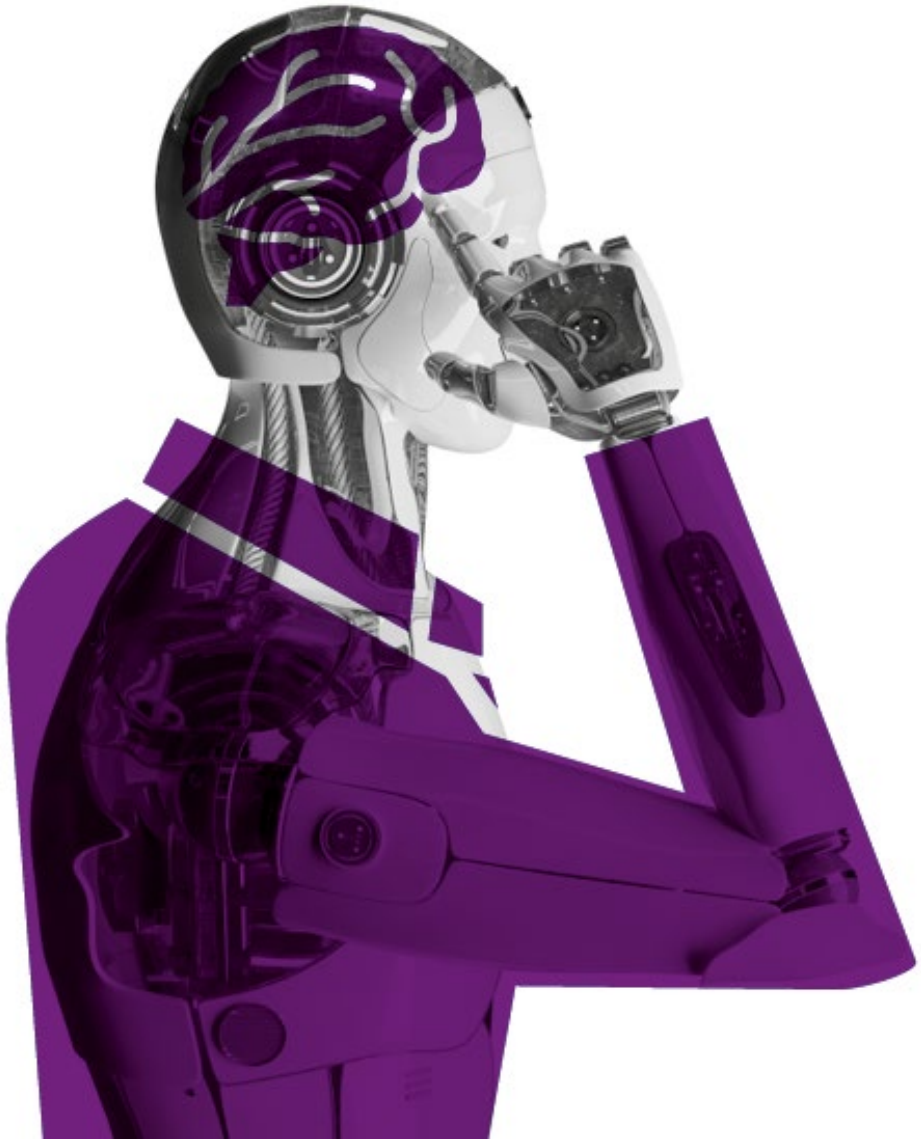
EVERSHEDS SUTHERLAND

TELESCOPE

April 2022 edition

Future thinking

Key developments impacting the TMT industry globally in 2022



In this issue

Future thinking
Key developments impacting the TMT industry globally in 2022

Nasser Ali Khasawneh
Partner & Global Head of TMT Sector

Welcome back to the latest edition of our Telescope Report, our publication which brings together knowledge, thought leadership and market commentary from our lawyers across the globe. As the world currently grapples with economic uncertainties, political unrest and the ongoing challenges of the COVID-19 pandemic, we scan the horizon in terms of technology, media, telecom and data center issues, with aim to equip the TMT sector with the current knowledge, and to give our best assessment of the direction of travel in the legal profession. The TMT sector is responding to numerous challenges in a highly impressive manner and it is clear that innovation and technology will continue to be at the heart of the response.

Businesses are forecast to spend $10 trillion over a five-year period on digital transformation. Digitalization is game-changing but it comes with numerous risks, challenges and obligations that need to be understood and navigated to stand the best chance of success. In response to this activity, Eversheds Sutherland is pleased to launch our digitalization campaign. In this publication we are pleased to share a snapshot of our newly released global thought leadership report, produced in conjunction with Longitude a Financial Times Company, **Shaping the Future of Digitalization**. The report draws upon extensive research gained from surveying 700 senior executives across the globe, supplemented by insights from leading industry experts from Microsoft, AstraZeneca, Thales, Rolls-Royce, Roche Pharma, CLSA and VMWare, to uncover perspectives on digital technologies, risk and corporate digital responsibility. More about the key findings on pages **20-21**.

In this edition, we address how TMT companies should take heed of criminal activity in relation to ransomware attacks as well as fighting 'crypto crime'. We are especially pleased to shine a spotlight on The Netherlands with commentary on the lessons learned on cryptocurrencies and the opportunities brought by digitalization. The digital revolution offers great opportunities for the Dutch economy as society aims to capitalize on the existing digital infrastructure and the ambitious cooperation between the sciences, businesses, 'start-ups', 'scale-ups', knowledge coalitions and the government. We also look at the impact on TMT companies who are affected under the release of the new European Online Safety Bill, the new Telecoms Code and the new Consumer Agenda, with local analysis from our teams in Ireland, Germany, France, the Netherlands and the UK.

Our specialist data centers lawyers comment on the latest trends of Hyperscalers and the subsequent impact on deal structures as well as how the industry is driving the transactional market. Finally, our authors give overview of how innovative technology is impacting sports, the way we handle contacts, and global employment through use of restrictive covenants as most of us continue to work somewhat, if not entirely, remotely.

I hope you will enjoy this read and we look forward to your feedback.

Changing times:
Telecoms in a new age of flux?

The business of fixed line and mobile telecommunications was once seen as a stable and predictable industry, more like a utility, with high fixed entry costs but stable long term ROI. While this image has not been true for some time, the unprecedented changes that are now taking place, and will continue to, make this original view seem rather quaint.

The pandemic underlined connectivity as critical and indispensable to work, play and learning. Through that period we have seen a combination of: (1) new and innovative solutions and players entering the market; (2) evolving technologies; (3) traditional MNO's changing business models; and (4) increased government intervention, all significantly disrupting the market. These changes, and their implications, are all explored below.

We are not alone

It is perhaps unique that an industry whose function in daily life is as critical as electricity and water should be subject to the potential for major disruption. However, 2022 is seeing the arrival of new players offering alternative business models that has the potential to disrupt current orthodoxies.

At the smaller scale we have begun to see various firms and institutions investigate the potential for Private Mobile Networks. On a larger scale, just now the world is watching Starlink provide internet services into Ukraine as it continues to ramp up its deployment (with roughly 2,000 satellites already deployed and plans for many thousands more). While the potential for low earth orbit satellite providers, such as Starlink and OneWeb, is at least in the medium term unlikely to disrupt established operators, it shows that any long term assumptions about the basic infrastructure required to provide telephone and internet services cannot be easily relied on, especially where new providers can offer enhanced services or fill perceived gaps.

Evolving technologies

With the industry already talking about what 6G may one day deliver, it is clear that in the short to medium term the potential remains with 5G, even as the roll out of this technology is slower than initially anticipated. Coverage, bandwidth and latency will remain key challenges to be addressed, especially as AR, VR and mixed realities become mainstream and almost all things become connected, sense, and share data.

Away from the headline grabbing potential of 5G and what it enables, there are further developments in network infrastructure with potential to increase significantly the diversity of the marketplace and change the way MNOs deliver services. 2022 is likely to be seen as a watershed moment where operators across the world begin to test and introduce Open RAN elements into their networks. The potential for MNOs to mix and match network components and diversify the choice of vendors deployed across new and existing infrastructure represents a real opportunity to manage costs, drive innovation and reduce dependencies.

Changing business models

With new competition, changing technologies and alternative providers, certain players are re-examining traditional business models. Where MNOs were once vertically integrated towers, masts, radio equipment and retail businesses this may be changing, with recent high profile deals and announcements by Hutchison and Deutsche Telecom regarding the sale of towers assets. With the Competition and Markets authority in the UK giving conditional approval to Hutchison's sale on 3 March 2022 this could represent a trend for the whole industry.

The implications of MNOs being fully separated from passive infrastructure is yet to be seen. However, it is clear that the market dynamics will certainly shift as a critical component of some or all of MNOs' businesses move solely into the hands of third parties. In addition, to fully capitalize on the rapidly evolving market, applications and services, we will see greater corporate activity, collaboration, partnering and alliances between MNOs and the wider ecosystem. This may also extend further into the supply chain, given the shortages and disruptions faced during the pandemic and continuing now.

Future thinking
Key developments impacting the TMT industry globally in 2022

Ongoing regulatory interventions

From around 2020 we have seen governments increasingly willing to intervene directly in the telecommunications industry. While competition concerns have been a feature of the market for some time, it is the concerns about cybersecurity and national security that have driven the most recent interventions. The most dramatic moves involved sanctions implemented by the US, in combination with measures introduced throughout Europe and other parts of the world, that forced operators to reduce and remove Huawei and ZTE technology. There are no signs of such measures being repealed.

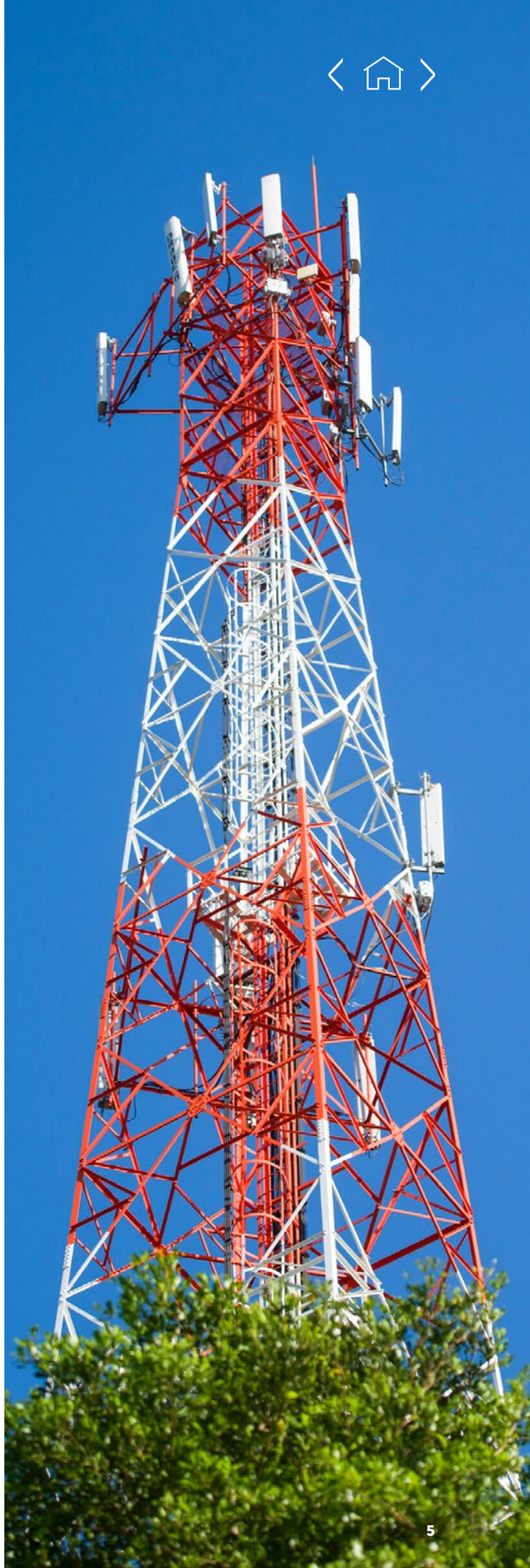
Of particular salience are the sanctions introduced in response to Russia's invasion of Ukraine. Since OFSI fined Swedish telecoms provider Telia in 2019 for indirectly facilitating telephone calls to a sanctioned entity in Syria, it has been clear in the UK and EU that providing telephone and internet services to sanctioned individuals will amount to the provision of "economic resources", in breach of sanctions. With the breadth of the new Russia sanctions on a different scale from previous regimes, the entire industry needs to be aware of its potential exposure.

What this all means

Some of the assumptions that have underpinned the industry for years have shifted and will continue to change. This brings a wealth of opportunities. However, as the ecosphere of the industry, once dominated by vertically integrated MNOs and a small handful of supplier vendors, becomes increasingly diversified and multi-faceted, we expect disputes between the larger number of participants to increase, and in more and different ways than before. All industry participants also need to appreciate the critical space in which they operate, in the context of the geopolitical landscape that is increasingly uncertain. They should be prepared for governments to continue to intervene in aspects of their businesses in ways that were previously unheard of.

James Hyde
International Telecoms Sector and TMT Disputes Lead
jameshyde@eversheds-sutherland.com

Phillip Richardson
Partner
phillipprichardson@eversheds-sutherland.com



Chain reactions:
importance of ESG in supply chains

A business' ESG (Environmental, Social and Governance) strategy and performance is increasingly viewed as the business' "store front", comprising the standards against which it is judged by stakeholders, customers, society, consumers and staff alike. The supply chain, both upstream and downstream, is inextricably linked to a business in the eyes of the public, so that a failure by a supply chain partner is seen as a failure by the business. Some very public human rights and environmental incidents in the last couple of years have demonstrated that getting ESG in the supply chain wrong can inflict huge reputational and financial damage on a business in a matter of hours.

Active support of supply chain partners (including sub-contractors and sub-suppliers, joint venture partners, distributors, agents and even your own group companies and affiliates) is essential for successful ESG performance.

ESG in the supply chain should not, however, be seen solely as a risk area. It also brings opportunities; businesses with strong ESG credentials can be more attractive than their competitors to customers, consumers and prospective employees and customers and consumers may be willing to pay more for products and services from a business that is seen to be "doing the right thing" and behaving responsibly.

Regulatory compliance

ESG in the supply chain includes compliance with regulatory regimes such as:

- anti-bribery, where non-compliance can result in strict liability and severe reputational damage
- anti-slavery, human rights and employee and worker protection legislation
- sanctions rules, in particular to ensure that there are no connections between supply chain partners and individuals, entities and/or countries subject to sanctions imposed by the UN, EU, UK or US
- sustainability reporting obligations for corporates
- requirements for large corporates to publish details on how quickly they pay suppliers
- the EU Regulation on Conflict Minerals 2017/821 that requires supply chain due diligence on minerals originating in "conflict" areas

New regimes in the pipeline

Under the UK Environment Act 2021, large businesses will be required to ensure that there is no illegal deforestation in their supply chain and to implement and report on a due diligence system in relation to use of forest risk commodities or products derived from them. Similarly, UK businesses that trade in or with the EU may also need to comply with pipeline EU legislation including the proposed EU Regulation on deforestation-free products that will require supply chain due diligence on certain products to ensure they have not been produced on illegally deforested land and the proposed EU Corporate Sustainability Due Diligence Directive that will require in-scope businesses to take measures to identify and prevent adverse human rights and environmental impacts in their operations and supply chains.

In addition to their regulatory obligations, most businesses will have their own ESG strategy which typically goes much further than what is required by law and may cover areas such as climate change risk mitigation and adaptation (often incorporating a Net Zero target), sustainability, ethical labor practices and working conditions, D&I (diversity and inclusion) and CSR (corporate social responsibility).

Selecting the right suppliers

Dealing with ESG in the supply chain is a shared journey; to achieve success it is important to ensure that your supply chain partners understand and share your ESG objectives.

The first step is to ensure that your procurement processes result in the selection of appropriate suppliers. ESG compliance should be seen as equally important to price and quality when it comes to supplier qualification and selection. Clear expectations and standards that work across all relevant jurisdictions should be set out in RFP and tender documentation and due diligence should be carried out on potential suppliers to ensure that they share your ESG values, have no historic violations and have processes in place to comply with ESG laws, your ESG policies and ESG contract provisions. Particularly when working with smaller businesses, there is likely to be investment needed to ensure buy-in, understanding and acceptance of ESG commitments and training and support may be required. Getting this right at the outset of a relationship is crucial; given the reputational issues at stake, remedies for failure to achieve ESG standards are very much a last resort.

Getting the contractual framework in place

Once a supply chain partner is selected, the next step is to ensure that the contract with that partner includes binding and enforceable obligations that cover:

- compliance with regulatory requirements (including doing what is required to enable you to fulfil your own regulatory obligations)
- compliance with your ESG policies (which you will need to ensure are drafted to apply to external contractors and not just to internal stakeholders)
- specific elements of your ESG strategy, for example reducing GHG emissions by specified targets, using data centers or manufacturing facilities which use 100% renewable energy or eliminating single-use plastics

These contract obligations need to "have teeth" – they must be clear, precise, coherent, objective and measurable so that it is possible to assess compliance. The challenge is to translate high level policy objectives into measurable contract standards, also bearing in mind that some standards may involve an element of continuous improvement towards an end target. There are many national and international standards that can be referenced in the contract and used to measure and assess compliance, for example for measuring and reporting on Scope 3 GHG emissions (which include emissions attributable to purchased goods and services).

Contractual obligations need to be backed up by the provision of information, record keeping, reporting and audit provisions so that you can assess whether the supplier is complying with their obligations and so that you have early notice of any non-compliance issues. It is essential that the contract deals adequately with the consequences of non-compliance, typically by requiring the supply-chain partner to develop and implement a remediation plan. Ultimately, you need to have a right to terminate the contract for material breach, or a failure to meet clearly defined, objective measures and standards. Being able to effectively exit a relationship with a tainted supply-chain partner will become a minimum requirement for boards, shareholders and an increasingly demanding customer-base.

Crucially, the contractor must be required to cascade all ESG obligations down through all levels of the supply chain to ensure that all entities are bound by these obligations, with a right for you to require the removal of any member of the downstream supply chain who does not comply with your ESG strategy and values. However, this is not just a contract issue. Your due diligence at the procurement stage, and ongoing audit and due diligence throughout the contract lifetime, needs to enable you to understand who is in your supply chain, where they are located and what their role is (however long and complex the supply chain is). Often ESG failures, particularly those associated with human rights abuses or negative environmental impacts, occur at the lower levels of the supply chain. Without sufficient oversight and transparency you may not even be aware that the offender is in your supply chain until the connection is made by the media.

The best way to successfully achieve these outcomes is to make ESG part of your "business as usual". If appropriate ESG objectives are set at board level and are flowed down throughout your organization and reflected and expanded upon in operational policies and processes, good ESG performance will become a normal part of the way your business operates and, over time, will be part of your reputation.

Craig Rogers
Partner
craigrogers@
eversheds-sutherland.com

Sara Ellis
Principal Associate PSL
saraellis@
eversheds-sutherland.com

The paradox of ethical hacking:

your privacy and security in hackers' hands enhance collaboration efforts

Security threats have become over the last decade one of the biggest enemies of many businesses, who as a result are pushed to strengthen internal cyber awareness and improve adequate measures to protect their assets and data. Phishing, drive-by downloads, distributed denial-of-service (DDoS) and other cyber-attacks require a real fight against intrusion into the systems of companies - enter the "white hats".

The engagement of the so-called "white hats" (ethical security hackers)is in increasing demand and considered essential to test corporate systems, find bugs and fix vulnerabilities. But what if they open their own home to the thief as a result?

Ethical hacking consists of gaining unauthorized access to computer systems, applications and data with the purpose of improving defenses before any possible breach from malicious hackers. In order to properly work and reach their goal, white hats replicate the techniques and practices of malicious hackers, with the awareness and approval from organizations – owners, CEOs, board members and management – but it raises quite a few issues in terms of legal and regulatory compliance to address in advance.

For instance, once they get the green light, white hats work at entering into the company systems and databases thus potentially getting to - and even affecting the confidentiality, integrity and availability of - the data contained therein.

How does this align with companies' data protection and privacy obligations?

The GDPR follows a risk-based approach in which the accountability of companies serves as key-principle for putting in place the security measures that best suit their organization.

While the use of tools and services aimed at assessing the robustness and adequacy of the implemented security measures certainly embodies and demonstrates the company accountability, particularly intrusive techniques and activities such as those performed by ethical hackers (e.g. penetration testing and red teaming), they may also expose personal data and confidential information to high risks and paradoxically generate conflicts with data protection laws and other applicable laws and regulations (such as, for example, labor law).

In fact, simulating malicious cyber-attacks could lead to damage and/or access to personal information and data without the due awareness of the concerned data subjects and of the employees to whom the attacked IT tools and infrastructures have been entrusted.

Therefore, any ethical hacking service which companies would make use of to test their security measures and assets would need a preliminary in-depth assessment of the data protection related profiles and matters - which may include careful and specific assessment of the entrusted ethical hackers, drafting and providing them with specific adequate instructions, performing privacy impact assessments, addressing any possible relevant impact from the employment law perspective etc. - involving all the relevant corporate functions, such as the legal and compliance departments, the DPO, if appointed, as well as, where necessary, the external data protection legal expert and advisors.

Massimo Maioletti
Head of Data Protection Italy
massimomaioletti@
eversheds-sutherland.it

Francesco Cerciello
Associate
francescocerciello@
eversheds-sutherland.it

Italy in focus:

the implementation of the Italian Audio Visual Media Service Directive and new rules on the promotion of Italian and European Works

On 8 November 2021, the Italian Government issued the D.lgs. n. 208/2021, that fully replaced the Italian Audiovisual Media Services Consolidated Act (AVMSCA) - introduced by the D.lgs. n. 177/2005 - in order to implement Directive (EU) no.2018/1808 (AVMS Directive), with which the European Union has defined the necessary amendments to the provision of audiovisual media services, in response to technological developments in the sector.

Under the new Italian Law, particular attention has been given to the promotion of European works, especially to the cinematographic ones of Italian original expression (also produced under international co-productions). As result, the discipline under Articles 52-58 provides specific obligations on providers, both in terms of programming schedules and investments.

Under article 53 it has increased the minimum share of Italian works of Italian original expression (wherever produced) that must be contained in TV catalogues; it provides that the Italian Public Service Broadcaster (RAI) must reserve at least a quarter of the share to cinematographic works.

Under article 54 more specific financial obligations are imposed on audiovisual service providers in terms of pre-purchase, purchase or production of works of Italian original expression in particular both on the ones produced by independent producers within the last five years and on the cinematographic ones:

- linear audiovisual media services providers have to reserve to European works at least 12.5% of their annual revenue, half of which has to be reserved to works of Italian original expression created by independent producers within the last five years, whereas a sub-quota of 4.2% has to be reserved to cinematographic works of Italian original expression
- Public Service Broadcaster instead have to reserve to European works at least 17% of its annual revenue, half of which has to be reserved to works of Italian original expression created by independent producers within the last five years, whereas a sub-quota of 4.2% has to be reserved to cinematographic works of Italian original expression (of which is at least 85% to co-production and pre-purchase)

These obligations must be respected by providers that have the editorial responsibility for the offers aimed at consumers in Italy, even if they operate in another Member State, unless they have no significant presence on the market (low turnover or low audience).

In view of the above, it is clear that the rules established under the new Italian AVMSCA are aimed to rebalance the level playing field giving relevance to cinematographic works of Italian original expression; it follows that the Italian audiovisual media market seems to be about to become more appealing for producers and distributors.

Giuseppe Rizzo
Partner
giusepperizzo@
eversheds-sutherland.it

Francesca Arangino
Associate
francescaarangino@
eversheds-sutherland.it

To pay or not to pay:
criminal law considerations for TMT companies facing ransomware attacks

Ransomware is big business for cybercriminals. These attacks – in which malicious software (or 'malware') is used to block access to victims' computer systems or data to extort ransom payments for its decryption or restoration – cost victims approximately USD 20 billion globally during 2021[1]. The UK and US recorded increases of 227% (totaling 33.5 million incidents) and 98% (totaling 421.5 million incidents) respectively from 2020 to 2021[2]. Continuing geopolitical volatility is likely to mean that ransomware attacks will remain a clear and present threat.

Victims of ransomware attacks face an unenviable choice. Those without appropriate data backups in place risk the permanent loss of sensitive information but have no guarantee of decryption after paying the ransom demanded. Likewise there is no assurance that threat actors will not sell or otherwise disclose the stolen data; in fact, 'double extortion' demands are increasingly common. Notwithstanding these risks, in 2021 more than 80% of UK based victims of ransomware made at least one ransom payment[3].

In the US and UK, paying a ransom is not illegal in itself. However, deciding how to respond to a ransomware demand needs consideration not only of commercial considerations (which on occasions may be existential for the business concerned) but also of whether making a payment may in itself involve breaches of criminal law. No two incidents are the same, and businesses should always receive specific advice on these points based on the facts. There are three key areas of concern.

01 Sanctions

It is an offense for any UK person (including UK based companies) to make funds available to persons listed on the designated list of sanctioned individuals and entities published by the Office of Financial Sanctions

Implementation. Similar prohibitions apply to EU persons regarding the European Sanctions List for Cybercriminals.

A complicating factor in cases involving ransomware attacks is that victims considering paying ransoms will not know who they are dealing with. Threat actors go to great lengths to hide their identity and typically demand payment in cryptocurrencies.

In the UK, no offense is committed where the paying party lacks knowledge or reasonable cause to suspect that funds would be advanced to a designated person. Conducting due diligence (to the extent possible) before making payments and updating checks based on information emerging during negotiations helps to mitigate risk in this area.

The US Office of Foreign Assets Control ("OFAC") has issued multiple ransomware advisories warning companies that ransom payments may violate US sanctions regulations. OFAC has signaled that it will view companies' efforts to implement blocking controls and measures to prevent cyberattacks in the first place as a significant mitigating factor in any OFAC enforcement response to a ransomware payment that violates US sanctions.

1 Forbes, 'Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats' (21 January 2022).
2 Sonicwall, 'Cyber Threat Report 2022' (17 February 2022).
3 Proofpoint, '2022 State of the Phish Threat Report' (22 February 2022).

Future thinking
Key developments impacting the TMT industry globally in 2022

02 Money laundering

UK based victims also need to consider the broadly drafted money laundering offenses under the Proceeds of Crime Act 2002[4]. Legitimate funds will become tainted by criminality (and therefore "criminal property") upon reaching the hands of cybercriminals. Enforcement action from prosecutors in the UK against parties making ransom payments is relatively unlikely. However, many victims of attacks (and their directors) will be cautious about the prospect of even theoretical criminal liability (for example through secondary participation in money laundering offenses committed by threat actors). Where sufficient detail is known about the nature of proposed payments, it may be appropriate to address such concerns by exploring the possibility of obtaining a defense against money laundering by filing a suspicious activity report ("SAR") with the UK's National Crime Agency ("NCA").

03 Terrorist financing

As above, paucity of available detail about the identities and motivations of threat actors may mean that terrorism financing offenses are not engaged[5]. However, there is a realistic prospect that some threat actors will have non-financial or mixed motives. Making payments to such actors knowing or having reasonable cause to suspect that the payment will or may be used for terrorist purposes is a criminal offense in the UK. Before making payments, victims should consider if it may be necessary to file a SAR with the NCA (which is in a slightly different form to that used for anti-money laundering concerns). Reporting duties will also continue after ransom payments are made[6].

Practical points for TMT companies

Whilst TMT firms have historically been amongst the most well prepared and resilient to cyberattacks, they must remain vigilant going forwards, after all, the TMT sector was the most heavily targeted sector by cybercriminals relative to its size during 2021[7]. Evidently, this threat is not going to go away and law enforcement should be engaged whether or not a payment is made or is being contemplated[8].

4 The most relevant offense in most cases involving ransomware payments will be the offense of being concerned in an arrangement facilitating the retention, acquisition or use of criminal property by a other person – Proceeds of Crime Act 2022, section 328(1).
5 See, for example, Terrorism Act 2000, section 15(3)(b) and Terrorism Act 2000, section 1(1).
6 Terrorism Act 2000, section 19(2).
7 Hiscox, 'Cyber Readiness Report 2021: Don't let cyber be a game of chance' (15 April 2021).
8 As confirmed in recent guidance issued by the UK's Information Commissioner's Office, '**Ransomware and data protection compliance**'

Emma Gordon
Partner
emmagordon@
eversheds-sutherland.com

Sarah Paul
US Head of Corporate Crime and Investigations
sarahpaul@
eversheds-sutherland.com

Michael Bahar
Global Co-Lead Cybersecurity and Data Privacy
michaelbahar@
eversheds-sutherland.com

Andrea Gordon
Counsel
andreagordon@
eversheds-sutherland.us

Chris Stott
Principal Associate
chrisstott@
eversheds-sutherland.com

Rory Brown
Associate
rorybrown@
eversheds-sutherland.com

Safety first:

an update on online safety in the UK and Ireland

The era of self-regulation for online platforms with respect to online safety is coming closer to an end as both the UK and Ireland look to implement new legislation which will regulate and hold platforms liable for harmful content and potentially impose criminal offenses.

Future thinking
Key developments impacting the TMT industry globally in 2022

UK

The UK Government has agreed to a number of changes to the **Online Safety Bill** proposed by a Joint Committee late last year, including a series of new criminal offenses. The Bill will now be considered by Parliament.

What is the Online Safety Bill?
The Bill seeks to regulate online content by placing responsibilities on the providers of online services in relation to illegal or otherwise harmful material. It sets out new duties on companies – specifically on providers of 'user-to-user services' and 'search services' – to keep their users safe online. If passed by Parliament, it will apply to companies whose online platforms allow users to generate and share their own content (such as social media sites, video communication platforms and search engines) whose services are capable of being used in the UK or of harming individuals located in the UK. The Bill designates Ofcom, the UK's telecommunications regulator, to oversee and enforce the new regime.

Duties on tech companies to tackle illegal content
The Bill would place a duty of care on tech companies to limit the spread of illegal content on their platforms. It designates a number of "priority offenses" such as hate crime, harassment and stalking which companies will have a proactive duty to seek out and minimize if the Bill is passed. In-scope companies would therefore need to design and operate their services to be safe by design and prevent users from encountering this content. The approach is similar to that required under the General Data Protection Regulation to ensure privacy by design and default is built into systems and processes, such as by avoiding free text options, to prevent the input by users of unnecessary/unwanted data.

This proactive duty can be contrasted with those proposed in respect of other forms of illegal content under the Bill, which companies would only be required to mitigate and/or remove upon them being reported. In-scope companies would also owe a host of other obligations under the Bill, including duties to carry out illegal content risk assessments (sections 8 and 23) and specific duties to protect children's online safety (sections 11 and 26).

Ofcom would monitor compliance with this regulatory regime through new enforcement powers, including powers to issue Provisional Notices of Contravention to companies which it has reasonable grounds to believe are non-compliant and to issue Confirmation Notices to companies which fail to take the remediation steps it prescribes. Companies which still refuse to comply would face financial penalties. Ofcom could also appoint 'skilled persons' to produce reports into companies' suspected breaches (section 88), mirroring equivalent powers granted to the Financial Conduct Authority under the Financial Services and Markets Act 2000.

Potential communications criminal offenses for users
The latest additions to the Bill include several 'communications offenses', including offenses for (i) sending communications which pose a real and substantial risk of causing harm to a "likely audience" (meaning a reasonably foreseeable recipient), (ii) sending knowingly false communications which are intended to cause harm to a likely audience and (iii) sending communications which convey a threat of death or serious harm (sections 150-152).

These offenses would apply to users of online platforms and aim to capture a wide range of harms which arise across different types of private and public online communications including abusive emails, social media posts and messages sent on instant messaging services. Where one of these offenses is committed by a body corporate, the responsible corporate officers of that company would be held criminally liable as well as the company itself, where the officer has consented, connived or been neglectful (section 155).

Potential criminal offenses for senior managers
The Bill additionally suggests new powers for Ofcom to issue 'information notices' demanding information and data from companies, including the role of their algorithms in selecting and displaying content (section 85). In issuing these notices, Ofcom could require companies to name the relevant senior manager with responsibility for its compliance. Where companies fail to comply with information notices (for example by providing false information), these senior managers could face individual criminal liability and, potentially, imprisonment for up to two years (section 93).

The previous draft of the Bill proposed commencement of these information offenses following a post legislative review at least two years after the Bill obtains Royal Assent. The Government now intends to accelerate this timeline to only two months.

Other notable information powers for the regulator envisaged by the Bill include powers to request interviews with company employees (section 90) and to enter and inspect tech companies' premises (section 91).

What does this mean for online platform providers?
We are now one step closer to a major change to the regulatory landscape in respect of content published online, although further changes to this hotly debated Bill seem inevitable. Its passage through Parliament will be of keen interest to online users and platform providers alike.

Emma Gordon
Partner
emmagordon@
eversheds-sutherland.com

Liz Fitzsimons
Partner
christopherstott@
eversheds-sutherland.com

Chris Stott
Principal Associate
chrisstott@
eversheds-sutherland.com

Rory Brown
Associate
rorybrown@
eversheds-sutherland.com

Ireland

In our TMT 2021 Outlook edition, we carried out a cross-jurisdiction comparative analysis of the regulation of online content in the context of the proposed EU Digital Services Act (the "DSA") which contains certain provisions aimed at regulating harmful and illegal content. At the time of publication of the DSA, Ireland had also taken the initiative to proactively propose legislation to regulate harmful online content. In this respect, our previous article considered the regulation of harmful online content in Ireland vis-à-vis the General Scheme of the Online Safety and Media Regulation Bill 2020 ("General Scheme"). Just over a year later, the Irish government has now published the Online Safety and Media Regulation Bill 2022 (the "Bill") which incorporates recommendations and updates following public consultation on the General Scheme.

In this article we focus on the key changes to online safety that have been introduced in the Bill and we give a brief update on the current status of the DSA.

Online Safety and Media Regulation Bill 2022

Meaning of harmful content
Under the Bill, the term "harmful online content" has been further refined. Harmful online content now includes both illegal and offense-specific online content as well as a wider category of harmful content that is not necessarily illegal content. For example, "harmful online content" includes online content which is contrary to certain pieces of existing legislation (e.g. child sexual abuse material) as well as online content which bullies or humiliates another person, which promotes or encourages a feeding or eating disorder, self-harm or suicide. With respect to harmful content that is not offense-specific, certain additional considerations and requirements must be met. The Media Commission may propose additional categories of online content to be considered "harmful".

Online Safety Codes
As per the General Scheme, the Bill provides that the Media Commission may make binding online safety codes which ensure service providers take appropriate measures to minimize the availability of harmful online content and risks arising from availability of and exposure to such content. The Bill provides for new additional enforcement powers of the Media Commission to ensure compliance with online safety codes (e.g. the Media Commission may issue a content limitation notice which requires an online service provider to remove or disable harmful online content).

Interaction with the eCommerce Regulations 2003
The Bill provides clarity that the online safety codes, guidance, materials or advisory notices published by the Media Commission are not intended to override the "notice and take down" obligations under the eCommerce Regulations 2003 (the "Regulations"). In particular, the Media Commission is required to develop an e-Commerce compliance strategy to ensure that the online safety codes do not impose a general obligation on providers, when providing services covered by regulations 16 to 18 of the Regulations, to monitor information which they transmit or store or to actively seek facts or circumstances which indicate illegal activity.

What's next?
The Bill is currently going through the Irish legislative procedure and is expected to be enacted before the summer recess this year. The Bill will reform the regulatory landscape that governs harmful content to create a more inclusive and safe online space for its users. As such, online providers should takes steps now to prepare for the changes that will be brought about once the Bill is enacted into legislation.

Current status of the DSA

The DSA is following the EU's ordinary legislative procedure which means that the European Parliament and European Council are each given the opportunity to propose amendments, with the aim of the Commission, Parliament and Council coming to a joint position. The European Council adopted its position in November 2021, and the European Parliament has introduced its amendments.

Amendments adopted by the European Parliament
On 20 January 2022, the European Parliament adopted its amendments to the proposal for the DSA. The amendments adopted include changes to removal of illegal content. In this respect, Members of the European Parliament suggested linking the concept of 'illegal content' to the general idea that 'what is illegal offline should also be illegal online'. The European Parliament also proposed measures to address the procedures for removing illegal products, services and content online. Under the adopted amendments, online platforms would be empowered, subject to certain conditions, to suspend the provision of their services to users under certain circumstances including, for example, where a user repeatedly provides illegal online content in their use of the service.

What's next?
Now, negotiations between the European Commission, European Parliament and European Council can commence in order to adopt a joint position ("trilogues"). The trilogues are due to run through April, with the French Presidency of the Commission hoping to reach a final agreement by the end of June, before the end of its EU Presidency.

Future thinking
Key developments impacting the TMT industry globally in 2022

Marie McGinley
Head of Intellectual Property, Technology and Data Protection Ireland
mariemcginley@eversheds-sutherland.ie

Leona Chow
Solicitor
leonachow@eversheds-sutherland.ie

Sophie Delaney
Solicitor
sophiedelaney@eversheds-sutherland.ie

Geileis Garrett
Solicitor
geileisgarrett@eversheds-sutherland.ie

Obtaining the unobtainable:
cryptocurrencies and attachments

It is still a widespread believe that cryptocurrencies are safe from (prejudgment) attachments, due to a lack of formal legislation and case law on this topic. However, it is a fact that cryptocurrencies are assets that represent a value. Any asset that has value, can in principal be attached.

In the Netherlands we were successfully able to obtain an attachment by means of progressive argumentation based on current legislation and case law. It is important to note that this attachment was placed on a software wallet at Coinbase, rather than a hardware wallet. We have outlined below some the key lessons learned.

01 The exchange platform ≠ the bank

When requesting the court for an attachment on a crypto wallet, the inclination might be to use the legal basis for attachments on a regular bank account. However, the comparison between banks and the exchange platforms cannot be made that easily. Banks have to comply with all sorts of financial regulation and therefore control the bank accounts of their customers to a level that the exchange platforms never will and never want to do due to the nature of the blockchain. Therefore, the attachment should be placed directly on the owner of the crypto wallet and not the exchange platform as a third party, like you would with a regular attachment on a bank account.

02 Cryptocurrency ≠ legally recognized means of payment

Most jurisdictions do not recognize cryptocurrencies as a means of payment. From a formal legal point of view, the cryptocurrencies do not have any value until they are converted into legally recognized currency's. In other words, cryptocurrencies are tradable financial assets. Therefore, it can be – and it was successfully – argued that cryptocurrencies are securities. Securities are assets susceptible to (prejudgment) attachments. The benefit of this qualification is that the attachment of securities has been a long standing practice and has a firm basis in existing legislation.

The fact that cryptocurrencies are not legally recognized also poses a practical problem. What to do with changes in market value? The Dutch Financial Supervision Office states that if cryptocurrencies are attached, you have attached the right to the X amount of cryptocurrencies, regardless of its market value. Compare it to placing an attachment on a gold bar. You have the right to the proceeds of the execution sale of the gold bar itself, but not the right to the market value at the moment of prejudgment attachment. If the market value has gone up by the time of execution, you are lucky. If it has dropped, that is unfortunate.

Future thinking
Key developments impacting the TMT industry globally in 2022

03 Gaining access to the account through a duty to assist

In Dutch international property case law it has been decided that if an attachment is placed on information that is uploaded to the cloud – and therefore accessible from anywhere – penalty fines may be incurred immediately if access to the bailiff to the cloud is not provided. Without this duty to assist the bailiff and in the court's own words: "the attachment order is practically useless". It can be – and it was successfully – argued that the same holds for attachment on cryptocurrencies. Therefore, requesting the court to order for substantial penalty fines in case the respondent does not assist the bailiff, is essential when trying to obtain cryptocurrencies through attachment.

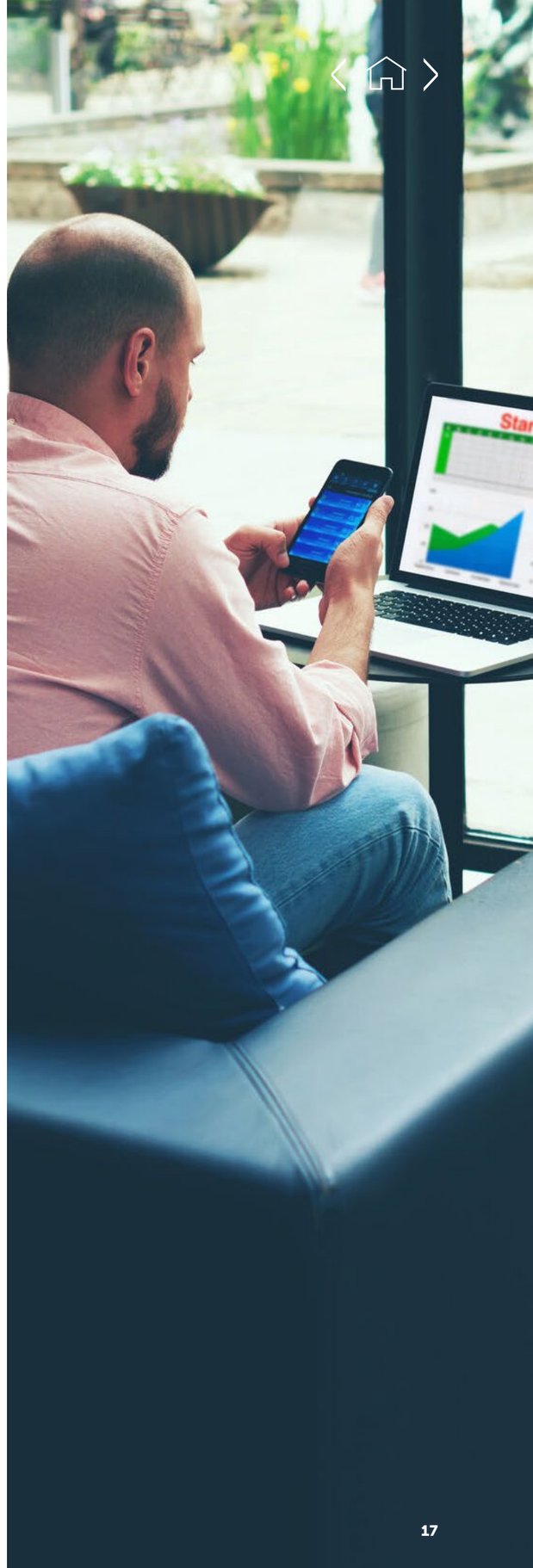
04 Be mindful of the practicalities

The bailiff executing the attachment order should be well prepared or assisted by an IT-expert when placing the attachment. The bailiff has to open its own crypto wallet in order to take into custody the cryptocurrencies that are successfully attached. It is essential that the bailiff knows how the transfer of cryptocurrencies works or is assisted by an IT-expert to help him do so on the basis of the duty to comply by the respondent as mentioned above. Preparation is key.

More and more cryptocurrencies are accessible to the general public and becoming part of our economy. As a result, there is an increased interest in the possibility to obtain cryptocurrencies as valuable assets through attachments. In the Netherlands we have been successful in obtaining such a leave from the court. Companies who own cryptocurrencies and/or make use of the exchange platforms as part of their business should be aware of this.

Olaf van Haperen
European TMT Lead
olafvanhaperen@
eversheds-sutherland.com

Marije van de Langemheen
Associate
marijevandelangemheen@
eversheds-sutherland.com



The new Italian Electronic Communications Code:
what are the implications?

On 24 December 2021, Legislative Decree No. 207 of 8 November 2021 (New Code) came into effect amending the Italian Electronic Communications Code (Legislative Decree no. 259/2003). With this new legislation, the Italian Government has transposed the Directive (EU) No. 2018/1972 (Directive) setting forth the new European Electronic Communications Code.

The new piece of legislation affects the entire telecommunications' regulatory framework and introduces profound changes to the electronic communications sector, including:

- a new and broader definition of "electronic communications services" that includes interpersonal communications services, thus including within the scope of the New Code new players, such as Over the Top operators. Under the new definition, the regulatory regime will also apply to machine-to-machine communications services (Art. 2)
- in line with the Directive, the promotion of the connectivity and access to very high capacity networks has been included among the general objectives of the New Code, entailing the access to fixed, mobile and wireless networks and to their usage by all citizens and businesses (Art. 4)
- a revised general authorization regime that, among other things, takes into account the new definition of electronic communications services. In particular, the Decree updates the information to be notified, as well as the administrative fees to be paid. General authorizations are not required for interpersonal communications services not connected to numbering resources (Art. 11)
- clarification of the roles of the competent regulatory authorities, i.e. the Italian Ministry of Economic Development (MISE), the Italian Communications Authority (AGCom) and the Italian Cybersecurity Agency
- in particular, MISE and AGCom have been empowered to ask for a wider range of information from services providers to allow geographical mapping of the infrastructures related to the electronic communications networks and to carry out periodic analysis on the current and foreseeable reach of the broadband networks in Italy (Art. 22)
- the penalties applicable to certain infringements have been increased, such as the provision of sanctions up to EUR 5 million for operators that do not comply with the authorities' orders (Art. 30). Furthermore, new administrative fines have been introduced (e.g., an administrative fine between EUR 1,000 to EUR 10,000 has been introduced for anyone engaging in activities which cause damages to communication services) (Art. 31)
- a simplified authorization procedure for installing radio facilities (Art. 47-48)
- a revised system concerning operators with significant market power, including the possibility for such operators to propose commitments to AGCom as conditions for access and co investment (Art. 93)
- enhanced rights for end users of electronic communications services, including enhanced transparency on the automatic extension of contracts and unilateral amendment of the service, formal requirements for providing information to end users, a stronger right of withdrawal in case of unilateral amendments to the contract, and a maximum duration of contracts for the provision of electronic communications services

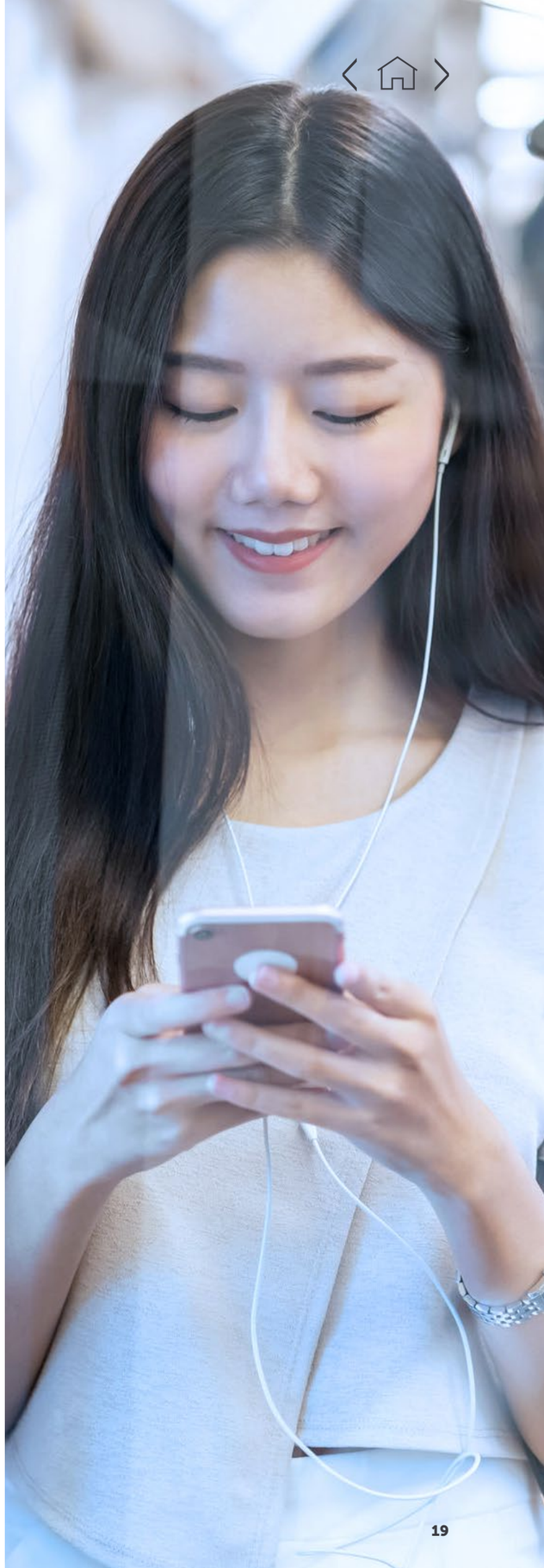
Future thinking
Key developments impacting the TMT industry globally in 2022

All of the changes introduced by the New Code are expression of the common European Union objectives on regulating the telecom industry in light of the changes in markets, consumer trends and technology over the last few years. In particular, the New Code's provisions include measures to stimulate investment in and take-up of very high-capacity networks in Italy, new spectrum rules for mobile connectivity and 5G, as well as changes to governance, the universal service regime, end-user protection rules, and numbering and emergency communication rules. The New Code gives national regulators the appropriate tools to deal with current and future technological challenges.

Alessandro Greco
Partner
alessandrogreco@
eversheds-sutherland.it

Antonio Campitiello
Associate
antoniocampitiello@
eversheds-sutherland.it

Lorenzo Maniaci
Associate
lorenzomaniaci@
eversheds-sutherland.it



Shaping the future

Navigating the risks and rewards of digitalization

Businesses are forecast to spend $10 trillion over a five-year period on digital transformation[1]. Digitalization is game changing. But it comes with numerous risks, challenges and obligations that need to be understood and navigated to stand the best chance of success.

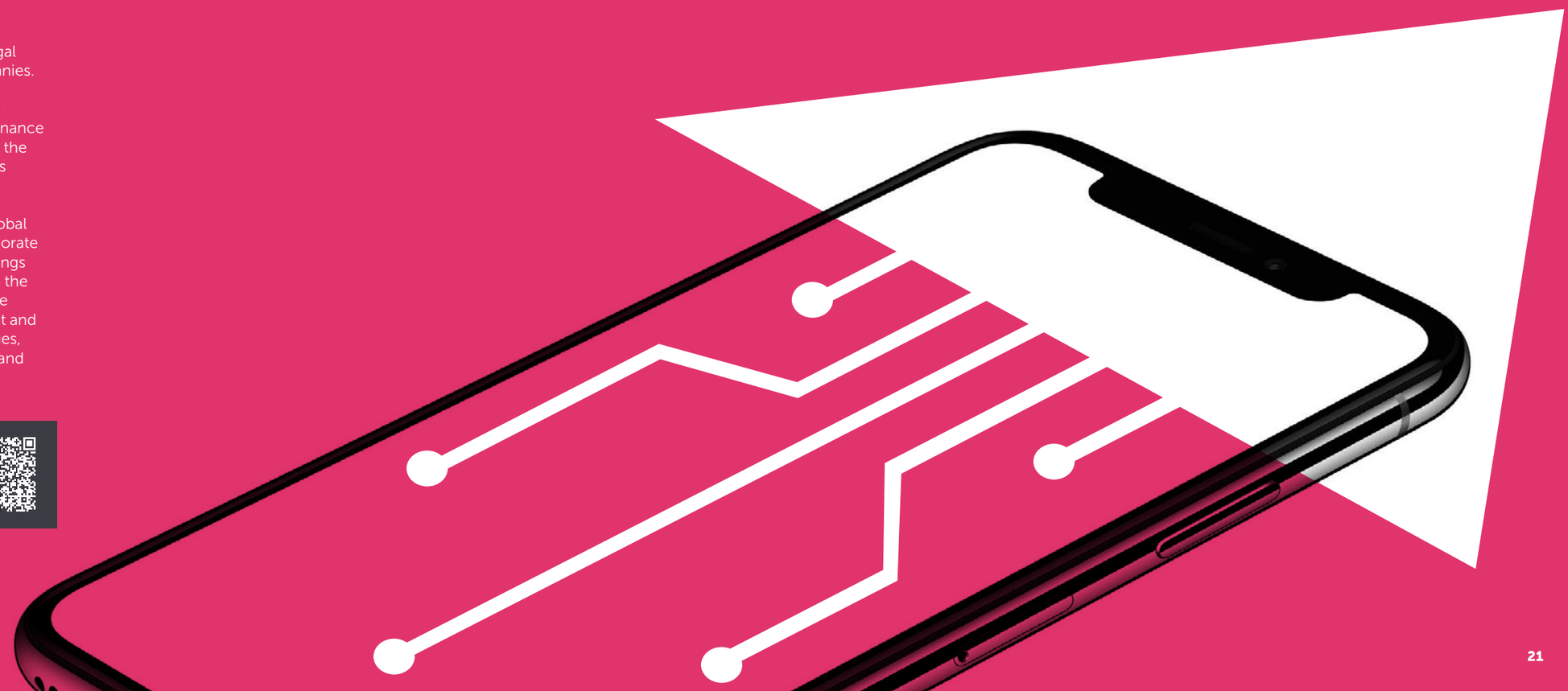
There are numerous complex laws and regulatory responsibilities across the globe, both current and impending, that create or will create significant legal obligations around digital responsibility for companies. These laws extend significant obligations and expectations to the board and senior leadership in relation to ensuring adequate oversight and governance in this area. It is now a business imperative to have the right approach and strategy to deal with these risks and obligations.

Our report "Shaping the future of digitalization: global perspectives on digital technologies, risk and corporate digital responsibility (CDR)" highlights the key findings from a survey of 700 senior executives globally on the uptake of digital technologies, as it relates to future digitalization strategies, M&A activity, development and procurement activity, perceived risks and challenges, approaches to the responsible use of technology and data, and corporate digital responsibility.

Read the full report here.

1 **https://www.idc.com/getdoc.jsp?containerId=prUS48372321**

Future thinking
Key developments impacting the TMT industry globally in 2022



Future thinking
Key developments impacting the TMT industry globally in 2022

The power of data:
increasing collaboration between competition law and data privacy

From both a competition, consumer and privacy law perspective there is a dilemma in relation to how people gather and access data. There has also been increased collaboration between competition and data privacy, both in respect of law and regulators. As such, increasingly we are seeing issues relating to how to address the intersection of these two areas, both as external legal advisers and commercial organizations dealing with those overlapping frameworks.

What does competition law have to do with privacy?

Traditionally businesses competed on price and quality of goods/service only. However, data has become an important parameter of competition. Personal data is often processed in exchange for goods or services that are free or do not reflect the value of the data; data generates revenue; data is a unique asset and may be hard to replicate; and data enables customized advertising, marketing, pricing and decision-making.

In the UK, the Information Commissioner's Office ("ICO") and the Competition Markets Authority ("CMA") have a memorandum of understanding on how the two areas should work together. The understanding is that robust data protection can support vibrant competition in digital markets.

Previously, regulators had not considered competition and data to be natural neighbors, however, this has changed as the regulators have become increasingly aware of the fact that data generated can be just as valuable as the product/service itself.

Data can be a source of market power and have limiting effects on competition, for example, by allowing price discrimination (for example, vertically integrated platforms such as marketplaces can adjust products and pricing more efficiently), facilitating price collusion through pricing algorithms, establishing barriers to entry, and cementing a substantial position that a company already has in the market.

Regulators around the world are considering how to address these issues in digital markets and are encouraging the legislator to take action and adjust the law in a way that equips the regulators with the toolbox needed to deal with these issues.

How can the acquisition of data create market power?

There are a number of recent competition law cases, both in Germany and the UK, highlighting the importance of data in creating potential market dominance which may, in turn, prejudice adequate competition in relevant markets. These are outside of the scope of this note but a relatively quick internet search throws up an increasing number of examples. These are not only confined to the acquisition of business assets and companies but may also arise where a group of companies shares data sets between its parents and associated subsidiaries (whether this is permitted depends on the nature of the privacy policies in question at the time and the extent to which you may be considered to have dominance in a particular market and behave potentially abusively as a result of consolidating data sets (whether of personal or non personal data intelligence)).

Future thinking
Key developments impacting the TMT industry globally in 2022

What new laws are on the horizon that seek to address some of these issues?

Germany

In Germany the Acts Against Restraints on Competition has been modernized to address the specific competition problems in the data based economy.

Some of the new rules are particularly relevant to data heavy companies. Previously, German merger control was triggered only if the parties met certain worldwide and national merger control thresholds. However, there are situations where, for example, a start-up with little turnover may be acquired due to the data that it holds or will hold if successful. As such, a new test has been introduced, which captures any acquisition where there is a disproportionality between the target's turnover and the purchase price. The regulators have also tried to quantify what this means by setting out that this would arise where the purchase price is €400m or more, and the target has virtually no turnover.

Regulators have also introduced a review for specific companies of which they are suspicious. Certain companies are required to record and notify each and every acquisition they do irrespective of size, to the regulator for three years following the decision made.

Furthermore, the German competition authority has gained new powers allowing it to focus on companies with huge data sets, monitor terms and conditions and behaviour (for example, if the companies give preferential treatment to their own products). A right to claim private damages in cases where such abusive behaviour occurs has also been established and we may see a lot of lawsuits resulting from that.

EU

The EU has proposed a Digital Markets Act ("DMA") which will be very similar to what exists in Germany and would provide the European Commission with the means to intervene in similar cases, with the possibility of imposing fines/remedies and, in worse cases, to even break up companies. The DMA is designed to tackle the dominance of large, systematic online platforms who are considered to be "gatekeepers".

A company will be considered to be a "gatekeeper" if it has:

- a strong economic position, is active in multiple EU countries and has a significant impact on the internal market
- a strong intermediation position (is able to link a l arge user base to a large number of businesses)
- an entrenched and durable position in the market

If a company fulfils the criteria, a number of obligations will be imposed on it relating to its daily operations. Examples of these include that gatekeepers will have to allow third parties to inter-operate with their own services in certain situations and that they will not be able to prevent users from un-installing pre-installed software and/or apps.

There will also be consequences for non-compliance, including potential fines of up to 10% of the company's annual worldwide turnover and periodic penalty payments. The DMA also contains provision for the imposition of additional remedies following systematic infringements, including non-financial remedies as a last resort.

UK

In the UK, the UK Government recently conducted a consultation on a new "pro-competition regime for digital markets". This foresees three major changes:

- the introduction of a legally enforceable code of conduct for firms with "strategic market status" ("SMS"). This would be tailored for each firm based on its activities and business model, and centred around (a) fair trading; (b) open choices and (c) trust and transparency. The aim of the code would be to prevent SMS firms from abusing their market power and exploiting consumers and businesses
- empowering a new regulatory body (the Digital Markets Unit which would sit within the CMA) to impose pro-competitive intervention remedies to address market features which hinder competition and innovation including data-related interventions, such as enabling data portability
- the introduction of a new merger control regime for SMS firms. The current UK regime is voluntary, however, the UK Government is considering introducing a new mandatory merger control regime for SMS firms where their transactions meet (a) a certain transaction value test (£100-£200 million) and (b) a UK nexus test. In addition, SMS firms would be required to notify the CMA of all of their imminent transactions

Are there any practical considerations relating to M&A deals which aim to merge data sets or implement a "customer single view"?

In a general sense, from a privacy perspective, it may be unlawful to merge data sets. However, issues also arise relating, for example, to commercial data sharing agreements done at an arm's length or intragroup.

A company obtains a huge advantage from having a single view of customers across the company group and it provides them with a huge competitive edge. However, the consumer may not be happy with their data being shared in this way. As a consumer, you deal with one particular brand/company, and you may not have anticipated your data being shared with another brand, which is completely different to the company with whom you shared your data.

Offline vs. online markets

Although the focus is on "digital markets", this may be misleading. This new regime is all part of the general trend of digitalization generally and there is no segregation between offline and online markets. The issue of data and competition also arises in numerous other sectors, outside of the social media or app-based arena, for example in the: automotive sector or insurance sector. Many markets have significant datasets which have the potential to give great market power/dominance. For example, Tesla has made huge steps in terms of innovation into electric cars but they also have a heavy emphasis on digital applications and data in those cars.

Can you give us an example of how data can be a barrier to entry?

Open Banking in the UK is a good example. Following a market investigation into retail banking back in 2016, the CMA concluded that the market was not working well. The CMA found that there were barriers to accessing information, barriers to switching and low levels of customer engagement. The combination of these features meant that there was a weak customer response to differences in prices or service quality. This lead to banks having unilateral market power over their existing customer base.

As a result, the incentives on banks to compete on prices, service quality and/or innovation were reduced. In addition, due to barriers to entry and incumbency advantages, the larger longer established banks were able to maintain high and stable market shares.

One of the remedies imposed by the CMA on the nine largest institutional banks in the UK was to open up their respective customer bank account data sets to promote, encourage and facilitate Open Banking.

Businesses sometimes enter into data sharing or data licensing agreements. What practical considerations should businesses consider when entering into such agreements?

It is relatively easy for data licensing agreements to be drafted in a way that can appear anti-competitive, for example, including provisions which restrict access to datasets or which impose obligations on other licensees and industry stakeholders which may distort markets and create unfair advantages for the companies that control those datasets.

Sharing data sets which disclose market industry data may inadvertently and unlawfully be classified as 'insider trading' (especially in the context of publicly listed or similarly industry regulated entities).

The following are examples of provisions in such clauses which may be unlawful:

- requiring a licensee, as a condition of access or license, to provide and grant a reciprocal license to its own (and other's) data sets (e.g. for the purposes of ensuring that the licensor is able to achieve a monopoly over a particular category or sector data set (or to 'feed' an algorithm with a particularly voracious appetite)
- reliance on a 'more favored nations clause' whereby a licensor (or a licensee) is required to offer the same or materially no less favorable terms to a counter-party (where it subsequently or otherwise has offered better terms to another commercial partner)
- terms which seek to require a distributor of data to 'fix' the price at which data is sold or licensed
- arrangements whereby one or more organizations agree to share industry data with one another so as to enable an algorithm to set unfair or higher pricing for a specific type of customer or consumer; and terms which allow the sharing of sales or performance data between a regulated entity and an investment fund, providing an unfair commercial advantage over other buyers of stock in a public listed market

Philip James
Partner
philipjames@
eversheds-sutherland.com

Martin Bechtold
Partner
martinbechtold@
eversheds-sutherland.com

Ros Kellaway
Global co-Chair of Competition, EU and Trade
roskellaway@
eversheds-sutherland.com

Annabel Borg
Legal Director
annabelborg@
eversheds-sutherland.com

Future thinking
Key developments impacting the TMT industry globally in 2022

Powering forwards:

how the data centers industry is driving the TMT transactional market

Alongside other data infrastructure assets, particularly mobile towers and subsea cables, data centers have continued to benefit from high levels of investment, with the volume of data center transactions being driven both by enterprise divestment and by consolidation. Following a number of significant data center deals at the tail end of 2021, including the sale of our client CyrusOne to a consortium led by KKR and GIP, and with continuing growth in the development of new data centers across the globe, the expectation is for 2022 to be another year in which the market runs hot.

Underpinning all of this activity, there are a variety of factors at work, including the ongoing impact of the pandemic driving online activity, the roll out of 5G and IoT technologies, and the surge of users towards public and hybrid cloud solutions. Increasingly over the last few years, enterprises have been moving away from on premises operations to cloud services, seeking the cost reductions and increased flexibility and capacity of a public cloud solution. Much of this demand is being met by the hyperscalers, who have the scale and financial resources to make sizeable global investment. And while there certainly remains plenty of scope for smaller data center operators, they can often become targets for consolidation as the hyperscalers seek opportunities for increased capacity and geographical growth.

But it is not just the existing data center operators who have seized the opportunity. As the CyrusOne deal illustrates, private equity has also accounted for some of the largest recent transactions, with investors who have large amounts of capital to deploy and are willing to pay significant multiples fueling the market in their quest to achieve scale and meet the ever increasing demand. Where the level of data center investment required is too much for even the largest operators, this influx of new money from external investors is helping to keep the growth of the sector on track.

So we certainly expect to continue to see high levels of data center M&A activity going forwards, but there are several factors which will be increasingly relevant considerations for those doing these deals:

- the environmental impact of data centers is under increasing scrutiny, as pressure builds on operators to make their data centers more energy-efficient and to reduce reliance on fossil fuels. This in turn is driving new technologies and new operational models to make these businesses more environmentally sustainable, with a consequent shift in the focus of new investment activity in the sector (including its supply chain). And in implementing data center transactions, the sustainability credentials and environmental compliance of target businesses is going to be even more of a key priority through the diligence process
- across the globe, there continues to be increasingly robust foreign direct investment regulation being applied to sectors and assets which are of national interest. In the UK, the new regulatory regime introduced by the National Security and Investment Act 2021 has the potential to impact at the least on the timeline for data center transactions (both share and asset deals), given the central importance of data centers to so many applications on which governments and consumers rely. While the full extent of the implications of the NSIA for data center deals is yet to become clear, for now it's an additional consideration to be worked through carefully by investors in their deal planning

The rapid evolution of the landscape of the data center sector – advances in product and operational technologies, the emerging cast of leading operators and investors and the extraordinary rise in global demand - has propelled this sector to the front and center of the TMT transactional market. There is every reason to believe that it will continue to occupy that position over the months to come.

Future thinking
Key developments impacting the TMT industry globally in 2022

Giles Dennison
Partner
gilesdennison@
eversheds-sutherland.com

Sebastien Bonneau
Partner
sebastienbonneau@
eversheds-sutherland.com

Digitalization in The Netherlands:

an opportunity and a threat

Digitalization is one of the key pillars in the new Dutch coalition agreement for The Netherlands as prosperous country. It states that the digital revolution offers great opportunities for the Dutch society and economy and The Netherlands are hoping to capitalize on the already existing excellent digital infrastructure and the ambitious cooperation between the sciences, businesses, 'startups', 'scale-ups', knowledge coalitions and the government.

At the same time, and this seems to get more attention, digitalization is also a potential threat for our security, rule of law, democracy, human and fundamental rights and our competitiveness. This requires solid rules, supervision and strategic autonomy.

Whether this will lead to substantial Dutch legislative action is to be seen because it seems that we will rely mostly on European legislation. It is to be expected that cybersecurity will get more attention and that the special Dutch governmental agencies tasked with cybersecurity, the National Cyber Security Centre and the Digital Trust Centre, will be more vocal in warning against cybersecurity threats and promoting measures to protect against cybersecurity attacks.

Regulation on Digital Operational Resilience ('DORA')

On 24 September, the European legislative proposal COM(2020) 595 was issued, which relates to the proposal for a uniform and legislative framework in the field of cyberthreats: Regulation on Digital Operational Resilience for the financial sector ('DORA').

The Dutch government endorses the importance of strong digital resilience. It is therefore no surprise that the Dutch government takes a positive view on this new Commission proposal in its assessment and position paper. This is addressed, among other things, in the Dutch Cyber Security Agenda. In view of the cross-border and interrelated nature of cyber security and cyber threats in the financial sector, the Netherlands considers a European and international approach important. In addition, the digitization of financial services is increasing, as a result of which digital threats pose a great risk to financial stability and confidence in the financial system in the Netherlands.

Financial supervisors attach great value of this as well; the Netherlands Authority for the Financial Markets (AFM) and the Dutch Central Bank (DNB) give priority to digital resilience in their supervisory strategies for the coming years. The basic rules that emerge from the DORA regulation concern ICT governance, the timely reporting of ICT incidents, conducting a basic test and the role of third-party service providers, among other things. In addition, the reporting obligation will play an important role for all parties in the financial sector. These must be clear. The National Cyber Security Centre (NCSC) will play a role in the reporting of incidents by essential services. By including basic requirements, there is room for flexibility. This should benefit smaller companies in the financial sector. How the exact financial and administrative consequences for companies will turn out in practice remains to be seen.

Future thinking
Key developments impacting the TMT industry globally in 2022

Proposal for the European Cyber Resilience Act

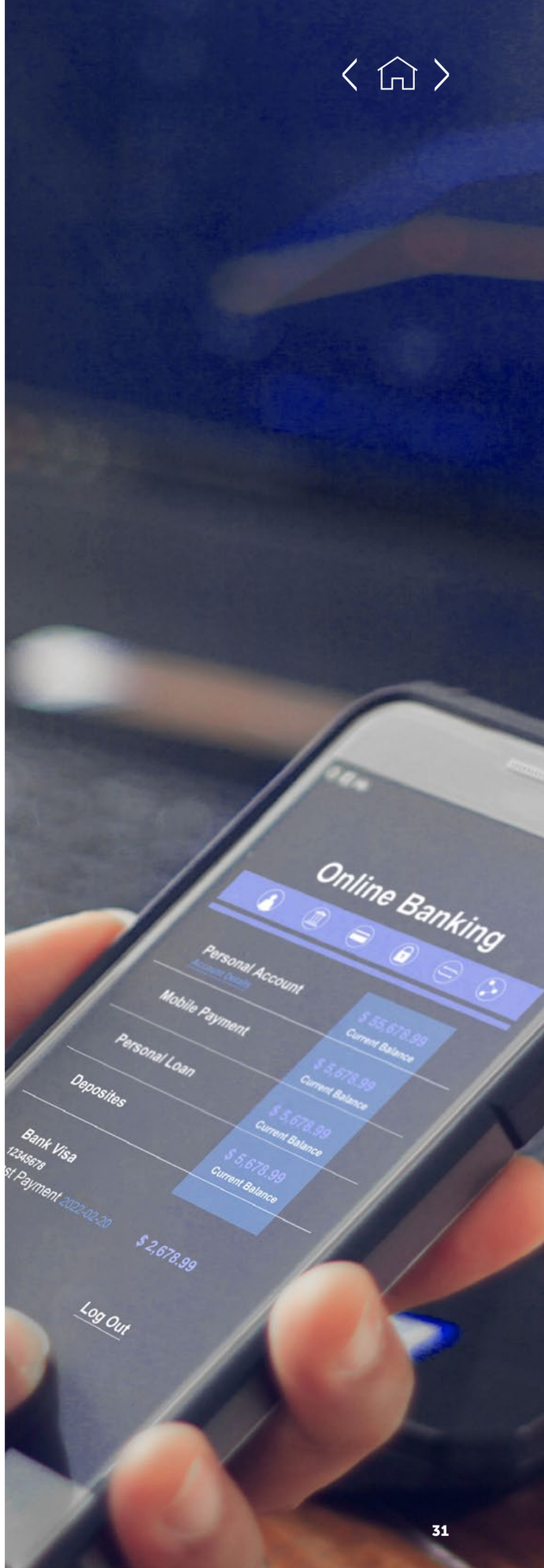
Although DORA is specifically addressed to the financial sector, cyber resilience will remain an important topic of the EU. In the Netherlands we recognize the increasing risk and vulnerability to cyber-attacks. As of 16 March 2022, the European Commission has opened a public consultation for feedback on the proposal of the Cyber Resilience Act. This Cyber Resilience Act would include horizontal cybersecurity requirements for digital products and ancillary services, which should complement the NIS-Directive and the Cybersecurity Act. The proposal for this Act will be in line with the ambitions of the Netherlands to be a front leader in strengthening cybersecurity resilience in the Netherlands. To that extent, as with DORA, this Regulation will likely be addressed in the Dutch Cybersecurity Agenda. This agenda includes several ambitions under which the aim of the Netherlands to possess resilient digital processes and a robust infrastructure and to successfully raise barriers against cybercrime by means of cybersecurity. It is most likely that the rules following from the Cyber Resilience Act will be endorsed by the Netherlands as to have one clear set of requirements when it comes to cybersecurity of digital products and ancillary services. This will have an impact on Dutch companies that offer such products and services. The Cyber Resilience Act is planned to be adopted 2022.

Olaf van Haperen
European TMT Lead
olafvanhaperen@
eversheds-sutherland.com

Robbert Santifort
Senior Associate
robbertsantifort@
eversheds-sutherland.com

Natalia Toeajeva
Trainee
nataliatoeajeva@
eversheds-sutherland.com

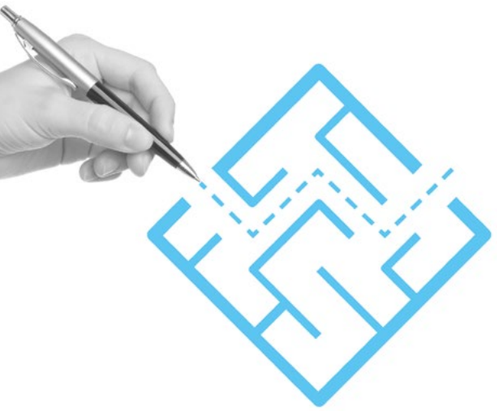
Nathalie Djojokasiran
Trainee
nathaliedjojokasiran@
eversheds-sutherland.com



Business protection:
the global use of restrictive covenants in employment

One of the consequences of the pandemic has been to boost the prospect of using technology to work from anywhere in the world. Employers willing to entertain that possibility for their existing workforce or in order to widen their talent pool face a number of tax, immigration and other legal considerations. However, an issue that can often be overlooked where the location of work is more fluid and spans jurisdictions is ensuring the appropriate protection of a business's client and supplier base and other legitimate interests, including through the use and enforcement of restrictive covenants.

Restrictive covenants are typically used to prohibit an employee or ex-employee from working for a competitor or performing competitive activities (non-compete provisions) or soliciting customers, suppliers or employees (non-solicitation and non-dealing provisions). The use of such restrictions across jurisdictions has the added complexity of different laws and practices dictating whether, where and how such clauses may be used and enforced.



Restrictions – a new tide of government regulation?

With the pandemic propelling the need for governments to support economic bounce-back, many governments are exploring ways to encourage and remove perceived barriers to innovation and competition and to maximize opportunities for individuals in the labor market.

The use of restrictions in employment, particularly non-compete clauses in contracts of employment, has been one area of focus for some governments, including in the UK and the US. In particular, there has been a focus on how to achieve an appropriate balance between ensuring the labor market is as open as possible and competition is not stifled, while at the same time protecting businesses' confidential information and proprietary interests in relationships that they have invested time and resources in developing.

In many jurisdictions, there are already legal constraints on the use of restrictive covenants, however the pandemic has spurred a renewed focus on that regulation. For example, in July 2021, President Biden signed an Executive Order on Promoting Competition in the American Economy, where it is proposed to introduce new rules banning or limiting non-compete agreements. In the UK, a government response is awaited following the public consultation that closed in February 2021 regarding potential curbs on the use of contractual post-termination non-compete clauses. In Finland, new legislation entered into force on 1 January 2022, ensuring that workers have an entitlement to compensation for all post-employment non-compete restrictions, with minimum levels of compensation and a maximum duration of restraint. In Washington state in the US, also with effect from 1 January 2022, salary/fee thresholds now apply for post-employment non-compete agreements to be enforceable against employees/ contractors.

Future thinking
Key developments impacting the TMT industry globally in 2022

In addition, the protection of confidential information, particularly that amounting to trade secrets, has been a focus. In China, the Anti-Unfair Competition Law was amended in 2019 and saw additional guidance being issued during 2020. In particular, this elaborated on the definition of trade secrets, the scope of prohibited acts and the potential administrative, civil and criminal liabilities. Those changes have resulted in a shift in the risk profile for the protection of confidential information in China, broadening the scope of protection for businesses and clarifying the activities that are unlawful, which expressly include using trade secrets in breach of confidentiality obligations.

In Europe, member states transposed the EU Trade Secrets Directive into national legislation between 2017 and 2019, which has resulted in a more defined legal framework in this area than previously existed in some jurisdictions. In addition, it has established a more harmonized understanding of what constitutes a trade secret and the different forms that misappropriation of such information can take in order to gain legal protection.

Use and enforcement – can an effective global approach be achieved?

For multi-national employers, global approaches around people strategy can often seem attractive, having the advantages of consistency of treatment, ease of messaging for implementation and simplicity in terms of policies and procedures. However, there are a number of reasons why striving to find a universal approach to the use and enforcement of restrictive covenants globally that is both effective and lawful is unlikely to be successful.

Permissibility of use

The extent to which post-termination restrictive covenants are permitted varies by jurisdiction, with some countries also having variations by state or region. For example, in Russia post-termination restrictions, whether non-compete or non-solicitation, are generally not permitted, except to ensure the non-disclosure of confidential information. In India, post-termination non-compete restrictions are not enforceable as a matter of law, although reasonable non-solicitation covenants and confidentiality provisions can be agreed.

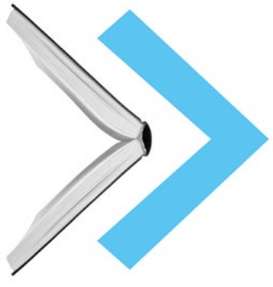
Scope of protection

Even where restrictive covenants are in principle permissible, the limitations around permitted scope vary by jurisdiction. Factors such as the type of interests that are capable of protection, the duration of the period to which the restriction applies, the geographic scope of the restraint and the type and seniority of employee, can all have an impact on enforceability. The use of such clauses to simply stop competition is rarely permitted and tailoring the restriction, taking account of any local limitations around permitted scope, will be particularly important if the enforceability of the restraint is to be maximized.

Compensation

In some jurisdictions, there will be requirements to provide compensation as a condition of the use of post-termination restrictive covenants. For example in Germany, where payment has to be made for the duration of any non-compete, non-dealing or non-solicitation restriction, in the amount of at least 50% of remuneration. Similarly in Belgium, a payment equal to at least 50% of the gross remuneration is generally required for the duration of a non-compete restriction. In China, monthly compensation is required to be paid during the period of any post-termination restriction, with the default position being that 30% of the average pre-termination monthly remuneration is payable.

For those countries that require compensation to be paid for the use of restrictive covenants, the calculation of that compensation can sometimes take account of elements beyond basic pay, such as bonuses and the value of other benefits, particularly where the right to such additional elements is incorporated into the terms and conditions of employment. Where applicable, this can significantly increase the amount payable in return for the benefit of restrictions and will therefore be an important consideration in their use.



Future thinking
Key developments impacting the TMT industry globally in 2022

Waiver

Although having restrictions in place may seem appropriate at the time they are entered into, that view may change at a later date, particularly where compensation is payable for their use. The ability to simply waive the right to rely on the restriction may however be limited in some countries. In Germany, waiver is possible pre-termination, but this will not automatically cancel the payment obligation, which for most categories of employees continues for 12 months after the waiver being declared. Waiver is also possible in France, but it is often the case that an applicable collective bargaining agreement will specify the required timings of such waiver.

Duration and geographical scope

The permitted duration and/or geographical scope of restrictions can also vary by jurisdiction. For example, in Argentina, a non-compete restriction of up to two years is permitted. In contrast, in Poland, the maximum duration of non-compete restrictions tends to be significantly less, in the region of three to nine months. The position held by the employee can also have an impact. In Italy a maximum duration of three years for non-compete restrictions can apply, but for executives this is extended to up to five years. In Spain, a restriction may last for up to two years for certain specialist or highly-qualified workers, but is limited to six months for other workers.

Garden leave as an alternative to post-termination restrictions?

Notice periods can often span many months. Particularly when coupled with a requirement to pay compensation for the use of a restrictive covenant at the end of the notice period, this can result in an ongoing financial commitment for a significant period that may outlast the benefit of the restriction. To avoid this, while at the same time ensuring a period where the employee is kept out of the market and therefore unable to compete, many companies consider the use of garden leave (i.e. a period where an employee remains on normal salary and bound by their contract of employment, but can be prohibited from attending the workplace or having contact with customers). In some countries, for example Brazil, the use of garden leave is not allowed, but where permitted under the employment contract and local law, garden leave can be an effective alternative to the use of restrictive covenants or can reduce the required duration of such restrictions.

See our at-a-glance comparison of some sample jurisdictions.

Cross-border enforcement of restrictions

For multinational employers considering the use and enforcement of restrictive covenants across borders, it will be critical to understand the applicable law that that will govern any restriction and where the restriction may need to be enforced. That understanding will inform not only the way in which any restriction should be drafted to maximize its enforceability but also the appropriate enforcement strategy.

The starting point is that, as long as the choice is expressed or demonstrated with reasonable certainty in the contract, the parties have freedom to choose the applicable law. However, this freedom is usually limited by legislation, with many jurisdictions having conflict of law rules that require the application of local employment law in certain circumstances where they are more favorable to the employee.

In all EU member states (other than Denmark), for contracts made on or after 17 December 2009 and where the governing law of the employment contract has not been chosen, under the so called Rome I Regulation the particular circumstances will determine the governing law. Consideration is given to where the work is habitually carried out, the place of business and/or the closeness of connection with a particular country. This includes consideration of the place from which the worker carries out tasks and receives instructions, where the employer and/or worker are based, the location of any tools or equipment, the place to where the worker returns after completing the tasks, how the worker is paid, how the worker is managed and the locations from which disciplinary decisions emanate.

It is also important to bear in mind that the fact that a country's law is the governing law of a contract does not mean that claims under that contract can be automatically brought in that country's courts. Whether a national court has jurisdiction to hear a claim with an international angle will be determined by applicable local legislation (or EU legislation, where applicable).

Giving early consideration to these factors will be an essential element of an effective business protection strategy.

Summary - the global use of restrictive covenants for business protection

In the wake of the pandemic, it is expected that movement in the employment market will continue to grow, with a consequent rising importance of having a strategy in place to safeguard business relationships and confidential information. Although the ability to restrict certain activities varies significantly around the world, having in place up to date enforceable protections can maximize the options available should an individual depart and seek to operate in a manner that has the potential to damage the business.

Practical checklist for employers considering the use and enforcement of restrictions in employment.

Global enquiry and analysis - understand the legal position in relation to the use and enforcement of restrictive covenants in employment in all jurisdictions of operation.

Strategic planning – determine the approach to be taken that best fits the organization's culture and attitude to risk and business protection.

Tailored restrictions – where a strategy is adopted that seeks to maximize the enforceability of restrictions, ensure that the restrictions are carefully drafted to take account of the legal position in the jurisdiction of operation. This may mean tailoring the restriction based on the type of interests that are capable of protection, the duration of the period to which the restriction applies, the geographic scope of the restraint and/or the type/ seniority of the employee.

Choice of law – ensure the appropriate use of choice of law clauses, including taking account of enforceability and/or remedy.

Future thinking
Key developments impacting the TMT industry globally in 2022

Reviewing and updating – ensure that a process is in place to ensure that restrictions are regularly reviewed and do not go out of date, for example as a result of promotions, transfers, changes in location or changes in client portfolio.

Leaver process – determine the approach to be taken when a key employee announces that they are leaving, to secure key information and relationships.

Monitor developments – reforms on the legislative landscape in relation to the use of restrictive covenants reflects a trend in recent public policy that employers should monitor and be mindful of when considering the use and enforcement of restrictions.

Diane Gilhooley
Global Head of Employment, Labor and Pensions
dianegilhooley@
eversheds-sutherland.com

Paul Fontes
Partner
paulfontes@
eversheds-sutherland.com

Constanze Moorhouse
Partner
constanzemoorhouse@
eversheds-sutherland.com

A different playing field:
how has technology influenced sports?

Technology: the most valuable player in the Sports industry.

Take a snapshot of the modern day sports industry. What do you see? How we play sport, how we watch it, and how we exploit it commercially is now being driven by an increasingly evolving force – technology. Last year, the global sports technology market reached an all-time high of roughly US$18 billion. By 2026, it is touted to hit US$40billion. Sports tech is big business. So what are some of the main players behind this rapidly evolving industry and what does the future hold?

The exploitation of sports data rights, in particular performance data, is an exponentially growing area within the sports industry that brings cross-sector engagement from a range of stakeholders. Sports leagues, for example, are increasingly engaging data analytics firms to analyze and collect player performance data, which in turn is distributed to third party businesses in the sports betting, fantasy sports and video game worlds. In 2021, we also saw a remarkable shift in the way in which contract negotiations for athletes are undertaken. Manchester City FC's Kevin De Bruyne is one example, who engaged a data analytics firm to support his negotiations for a new contract with the club. Through the use of AI (specifically, algorithms), De Bruyne was able to demonstrate his future performance and value to the club based on various subsets of past performance data. The result? A new five year contract worth £20 million a year.

For the fans, the demand for quality content and engagement has never been higher. The COVID-19 pandemic has accelerated a paradigm shift in OTT streaming consumption that was already fast moving, and the sports industry certainly played its part. Whilst we may not have been able to watch our favorite sports team in person, through the beauty of live broadcasting on a variety of platforms and devices, enhanced by AI simulated crowds, automated cameras and remote studios, we still managed to get our sports fix.

But demand for quality entertainment now stretches far beyond live sport. Cryptoassets, in particular the advent of non-fungible tokens (NFTs) and fan tokens, are now driving growth in sports across the globe. A significant amount of capital is now flooding the NFT market, leading to the launch of various NFT projects across a number major sports. Currently, one of the most popular sports-related NFT applications is NBA Top Shot – the NFT marketplace for NBA highlight reels, notching over US$700 million in sales in less than a year. In the UK, it is no surprise that the Premier League has ramped up its plans to enter the world of digital memorabilia, with an NFT offering for fans likely to arrive later this year. Meanwhile, fan tokens are taking the Premier League by storm, with a number of clubs now offering fan tokens that give holders access to a variety of fan-related perks, from voting rights in club polls to access to unique content.

And last, but certainly not least – esports. The world of esports now rivals that of traditional sports, and professional gamers are not only elite athletes, but superstars. As esports continues to integrate into popular culture, everyone is paying attention – from celebratory investors and mainstream media platforms to luxury brands and consumers. Consequently, the industry has seen a large increase in investment from venture capitalists, and more recently from private equity firms. In 2021, the global esports market was valued at just over US$1 billion, an almost 50% increase from 2020. For 2022, it is projected to reach US$2 billion, with the lion's share of revenues generated by media deals, sponsorships and broadcasting rights.

Sebastian Butcher
Associate
sebastianbutcher@
eversheds-sutherland.com

Smart thinking:
how smart contracts are changing the legal industry

Smart contracts are increasingly gaining traction within the legal industry, due to their potential to save time and costs, however, there can be drawbacks which need to be fully understood.

Smart contracts is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain. The code can either describe the entire agreement between parties or it can supplement a text based contract and execute certain clauses, such as termination of an agreement at a specific date or transfer of funds from one party to another.

Smart contracts require defined and objective input parameters and execution steps, such as if X occurs, then execute step Y, and once these criteria are met, smart contracts can self-execute, eliminating the need for intermediaries or third parties.

Transactions are recorded on the blockchain, which is a public database that records and monitors all automated contract executions in the order they occur. Because transactions cannot be reversed or rolled back, smart contracts are unmodifiable and final.

Smart contracts are gaining traction within the legal industry given some of the potential benefits including:

- contracts are self-executing as long as certain conditions are met, eliminating the need for third-party authorizations and decreasing the back and forth of creating, negotiating, and executing agreements. This has the potential to result in significant cost savings for the legal industry as a whole
- in order to execute, smart contracts require all terms and conditions to be precise and detailed, allowing no room for miscommunication or misinterpretation, as well as any potential of manipulation, bias, or error
- the terms and conditions of these contracts are fully visible and accessible to all relevant parties reducing disputes

However, while there are a number of possible benefits, there are also risks and areas to consider, including:

- the need to rely on a trusted, technical expert to either capture the parties' agreement in code or certify the accuracy of code created by a third party
- the need to be explicit about each provision and condition and translate that into contract code
- the requirement for additional levels of insurance and protection in the event that the smart contract code fails to execute or perform the necessary actions
- extra fees related with contract execution on various blockchain platforms
- contract enforceability, particularly where performance is connected to a subjective criteria such as "reasonable" or "best endeavors"
- some of the underlying technology used to support smart contracts is still in its early stages, and there may be vulnerabilities or concerns that are not yet known

Sectors based on defined rules and quantifiable terms of engagement, such as banking, insurance, and real estate, would gain first from investing in this technology, particularly in areas like digital payments, claims settlements, and modifications to public registries.

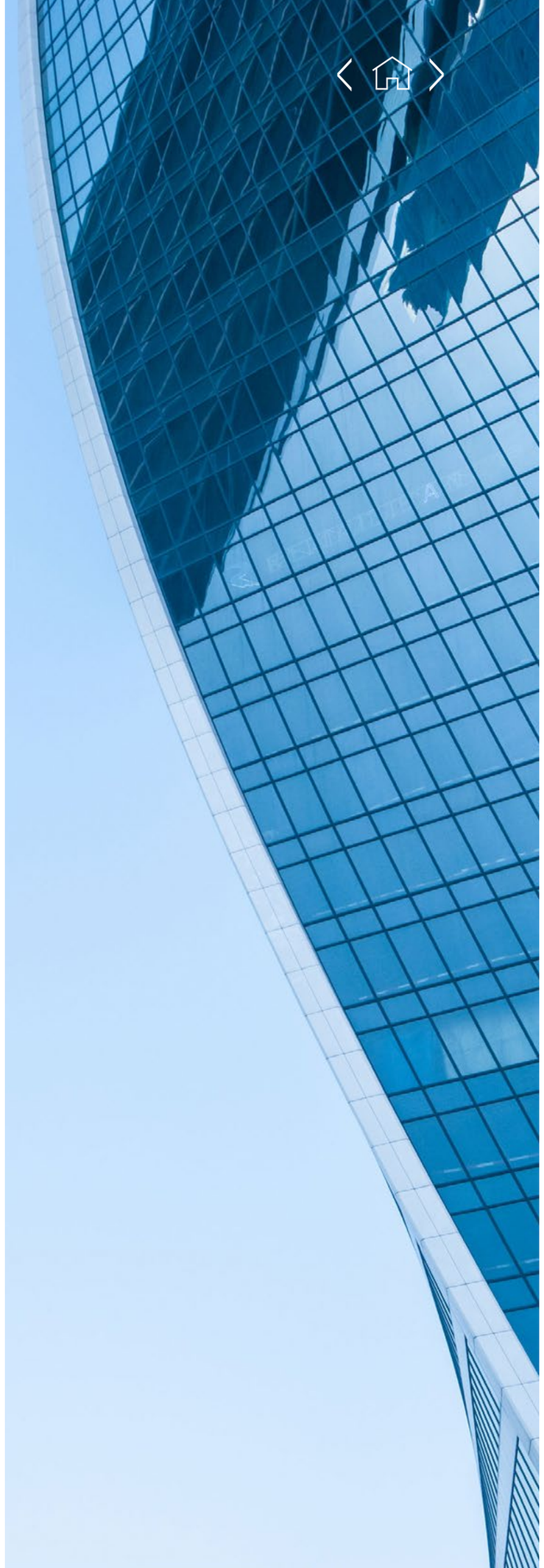
A recent **law commission report, published 25th November 2021**, concluded that the current legal framework in England and Wales is clearly able to facilitate and support the use of smart legal contracts, without the need for any statutory law reform. **In a recent update**, we noted that the same principles that apply to "traditional" contracts (e.g. interpretation of terms and conditions and errors which are contrary to the intention of the parties) could equally arise in the context of smart contracts.

Additionally, whilst the report will not fundamentally change the way existing applications of smart contracts technology are deployed, it will give companies and organizations (and their legal advisors) the confidence to develop smart contract solutions - and to attract investment - on the basis of a solid foundation based on existing legal principles.

Smart contracts have the potential to significantly alter the way the legal industry manages contracts, and businesses would benefit from exploring the opportunities and risks they present. However, there is still a long way to go and a number of key questions to be answered before smart contracts become widely adopted. Similar to other technology advances (e.g. electronic signatures), smart contracts are likely to have a beneficial influence on the way lawyers operate, while also increasing demand for legal services.

Babar Hayat
Head of Technology and Transformation
babarhayat@
konexoglobal.com

Craig Rogers
Partner
craigrogers@
eversheds-sutherland.com



Future thinking
Key developments impacting the TMT industry globally in 2022

Data centers – ‘to own or not to own?’:

the question facing many Hyperscalers and the subsequent impact on deal structures

The acceleration of digitalization as a result of the COVID-19 pandemic as put an increasing importance on data storage and the demand for powerful data processing at a global level. Subsequently, the grow of “Hyperscalers” such as Google, Meta or Amazon, that are intrinsically dependent on data storage and high performance data processing power, has had a significant impact within the data center industry on the way deals are structured.

A typical strategic issue for a CEO is to decide whether to ‘make it’ or to ‘buy it’. The common strategy is that only the core services of a company will be made internally, and the rest are outsourced.

In the context of Hyperscaler CEOs this decision has now reversed, and they are choosing to grow their own internal data storage capacities as a result of how important the storage and processing of data is in their business model. They are now more willing to source their own data center solutions, and subsequently become the legal owners of the land on which data centers are built.

The new variety of deal structures outlined below may also result in a more efficient use of cash reserves, as the money is ultimately invested in a real estate asset. This offers the Hyperscaler several options as to whether or not to operate the data center, manage the provision of electricity directly, avoid paying recurring payments to a data center provider eventually, or being in a position to transfer the reversion of the ground lease upon termination to the date center operator itself.

Classic Colocation LSA and Built-to-Suit NNN Lease

The Hyperscaler owns the site and grants a 15 year+ ground lease to the data centre operator. The parties develop and agree on a detailed design for the data centre, and the data centre operator is responsible for securing requisite permitting and developing the data centre in line with the detailed design. The data centre operator generally engages a general contractor and a professional team for that purpose.

On successful commissioning and testing, a 15 year Colocation LSA is granted on the data center halls by the data center operator to the Hyperscaler. During the term of that contract, the maintenance, operation and insurance of the data center (including typical colocation service level agreements) and all attendant OPEX and CAPEX costs is either supported by the data center operator (traditional ‘Colocation LSA contracts’), or is the responsibility of the Hyperscaler itself (‘Built-to-Suit NNN leases’).

In the Built-to-Suit NNN leases deals, the Hyperscaler is most frequently the sole occupier of the data center building. It manages the payment of electricity costs directly with the relevant utility provider, avoiding to pay for the power usage effectiveness (or ‘PUE’) uplift from the data center operator.

In both Colocation LSA and Built-to-Suit NNN leases deals, the data center operator is granted with the option to purchase the reversion of the ground lease at discounted market value at the end of the term of the Colocation LSA or NNN lease, as applicable.

New Design, Build & (optionally) Operate transactions:

The Hyperscaler owns the site and grants a building license to the data center operator, not a ground lease. The data center operator acts as a developer and the cost of developing the data center is directly supported by the Hyperscaler, on a monthly basis, against independent cost monitor's certificates. Any cost overrun beyond the cost budget is at the data center operator's risk.

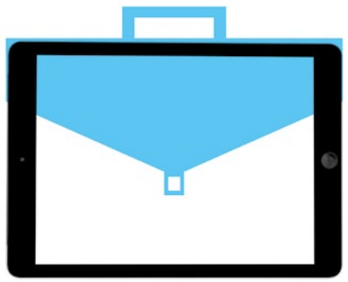
On successful commissioning and testing, the data center operator is expected to make a profit above the retention due to the general contractor.

As in Built-to-Suit NNN lease deals, the Hyperscaler – and not the data center operator – is responsible for the maintenance, operation and insurance of the data center, save for any defects arising during the defects liability period of typically 12 months after the successful commissioning and testing.

By default, the Hyperscaler will operate the site and there will be no recurring payments to the data center operator except for optional critical services and force majeure agreements. Optionally, the Hyperscaler may engage the data center operator to operate the data center, but will retain responsibility for all CAPEX costs.

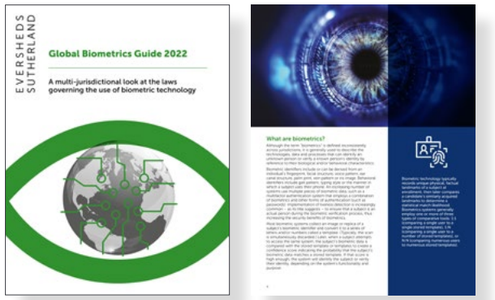
The increasing importance of data storage and demand for powerful data processing at a global level is not expected to decline for Hyperscalers in the decades to come. The recent influx of capital invested into digital infrastructure confirms this trend is here to stay.

Sebastien Bonneau
Partner
sebastienbonneau@
eversheds-sutherland.com



Global Biometrics Guide 2022:

a multi-jurisdictional look at the laws governing the use of biometric technology



As any fan of Sherlock Holmes can attest, identifying a person through their unique biological characteristics, such as fingerprints, is nothing new. Harnessing the power of cutting-edge technology and Artificial Intelligence (AI) to leverage an individual's inherent physical and behavioral traits is, however, another story altogether. Over the last 15 years, biometric technology has hit the mainstream, exploding into a multibillion-dollar industry and touching nearly every aspect of modern life. Whether through a simple finger scan to unlock a phone, access a bank account, move ahead of a queue or gain entry to a secure work area, or via a facial recognition scan as they move through a crowd, most people have provided their biometric information to a private entity, even if they do not necessarily know about it. The dramatic growth and innovation of biometrics only accelerated during the COVID-19 pandemic, as it became clear early in the crisis that biometrics are uniquely positioned to solve many practical problems that arise in a socially distanced world. As we look toward a post-lockdown world, the biometrics industry shows no signs of slowing. As is often the case with emerging technology, however, legal questions and hurdles abound. Across the globe, companies that employ biometrics – with their customers, employees and the public at large – must navigate a shifting legal and ethical landscape. This guide aims to provide an overview of relevant laws, regulations and other considerations for companies operating in many regions around the globe. We begin with the basics.

What are biometrics?

Although the term "biometrics" is defined inconsistently across jurisdictions, it is generally used to describe the technologies, data and processes that can identify an unknown person or verify a known person's identity by reference to their biological and/or behavioral characteristics. Biometric identifiers include or can be derived from an individual's fingerprint, facial structure, voice pattern, ear canal structure, palm print, vein pattern or iris image. Behavioral identifiers include gait pattern, typing style or the manner in which a subject uses their phone. An increasing number of systems use multiple pieces of biometric data, such as a multifactor authentication system that employs a combination of biometrics and other forms of authentication (such as passwords). Implementation of liveness detection is increasingly common – as its title suggests – to ensure that a subject is an actual person during the biometric verification process, thus increasing the security benefits of biometrics. Most biometric systems collect an image or replica of a subject's biometric identifier and convert it to a series of letters and/or numbers called a template. (Typically, the scan is simultaneously discarded.) Later, when a subject attempts to access the same system, the subject's biometric data is compared with the stored template or templates to create a confidence score indicating the probability that the subject's biometric data matches a stored template. If that score is high enough, the system will identify the subject or verify their identity, depending on the system's functionality and purpose.

Read the full guide here.

Frank Nolan
Partner
franknolan@
eversheds-sutherland.com

The gloves are off:

New Consumer Agenda from the EU Commission - how to prepare

The Europe Union ("EU") is taking the gloves off in the field of consumer protection law. As part of the EU Commission's "New Consumer Agenda", which presents a vision for EU consumer policy from 2020 to 2025, building on the 2012 Consumer Agenda (which expired in 2020) and the 2018 New Deal for Consumers, the new Omnibus Directive will be transposed to local law in all Member States with effect as of 28th May 2022.

When the local law adoptions of the Omnibus Directive come into force, not only online-based business models, which address consumers in the EU, but all sellers of IoT products will be addressed by a large number of new information requirements, because the EU implements additional requirements for the newly established product category of "Goods with Digital Elements". Offers of such products will have to include very specific pre-contractual information, such as information on functionality, compatibility and interoperability of goods with digital elements.

This package of information requirements sounds rather straight forward but it is actually a tough one which becomes clearer when read in conjunction with the recitals of the directive. For example, the requirement for information on the functionality of a product not only covers the immediate technical functions of the product. It also includes "the ways in which digital content can be used, for instance for the tracking of consumer behavior". By way of this information requirement, consumers, who are interested in the purchase of an IoT product will therefore need to be informed about privacy related topics, prior to the conclusion of the contract.

The implications of the new information requirements go far beyond potential attacks from competitors or administrative fines. In the example above, as of 28th May 2022, the mandatory information on compatibility, interoperability and functionality of the product, also serves as basis for the qualification of the nominal condition of the product from a sales law perspective. This means that, if the consumer is not informed properly, the product will actually be defective from a sales law perspective, triggering the consumer's warranty rights and remedies. This should be reason enough to ensure that adequate information on goods with digital elements is provided.

Additionally the public enforcement of consumer protection law in the EU will become significantly stricter in regards to administrative fines. Infringements of the new consumer protection rules under the Omnibus directive will be subject to administrative fines of up to 4% of the group-wide annual turnover, just as violations of the GDPR.

Nils Müller
Partner
nilsmueller@
eversheds-sutherland.com

Steffen Morawietz
Associate
steffenmorawietz@
eversheds-sutherland.com

World Economic Forum - Advancing Digital Agency:

The Power of Data

The power of the data ecosystem has never been greater but the system itself is becoming more difficult to navigate.

Michael Bahar, *Partner, Co-Lead, Global Cybersecurity & Data Privacy* and **Paula Barrett**, *Partner, Co-Lead, Global Cybersecurity & Data Privacy* join the Task Force on Data Intermediaries, co-authoring the World Economic Forum's February 2022 Insight Report.

The report explores the potential to outsource human decision points to an agent or trusted intermediary to act on an individual's behalf, with implications for many companies, including within the technology and financial sectors.

Read the full report here.

Fighting "Crypto" crime:
Criminal and civil law the dynamic duo

The adoption of "Crypto" assets in the execution of fraud and other financial crime has forced the criminal and civil law to adapt – can it keep pace?

Cryptocurrencies, blockchains and non-fungible tokens: these terms and assets have become increasingly mainstream and ubiquitous in recent years. Indeed, it is estimated that the transaction volume of cryptocurrencies alone was some $15.8 trillion in 2021 (up a staggering 567% against 2020), with a market capitalization of at least $2 trillion. Crypto-assets are no longer the purview of sophisticated institutional investors only, but of broader unsophisticated 'mom-and-pop' investors alike.

The rise of the crypto-economy, as well as the very nature of the assets, has resulted in the rise of crypto-crime as an ever-growing threat. Innovation in the crypto world is matched only by the rate at which criminals are developing new ways to exploit and criminally monetize crypto-assets, including through:

01 **Hacking and theft:** with crypto-assets generally stored in "digital wallets", assets have been irretrievably lost if private encryption keys to such wallets are hacked or stolen. Further, there have been numerous examples of crypto exchanges being hacked. One of the first Bitcoin exchanges, "Mt Gox", filed for bankruptcy following a cyber-attack in 2014, with over 850,000 Bitcoins stolen (worth approximately $8.5 billion today).

02 **Crypto-malware:** the infection of computers with undetectable malware to use the computing power (without its owner's knowledge) to 'mine' cryptocurrency, so called "crypto-jacking".

03 **Cyber extortion:** deployment of malware or "distributed denial of service" attacks that infects victims' computer networks. Payment is extorted from victims via virtual currency in exchange for suspending (or not deploying) such attacks.

The characteristics of crypto-assets and virtual currencies pose new challenges for regulators and investigating authorities. Crypto-assets provide a degree of "pseudo-anonymity", such that the identity of the owner, and payment account information, are not directly tied to the crypto assets (in contrast to a payment of a fiat currency via a traditional bank). Given that crypto transactions are typically decentralized, the monitoring and analysis of suspicious trading activity is severely restricted when compared to more traditional trading venues, and is further complicated by the ease with which cross-border transactions can be processed. These characteristics have led to fears of a significant increase in use of crypto in criminal activity such as money laundering, terrorist financing and even the evasion of sanctions.

Regulators and authorities are evolving to meet the challenges posed by crypto. The UK's Financial Conduct Authority (FCA) is generally considered to be ahead of the curve as regards regulators developing regulatory oversight and guidance for crypto assets. Indeed, all businesses that conduct crypto asset activities in the UK (including cryptocurrency exchanges and custodian digital wallet providers) are required under the Money Laundering Regulations to register with the FCA. Regulators have recognized the need to adapt their tactics, tools and enforcement activity, with HMRC in the UK recently seizing for the first time non-fungible tokens (NFT) as part of an investigation into suspected VAT fraud.

The civil courts have also adapted, and have demonstrated in several high profile cases that they will support victims of cyber fraud to recover losses, even if those losses have been sustained in crypto assets. In England and Wales (and many other common law jurisdictions), caselaw has established that crypto assets have the status of "property", opening up the pathway for victims to seek proprietary based remedies (including proprietary injunctions), which is key when the ultimate perpetrator of the fraud is unknown. Further, disclosure orders can be sought against cryptocurrency exchanges, to force them to disclose the identity of their client (i.e. the owner of a digital wallet). A key challenge remains that crypto currency exchanges are often (by their nature) difficult to pin down to a particular entity and jurisdiction, rendering it difficult for parties to establish a jurisdictional basis for relief and/or to enforce such an order when it is obtained. There will need to be an unprecedented level of cross-border cooperation between civil jurisdictions to address this challenge. While these challenges remain for victims of fraud whose losses are sustained in crypto assets, experience shows that, at some stage, fraudsters need to exchange their cryptoassets for fiat currency in order to meet "real world" expenditure.

Future thinking
Key developments impacting the TMT industry globally in 2022

Both criminal and civil laws are rising to the challenge posed by crypto assets, but the pace of change is frightening. Addressing these issues on a cross-border basis and the actions required by companies operating in the TMT sector to mitigate the ever growing risks they face, and to bolster the protections offered by governments and regulators are undoubtedly the challenges that need to be addressed.

Emma Gordon
Partner
emmagordon@
eversheds-sutherland.com

Tim Browning
Partner
timbrowning@
eversheds-sutherland.com

Daniel Jackson
Principal Associate
danieljackson@
eversheds-sutherland.com

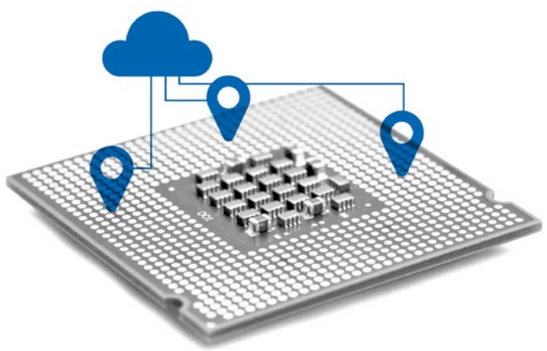
Kimberly Jones
Associate
kimberlyjones@
eversheds-sutherland.com

New Data Protection Laws in the Middle East:
what are the implications?

In line with the regional trends in the Middle East, Sultanate of Oman ("Oman"), Kingdom of Saudi Arabia ("Kingdom" or "Saudi Arabia") and United Arab Emirates ("UAE") issued their very first standalone Data Protection Laws. In September 2021, both, Saudi Arabia and the UAE enacted their first comprehensive Data Protection Laws and both laws become effective by March 2022. On 9 February 2022, Oman enacted its Data Protection Law. The Omani law will become effective by 9 February 2023.

It is expected that the implementing regulations to the three new Data Protection Laws, once issued, will provide further details on the implementation of these laws.

On 23 March 2022 the Saudi Data and Artificial Intelligence Authority known as "SDAIA", the authority in charge of regulating the use and process of data in the Kingdom, decided to postpone the full enforcement of the Saudi Data Protection Law until 17 March 2023 (initially 23 March 2022).



How do the Data Protection Laws compare to the European GDPR?

While these Data Protection Laws contain many aspects that are similar to the GDPR and other data protection laws around the world, there are a number of unique aspects and features:

Saudi Arabia

The Saudi Data Protection Law operates a more stringent approach to data sovereignty than many comparable laws. The law prohibits data controllers from transferring data to an entity outside the Kingdom. The law suggests that certain controllers may be granted exemptions by the SDAIA. Given the ambiguity around this point it is expected that the implementing regulations may provide further basis for lawful transfers and more clarity on such arrangements. In any cases, there are further requirements to ensure that the data transfer or disclosure to a party outside the Kingdom does not impact national security or Saudi interests.

It is worth noting that the breach notification provisions are stricter than many international laws including the GDPR, with requirements to notify the relevant authorities/parties "immediately" rather than within a "specific period."

Future thinking
Key developments impacting the TMT industry globally in 2022

UAE

Data breaches that are likely to result in a risk to the privacy, confidentiality and security of data and to affected data owners must be notified to the UAE Data Office (yet to be established) within a "period" (such period shall be specified under the implementing regulations). Unlike the GDPR, there does not seem to be a materiality threshold or higher bar for notifications to data owners.

In terms of transfer, data may be transferred outside the UAE to states or territories that offer an adequate level of protection but subject to the approval of the UAE Data Office. It is unclear at present (i) at which stage such approval will be required or (ii) what are the process to obtain such approval or (iii) if the UAE Data Office will designate a list of approved countries for data transfers similar to the adequacy decisions made by other international regulators.

Similar to the GDPR, processors are required to act on the instructions of controllers and implement contracts with controllers for the processing of data. The UAE Data Protection Law requires controllers and processors to maintain a special record for personal data.

Oman

While most international data protection laws allow for a range of circumstances where data may be processed without the data owner's consent, the Omani Data Protection Law appears to adopt a different approach of requiring the explicit and documented consent of data owners to any processing of their data. Furthermore, the Omani Data Protection Law goes beyond the UAE and Saudi Data Protection Laws by prohibiting the processing of data related to a child without the guardian's consent.

In conclusion, many of the Saudi, UAE and Omani Data Protection Laws' provisions are only similar to some aspects of the GDPR. However, there are significant differences in many cases, and organisations which will be subject to the these Data Protection Laws should ensure that they have, or will put in place, procedures for processing personal data which comply with the relevant laws and the additional requirements which will be set out in the implementing regulations.

Nasser Ali Khasawneh
Partner & Global Head of TMT Sector
nasseralikhasawneh@
eversheds-sutherland.com

Christine Khoury
Principal Associate
christinekhoury@
eversheds-sutherland.com

New rules on the horizon?:
improving competition in Digital Markets

The growth in the digital economy has resulted in significant benefits for business, consumers and society particularly during the COVID-19 pandemic. It has, however, also created challenges for both competition enforcement and policy. In recent years, competition authorities worldwide have been considering whether their enforcement powers are sufficient to address these new challenges.

At the end of last year, the G7 published a compendium, developed by the G7 and guest competition authorities, to provide an overview of how different authorities are working to promote competition in digital markets. This followed a meeting of G7 competition authorities (the "Authorities"), including the European Commission, the CMA, and competition authorities from the USA, Germany, Canada, Australia, India and South Africa (amongst others), to discuss "long term coordination and cooperation" in this sphere. The compendium indicates that the Authorities have already done a great deal of work in digital markets. This includes considering complex issues such as the role of algorithms, as well as trying to understand new and "next generation" technologies so that harms and challenges can be addressed at the earliest stage.

Key challenges

The compendium summaries the key challenges in digital markets faced by the Authorities:

- there are common features in digital markets which lead to companies gaining market power, often increasing market concentration, raising barriers to entry and/or strengthening durability to the market. These features include: network effects; multi-sided markets; and the role of data
- market concentration and lack of competition in the digital sphere can result in different types of harm for consumers, businesses and society, which often vary from traditional price-related effects. As a result, addressing challenges in the digital market may require new theories of harm and new ways to consider and demonstrate the effects of these harms
- digital markets offer new, complex and multi-sided business models for firms which can include zero price markets. This can, in turn, be difficult to fit into the traditional frameworks, such as market definition. Authorities may need to new tools to investigate and understand anti-competitive behaviour in this sphere, and to consider key factors such as the scale and importance of data, use of algorithms and other complexities
- although there have been attempts by the Authorities to tackle anti-competitive behaviour by powerful digital firms, many investigations and remedies have not sufficiently restored competition. Legal reforms may be required, and/or a new complimentary regulation, to address these challenges effectively
- the global nature of digital firms and the interaction between competition and other key areas such as data protection, consumer and media sustainability has increased the need for regulators and policy makers to cooperate and coordinate, across both jurisdictions and disciplines in relation to digital markets

Key findings

The compendium found that regulatory cooperation in digital markets is hugely important, because competition issues rarely occur in a vacuum. Links exist between data protection, privacy, consumer and competition law which require the Authorities to work alongside both data protection and consumer enforcement authorities. The necessity of this is evident in the fact that the use of data is key for many digital platform business models and access to large data sets can increase a platform's market position, which can be leveraged to collect more data to improve targeting consumers, and develop products and services. This in itself can create barriers to entry and innovation in digital markets.

Several agencies have already considered the tensions which can arise between competition, data protection, privacy and consumer protection. For example:

- the Japanese Competition Authority published guidelines relating to an abuse of a superior bargaining position, aimed at increasing transparency relating to data collection, and transactions between platforms and consumers providing personal information
- Italy's Communication Regulator and the Data Protection Authority published a report in 2020 recommending the use of a framework to address issues raised by big data. They also advocated for the establishment of a coherent and consistent framework covering data collection, enhancing transparency and facilitating data portability
- the CMA and the UK Information Commissioner's Office published a joint statement identifying strong similarities between the aims of competition law and data protection law. They also set out how regulators can collaborate to overcome perceived tensions in these areas

The Authorities are focussing on a number of areas in digital markets including digital advertising, algorithms, marketplaces, app stores and mergers. The Authorities are working to improve their ability to investigate, understand, analyse and remedy anti-competitive behaviour in digital markets, through creating specialist departments and teams, upskilling staff and undertaking in-depth market studies to increase knowledge of digital markets. There was also a shared understanding that modernising reforms are required to existing powers and approaches, and that additional mechanisms, powers and/or safeguards are necessary to strengthen the armour with which the Authorities can tackle key challenges in digital markets.

What does this mean?

The compendium shows that competition in digital markets remains a hot topic for the Authorities. They have all increased their enforcement activity in this area and this trend is set to continue. Moreover, regulatory reforms are on the horizon in certain jurisdictions. In the EU, for example, the European Parliament and the Council of the EU recently reached political agreement on the text of the Digital Markets Act. Once adopted, the Act will introduce a code of conduct for digital platforms that act as "gatekeepers" to prevent them from imposing unfair conditions on businesses and consumers, and aims to ensure the openness of important digital services. The UK Government is also expected to implement a new competition law regime to regulate the most powerful digital firms in the market. Companies active in digital markets should carefully assess compliance with any new rules that may come into play.

Philip James
Partner
philipjames@
eversheds-sutherland.com

Annabel Borg
Legal Director
annabelborg@
eversheds-sutherland.com

Ruth Haynes
Trainee
ruthhaynes@
eversheds-sutherland.com

Switched on to climate care:

mitigating the environmental impact of data centers

Today's global reliance on digital services, such as artificial intelligence, the cloud, and social media platforms, has led to rapid growth in the world of data centers. Whilst this boom has been, and continues to be, great for business, it has resulted in a huge increase in energy consumption and carbon emissions around the world. Data center operators are therefore increasingly coming under pressure to find ways to address the impacts that they are having on the environment, whilst maintaining uninterrupted service for clients.

Reducing the environmental impact

The baseload requirement - one of the most effective ways that operators can address their environmental footprint is to either (i) reduce their baseload, or (ii) find a renewable source for their baseload, i.e. procure "green" power. Reducing baseload is unattractive in the world of booming demand, however two developments in particular can help make it possible for data center operators to source their power renewably, locally and reliably: one is increasing prevalence of baseload corporate PPAs (see below), and the other is the rise in utility-scale batteries and co-located storage, as batteries can help manage intermittency.

Waste heat - Data centers produce large amounts of heat which is often released into the atmosphere and wasted. The heat produced by data centers can however be a reliable and stable source of energy and one that can be utilised to reduce the environmental footprint of data centers and surrounding businesses, at a time when decarbonisation of heat (together with transportation) is becoming a new frontier for decarbonisation. Data center operators can for instance look to export waste heat into a local district heating network. The location of a data center will be crucially important, to overcome difficulties around the transportation of heat, e.g. if it is located close to group of buildings or development which share a district heating network.

Climate change disputes & risk management

Climate disputes and related regulatory action are on the rise globally, with a substantial increase in claims being initiated in recent years. Much of the litigation is aimed at governments and public bodies, often seeking increased climate commitments or the implementation of existing obligations. Increasingly however, companies are coming under scrutiny and are beginning to face claims. This is extending beyond the so called 'carbon majors' to include industrial sectors, particularly energy intensive industries that are harder to decarbonise.

Regulators and lawmakers have a focus on corporate climate disclosures and reporting. Investors, including activist shareholders, customers, employees and the wider public are also paying close attention to company performance and now expect companies to set, and deliver against, ambitious decarbonization targets/net zero commitments. Data center operators are no exception in this respect.

Companies that overstate the green credentials of their business or products, referred to as 'greenwashing' are being publicly named and shamed and in some cases becoming the target of climate activists, regulators or group actions. Much of this action is being initiated in the US, but it is an indication of a growing trend. We have also seen legal action initiated against Santos in Australia by the Australasian Centre for Corporate Responsibility (ACCR), challenging the statements in Santos' annual report that it has a credible pathway to net zero by 2040 and its claims that natural gas is a 'clean' fuel. This is the first court case to specifically challenge the veracity of a company's net zero emissions target. In addition, we saw successful litigation in the Netherlands in 2021, against one of the carbon majors, where the court has held that while the company's actions were lawful, it also owes a duty of care to reduce its GHG emissions (currently being appealed).

In addition to climate disputes, companies and directors are under increasing pressure from shareholders and stakeholders to commit to a business model that meets other key ESG criteria. This can include sustainable commitments, with an appetite among stakeholders for companies to demonstrate social and ethical leadership.

ESG commitments made and delivery against them is therefore a significant board level matter, as a high profile dispute or regulatory enforcement action has the potential to have a significant negative impact on the business, both from a financial and reputational perspective.

Decarbonisation

There are two key routes for organisations to achieve their decarbonisation goals: firstly, to procure "green" power under a corporate power purchase agreement ("PPA"), and secondly, to reduce or offset their remaining carbon emissions.

PPAs are long-term electricity supply contracts which secure the price of green electricity for a specified term, usually by way of fixed price, or price floor/caps. The current energy market is highlighting the potential value of a long term fixed price renewable PPA, with the greenness almost being a "nice to have". PPAs are typically entered into with renewable generators (e.g. wind farm developers) for a the whole or a certain percentage of the generator's output. Baseload PPAs are increasing in popularity – this is where a fixed volume is bought and sold in a block, even if the underlying generating asset is intermittent, with the generator either sizing the block to ensure it can deliver or procuring top up volumes itself to shape the block.

Unless subject to an emissions trading scheme, carbon offsetting is not currently compulsory for the majority of organisations in the UK/EU, but more and more organisations are looking to offset their carbon emissions voluntarily. Carbon offsetting allows organisations to invest in environmental projects locally or around the world to balance our their own emissions, for example, in afforestation projects. Organisations can purchase carbon emission reduction credits certified by voluntary bodies (e.g. Verra or Gold Standard), each of which represents a unit of carbon dioxide absorbed or sequestered, to demonstrate their commitment to decarbonisation. As a purchaser of credits, organisations can commit to anything from simply buying credits on an exchange to underwriting an entirely new (sponsored) carbon project. Given the level and intensity of electricity demand at data centers, offsetting may be an avenue available for data center operators to explore, together with green power procurement, in their efforts to achieve Net Zero for the more hard to decarbonise parts of their business or supply chain.

Ben Brown
Principal Associate
benbrown3@
eversheds-sutherland.com

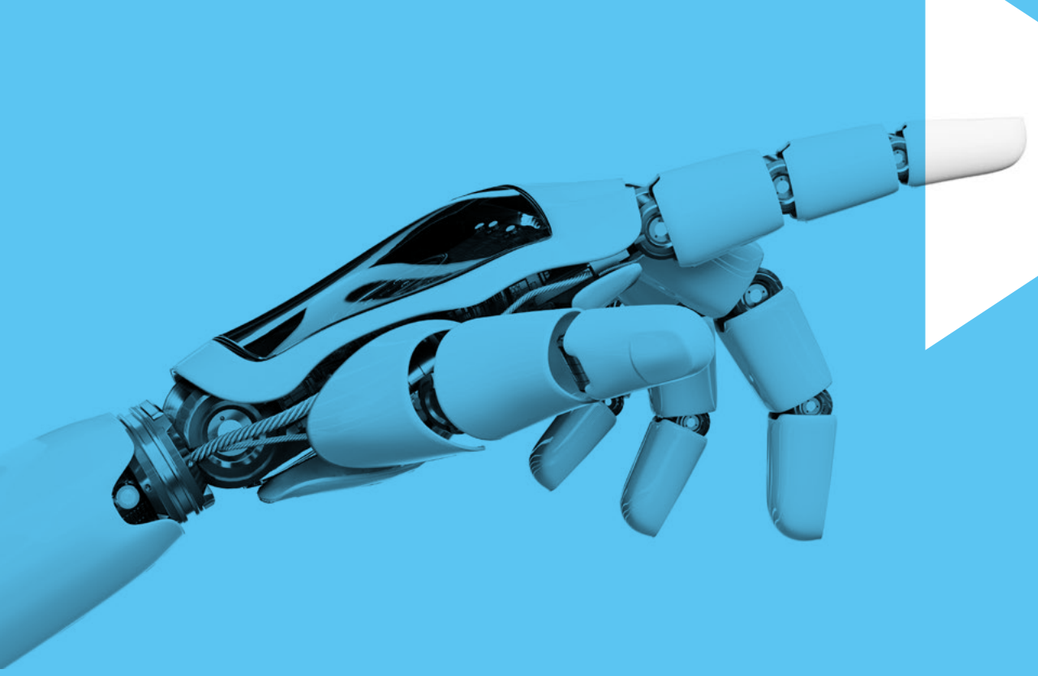
Simon Davies
Principal Associate
simondavies@
eversheds-sutherland.com

Sophie Lowe
Associate
sophielowe@
eversheds-sutherland.com

Future thinking
Key developments impacting the TMT industry globally in 2022

Shaping the future
Navigating the risks and rewards of Digitalization

Global Tech Week



For more information, view our Global Tech Week hub here

Future thinking
Key developments impacting the TMT industry globally in 2022

Between 28 February and 3 March we held the inaugural Global Tech Week which focussed on the opportunities posed by digitalization and the potential legal implications and challenges.

The four-day conference was designed to give attendees the opportunity to join industry leaders and our experienced lawyers in the Financial Services and Technology, Media and Telecoms sectors to explore these issues.

Expanding our footprint in the US

our new office in San Francisco

We are excited to have opened our first office in San Francisco, strengthening our presence in the US TMT market and the Bay Area in particular.

Baird D. Fogel, a highly regarded and experienced transactional attorney, has joined the firm from Morgan, Lewis & Bockius as Partner in Charge for the new San Francisco office. Data privacy Partner Brandi A. Taylor, who is our West Coast Technology Lead and counsels companies in product development, is relocating to San Francisco as well, further bolstering the firm's Bay Area technology practice. Through our new office we will expand the firm's Bay Area corporate and data privacy capabilities, including M&A, contract negotiations, stock sales, advising on product development for gaming and emerging technologies, including blockchain and Web 3.0, AI, and virtual and augmented reality.

"I've always been impressed with Eversheds Sutherland's strength in the Bay Area. That they already work with most of the big tech companies – even without a physical location here – truly speaks volumes to the firm's global reach and outstanding skillsets," said Mr. Fogel. "I'm also thrilled to have the opportunity to launch the new office alongside Brandi Taylor, who has established an exceptional practice advising tech companies on complex data privacy compliance issues. As one of the world's leading international gateway cities, San Francisco will serve as a bridge connecting our colleagues, practices and clients around the world."

The Eversheds Sutherland San Francisco office will benefit from the global support of Eversheds Sutherland international partners, namely, M&A Partner Antony Walsh, Technology Partner and International AI Practice and Technology Sector Head Charlotte Walker-Osborn, both from the UK, and Partner and Global TMT Sector Head Nasser Ali Khasawneh from the firm's Middle East practice, all of whom have significant client relationships in Northern California.

Read the full press release:
Eversheds Sutherland Opens San Francisco Office

Baird D. Fogel
Partner
bairdfogel
@eversheds-sutherland.com

Brandi A. Taylor
Partner
branditaylor
@eversheds-sutherland.com

Future thinking
Key developments impacting the TMT industry globally in 2022

Keeping you up to speed:
regulatory changes within the Telecoms industry in the UK

The Electronic Communications Code ("the Code") regulates rights for network operators and infrastructure providers to install and maintain digital communications infrastructure on public and private land throughout the UK.

The requirement for operators to have the ability to easily roll out and upgrade apparatus and infrastructure to reflect changes in technology was a major factor influencing the enactment of a new version of the Code in 2017, reflecting the Government's commitment and strategic vision to ensure that the country is at the leading edge of the global digital economy. It is set out in Schedule 3A of the Communications Act 2003. The Code's stated objective is the speedy and economical delivery of communications networks in the public interest.

Yet the version of the Code introduced in 2017 has led to more litigation than the previous version of the Code produced in over 30 years on the statute book and disagreements over how the Code applies have persisted. Stakeholders raised concerns with how aspects of the Code were working in practice and whether it was achieving its objective, citing difficulties in the negotiation of requests for rights to install, use and upgrade infrastructure, unresponsive landowners, protracted negotiations and difficulties in resolving issues in a timely manner.

This feedback informed a public consultation in January 2021. The Government set out to explore three main problem areas. These were:

- issues relating to obtaining and using Code agreements
- rights to upgrade and share
- difficulties specifically relating to the renewal of expired agreements

Whilst a significant number of stakeholder submissions referred to the statutory valuation regime under the Code, the government confirmed that it would not revisit the statutory valuation framework as part of the consultation.

The statutory valuation framework which underpins negotiations (set out in paragraph 24 of the Code) therefore remains applicable for the installation/ maintenance of digital communications infrastructure systems.

The introduction of the Product Security and Telecommunications Infrastructure Bill ("Bill") coincided with the publication of the Government's response to its consultation on reforming the Code, which received over 1200 submissions. These new measures proposed under the Bill build on the 2017 reforms, to ensure their original aims are fully realised.

Product Security and Telecommunications Infrastructure Bill

The Bill is currently at "report stage" in the House of Commons. The Bill is due to have a 3rd reading before moving to the House of Lords.

The measures in the Bill aim to support and encourage faster and more collaborative negotiations, and to ensure the procedure and framework for renewing expired agreements is clearer and more consistent. To optimise the use of existing networks, the Bill will enable greater upgrading and sharing of apparatus installed before the 2017 reforms. Finally, new measures will allow operators to secure Code rights more quickly and cheaply through the Courts if a landowner or occupier repeatedly does not respond to requests for these rights.

The reforms include:

- a requirement for operators to consider the use of Alternative Dispute Resolution (such as mediation and arbitration) to resolve disputes regarding agreeing terms. The aim is to avoid costly Court proceedings
- new automatic rights for operators to upgrade and share underground infrastructure such as fibre optic cables, which were installed prior to the Code reforms in 2017 and are not currently covered by the Code. However, there must not be any impact on private land/burden on the site provider
- new rules to allow operators to apply for time-limited access to certain types of land more quickly where a landowner does not respond to repeated requests for permission
- new provisions to speed-up negotiations for renewal agreements. Operators who have installed infrastructure under expired agreements will be able to either renew their expired agreements on similar terms or request new agreements

The current difficulties being experienced by operators under the Code clearly fly in the face of Parliament's desire to facilitate the roll out of world-class digital infrastructure in the UK, including for 5G.

Through these further reforms the Government hope to provide greater legal certainty and improved mechanisms to encourage greater engagement and collaboration. The aim is to facilitate the provision of digital coverage and connectivity, while ensuring rights and powers available to operators strike a proportionate balance between the increasing public need for digital services and the interests of landowners and occupiers.

Damian Hyndman
Partner
damianhyndman
@eversheds-sutherland.com

Jennifer Leah
Senior Associate
jenniferleah
@eversheds-sutherland.com

Future thinking
Key developments impacting the TMT industry globally in 2022

eversheds-sutherland.com

DTUK004128_04/22