.com

Emma Quinn
Solicitor
emmaquinn@eversheds-sutherland.ie

Contents

Deepfakes: the new age of synthetic media

Rapid advances in artificial intelligence (AI) in the last year have supercharged the development and proliferation of so-called 'deepfakes'. What began as little more than a gimmick for entertainment purposes now has the ability to completely mislead its audience to distort democratic discourse, erode public trust in what is seen online, and inflict significant damage on reputations.

What are deepfakes and how do they work?

The term 'deepfake', a hybrid of 'deep learning' and 'fake', refers to a form of synthetic media produced by sophisticated AI that creates audio and video representations of real people saying and doing made-up things.

Deepfakes rely on artificial neural networks ("ANNs"), which are computer systems that recognize trends in data and are one of the main tools used in machine learning. Typically, the creation of a deepfake involves feeding hundreds (or even thousands) of images or videos of a person into an ANN. The ANN is then trained to identify and reconstruct patterns in faces and/or voices.

Today, through freely available open source software, anyone with access to the internet can deploy this technology to create a deepfake with relative ease.

What are the other types of synthetic media?

Deepfakes sit at the upper end of the synthetic media spectrum, using sophisticated AI techniques to create hyper-realistic content. By contrast, 'cheapfakes' (or 'shallowfakes') are created by using more basic editing techniques such as speeding, slowing, cutting or re-contextualizing footage. Cheapfakes may sit at the lower end of the spectrum, but both types of synthetic media are of equal prevalence and threat to its audiences online.

As we enter 2021, we expect to see new frontiers of deceptive media develop beyond just audio and video. Synthetic text, or 'readfakes', is one of several emerging technologies to watch out for. As the name suggests, a readfake refers to AI-generated text that may be believable and engaging, but has not actually been written by a human. Whilst this new technology remains in its infancy, readfakes will no doubt become yet another contributor to the fake news infodemic that we all face online today.

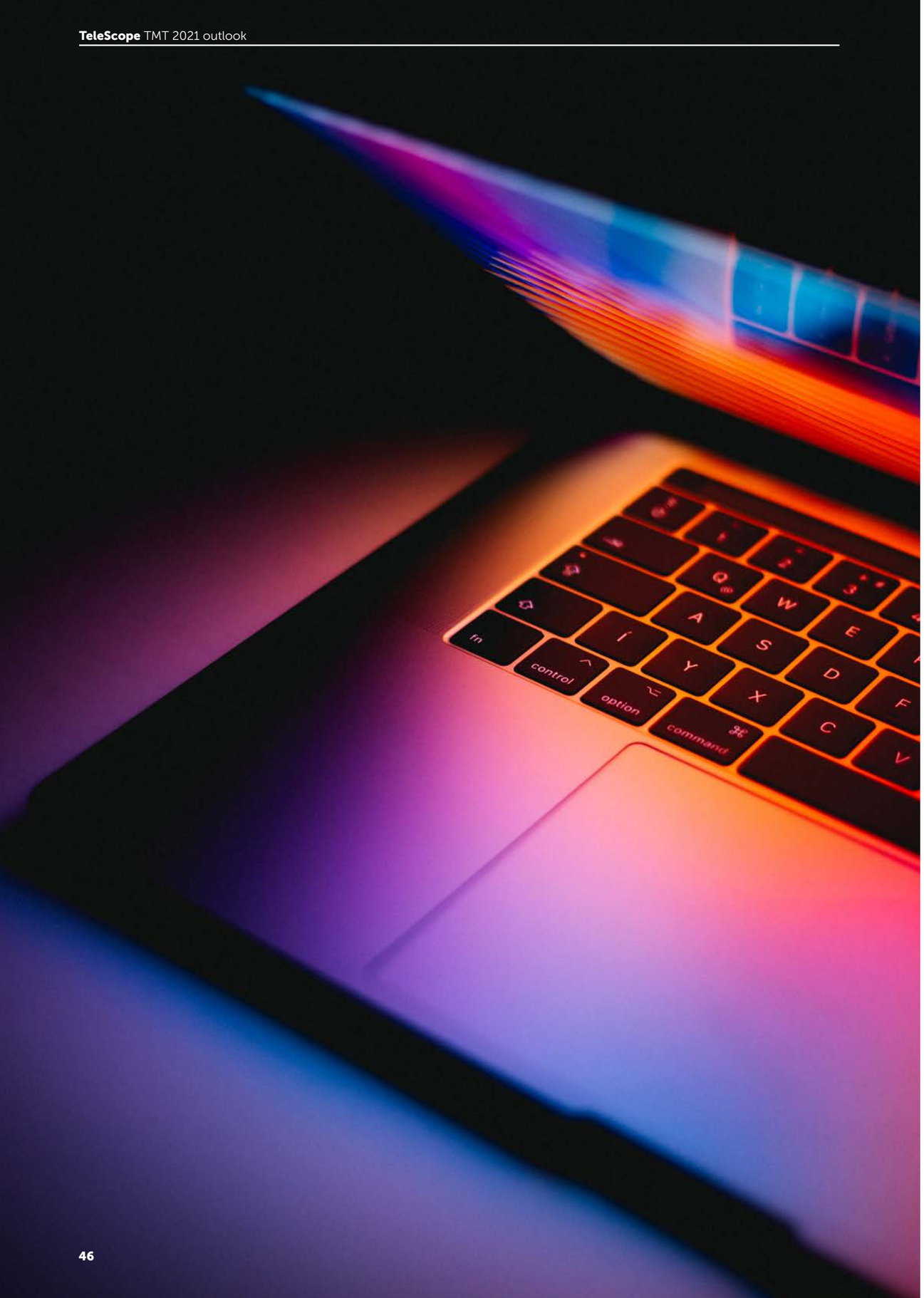
How is synthetic media regulated?

Whether we like it or not, synthetic media is here to stay. So what are the laws regulating synthetic media? The short answer is that there are very few. In the UK, there are currently no laws that explicitly refer to synthetic media, though there is an argument that existing, albeit outdated, laws could be applied. For example, if a deepfake has caused or is likely to cause serious reputational harm, defamation laws such as the Defamation Act 2013 could potentially apply. Similarly, the creation of a deepfake may have the potential to lead to copyright infringement or a breach of privacy and anti-harassment laws, though there is little to suggest that any of these laws are likely to be successfully relied upon.

Looking forward, the Government currently deliberates legislation that will attempt to tackle a wide range of harmful and illegal content online, including harms such as disinformation (fake news). The new legislation, initially set out in the DCMS's Online Harms White Paper, will impose a new statutory duty of care on Big Tech companies to regulate harmful content on their platforms and to establish an independent regulator for enforcement and oversight. It is expected that this legislation will come into force by 2022 or 2023, but whether it will be sufficient to address sophisticated and fast-developing technologies such as synthetic media remains to be seen.

Simon Lightman
Partner
simonlightman@eversheds-sutherland.com

Seb Butcher
Associate
sebastianbutcher@eversheds-sutherland.com



Contents

Cyber-fraud: asset recovery

For the majority of cyber security incidents, the primary motivation of the perpetrator is financial gain. The changes brought about by the rapid move to more distributed operations, people and systems through the pandemic have heightened the risks and incidence of cyber-fraud.

Cyber-fraudsters may seek to extort funds following a ransomware attack, or cause the misdirection of funds through some other email or systems hack. Funds are then shifted, often quickly and by sophisticated means, through various accounts around the world, in an attempt to bamboozle recovery efforts. Acting quickly is essential to the prospects of making a recovery, and an organization's cyber-security incident response protocol should include a plan for taking decisive action to recover misappropriated funds.

Civil courts around the world are grappling with the legal challenges that arise. The English civil courts have a range of measures available and demonstrated in 2020 that they will support efforts to recover misappropriated funds (including where funds are shifted overseas) in cases supported by persuasive evidence. We expect that 2021 will see more use being made of these tools:

- in most cases, all that will be known about the perpetrator is the details of the bank or cryptocurrency account to which funds were transferred. However, banks and exchanges generally will not volunteer the identity of the account holder. The English court can make orders against banks in this scenario (either as Norwich Pharmacal or Bankers Trust orders) to require disclosure of the identity of the account holder and other related information (such as details of any onward disposal). These can be effective tools when funds have been transferred to UK based institutions
- the court can make freezing injunctions and/or proprietary injunctions against 'Persons Unknown' (i.e. the unknown perpetrator, identified by available information such as a bank account). Initially, the benefit of such action would be serving the injunction on the receiving bank, as this would require it to freeze assets falling within the scope of the injunction. At this point, the game might nearly be up for an unsophisticated fraudster. Regrettably, fraudsters usually move funds between accounts quickly and by the time the injunction is served on the bank, there may be nothing left in the receiving account to freeze. Nevertheless, an injunction would typically be accompanied by ancillary disclosure orders seeking information about the onward disposal of the funds. Such information enables a fresh round of disclosure requests and/or adding new parties as respondents to the injunction. Eventually, the net closes in on the identity of the fraudster and location of the funds
- particular challenges arise when losses have been suffered in cryptoassets. The English court has made clear that most mainstream cryptoassets have the status of "property" in English law, which enables victims to claim proprietary remedies, although the extent to which such remedies can be enforced remains untested

Civil remedies should form an important part of an effective response to cyber-fraud, and in many cases will be the primary way to recover misappropriated funds. The key is getting necessary applications before the Courts within days (not weeks) as part of a coordinated response, which might also include regulatory and criminal action. We have worked with various law enforcement agencies such as the National Crime Authority's Cyber Crime Unit and the Police to assist companies in reporting cyber fraud incidents, alongside pursuing civil recovery measures.

Emma Gordon
TMT Investigations Lead
emmagordon@eversheds-sutherland.com

Tim Browning
Principal Associate
timbrowning@eversheds-sutherland.com

National Security and Investment Bill: the impact for the TMT sector

On 11 November 2020, The UK Government published its long-awaited National Security and Investment Bill (the "NSI Bill"). The NSI Bill sets out the Government's proposals for a new standalone foreign direct investment ("FDI") regime in the UK which will be comprehensive and far-reaching, and will have the effect of bringing the UK into line with other major jurisdictions around the world including the USA and Germany. It follows the government's 2017 and 2018 Green and White Papers on the national security and infrastructure investment review.

The proposed new regime is broad, and for the first time in the UK introduces a mandatory procedure for transactions in a wide range of sectors that will undoubtedly have a significant impact on deals, particularly given the low thresholds in terms of the levels of shareholdings and voting rights that will be caught by it. This follows a global trend, with jurisdictions such as France, Germany, Italy and Spain significantly expanding their domestic FDI regimes in recent months, and the recent introduction of an unprecedented EU-wide regime.

The proposed new UK regime, however, goes even further in some respects given that transactions which are not subject to the mandatory notification obligation, in any sector, are liable to be called-in by the Government for up to five years after completion if the Government considers that they give rise to national security concerns. This is a potentially intrusive power, particularly given the possible sanctions, and means that parties to transactions cannot rely on the certainty which is afforded by a solely mandatory regime.

The impact for the TMT sector

The new regime established by the NSI Bill is likely to capture a large number of deals in the TMT sector, and its application will therefore need to be considered as a matter of course as part of the majority of transactions. The NSI Bill identifies 17 key sectors which will fall within the mandatory part of the regime, including a broad category of 'communications', along with advanced robotics, artificial intelligence, computing hardware, data infrastructure and quantum technologies, which also may be relevant to TMT companies.

In addition, given that TMT companies are often regarded as being strategically important, certain transactions in the sector which do not fall within the mandatory part of the new regime are still likely to be vulnerable to scrutiny by the UK Government under the voluntary part of the new regime. It is therefore more important than ever that FDI, and the proposed new UK regime in particular, is a consideration in the early stages of all transactions in the TMT sector in the same way that merger control is, so that the impact on the deal timetable and the transaction more generally can be appropriately managed from the outset.

James Lindop
Partner
jameslindop@eversheds-sutherland.com

Laura Wright
Senior Associate
laurawright@eversheds-sutherland.com

Contents

Future fight club: key trends for 2021

For tech suppliers, 2021 will be another interesting year. They helped their customers through a seismic shift in 2020, progressing years of digital transformation and organisational change in mere months, all the while battling their own delivery challenges wrought by the pandemic. 2021 could go one of several ways for tech suppliers and it depends on what their customers do next.

After the rapid deployments and expenditure of 2020, customers of tech (whatever their sector) are now looking ahead to the post-pandemic new-normal. This reality will include permanent hybrid and work-from-anywhere arrangements for employees and the need for new, adaptable and flexible business models to serve changed economies, trade conditions, and end-customer bases with different expectations.

This is likely to drive a re-design of processes, products and services, including more automation, AI, IoT and more at the edge. Complex solutions, multi-vendor arrangements and increasing regulation will need to be navigated as a result, with heightened design and implementation risks. It is also likely to drive a re-appraisal of value for money, fitness for purpose and future need. Some customers may re-double digital transformation efforts; some may look to renegotiate or exit.

Regardless, migrations to the cloud are set to continue at pace, highlighting the continuing importance of data security and resilience, as well as the risk of system outages. For the reasons mentioned in our other article and here, the risk of corporate and personal data breaches, disputes and enforcement action will continue to be high on the agenda through 2021.

The rapid deployments of 2020 and the continuing change environment mentioned above also mean that the risk of unintentional software licence non-compliance is high. This underlines the need for licensors and licensees to regularly appraise and audit compliance.

Managing these risks and resolving disputes successfully will require speed of appraisal and decision making, as well as clear and actionable advice, in order to minimise disruption, cost and time for all involved. Organisations rightly continue to look beyond traditional approaches, to how their advisers use technology to save time and cost, and improve effectiveness. Enhanced e-discovery, AI, case collaboration and project management tools are now part of the package and those that don't offer them will fall further behind in 2021. Virtual mediations proved successful through the pandemic and will likely continue to some degree post-pandemic, as will continuing innovations in other 'online' dispute resolution.

Lastly, and as we mentioned through the pandemic and it still holds into 2021, with the unprecedented financial challenges some customers of tech face, litigation funding will continue to feature as an option. For example, and depending on the jurisdiction, with different combinations of third party funding, insurance and contingent fee arrangements, claims can be progressed at little or no cost to claimants and defendants can cap their potential liability. Expect more growth in this area through 2021.

Contents

James Hyde
TMT Disputes Lead
jameshyde@eversheds-sutherland.com

Joos Hellert
Partner
jooshellert@eversheds-sutherland.com

Vincent Denoyelle
European TMT Lead
vincentdenoyelle@eversheds-sutherland.com

Olaf Van Haperen
Partner
olafvanhaperen@eversheds-sutherland.com

Tom Whitfield
Legal Director
thomaswhitfield@eversheds-sutherland.com

eversheds-sutherland.com

DTUK003603_01/21