Baker McKenzie.

TMT LOOKING AHEAD

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

2020

Foreword

Raffaele Giarda
Chair
Global Technology Media &
Telecoms Industry Group

In the last decade, we have witnessed unprecedented technological progress across the globe with digitalisation impacting virtually every aspect of society. Technology is changing the way we interact with one another, we work, we consume information, we shop, we communicate, we travel and much more. In a similar vein, technology is changing the world of business with companies digitalising their supply chains, implementing data-driven business models and further increasing customer centricity. Personalisation, speed, convenience and security are just some of the benefits brought about by technology that we have come to value.

Lately, we seem to have reached a turning point and attention is shifting away from the benefits technology brings towards risks. Public trust in technology is under constant and increased scrutiny. Fake news, election interference, undue surveillance and algorithmic criteria are amongst the most discussed issues society is facing. They are novel, they are complex, and they are global. And they lie at the intersection of technology and human rights. Nothing less. Technology has the potential to protect fundamental human rights such as freedom of speech, privacy and non-discrimination as well as helping to combat threats from those who use it maliciously.

The TMT sector is key in driving technological progress and also a force for good. And it is naturally the target of increased review coming from various angles, including governments, regulators, legislators, employees, shareholders, customers and the general public.

In this publication, our global TMT team – consisting of over 1500 lawyers in 77 offices, covering all practices of law – explores some of the legal and regulatory trends that will be seen in the sector in 2020, including developments in content governance legislation, data sharing, regulation of facial recognition technology and Artificial Intelligence more generally, public policy, digital tax, antitrust and more.

On a closing remark, we are all going through very challenging times in light of the COVID-19 pandemic which is having such a shocking impact on people, entire ecosystems and business sectors. We are indeed addressing here some of the issues that affect the TMT industry. But, most importantly, we wish everyone reading this publication to stay safe and be well in the year ahead.

BACK TO MAIN PAGE

In this issue...

BACK TO MAIN PAGE

1

DATA AS AN ASSET?

Data may become a critical asset for any business that seeks to compete in our data-driven economy. But monetizing data is easier said than done. It requires businesses to identify the best use cases for their data, to find ways to protect their data as a business asset while increasing its value by sharing it with others, to comply with ever evolving and often inconsistent laws and regulations, and to meet consumer expectations for responsible and transparent handling of their data.

At a glance:

- **Data: Is it good to share?** We are witnessing a flurry of regulations around the world focused on the protection of personal data of individuals. In parallel, there is broad acceptance that data is a very valuable business asset and there is a clear trend towards greater data sharing in the name of competition and innovation. But data sharing can raise tricky legal challenges from data privacy compliance to antitrust. Moreover, given the intense scrutiny on the use of data from policy makers, regulators, the media, the public and employees, companies are increasingly being required to think beyond compliance with the law when it comes to data sharing.
- **Personal data regulation: What is on the horizon?** At the same time as companies, governments and individuals are increasingly recognizing the significance of data for innovation, governance and competition, politicians, data protection authorities and legislatures are ever-more rigidly regulating and restricting the processing of personal data. Taking the example of healthcare, discouraging organizations from collecting, using, retaining and sharing personal information could likely hinder medical progress by slowing down treatments, referrals, research and development.
- **Data in deals: Making sure our due diligence in M&A transactions covers data -** Data is increasingly a core asset in corporate transactions and we expect a further shift away from acquiring traditional assets (like registered IP and brands) towards acquiring novel assets (like data and new technologies). It will be ever more important to reflect this in the due diligence process and throughout the entire acquisition to ensure you get what you pay for and you protect yourself against significant data privacy compliance risks that might result from the target's data practices preceding the deal.

BACK TO MAIN PAGE

Data: Is it good to share?

In recent years, we have seen a rise of laws and regulations around the world focused on the protection of the personal data of individuals. In parallel, we have seen a broad acceptance that data is a very valuable business asset and often derives value from sharing and combining it with other data (as discussed in our report, Data as an Asset), together with a push from industry and regulators to encourage greater data sharing in the name of competition and innovation.

Open Data

One data sharing trend that will continue to move forward apace in 2020 is open data. In recent years, we have seen a wave of initiatives focused on incentivising data sharing or requiring organisations to make data available – often driven by a consumer protection, competition or innovation agenda.

This started with Open Banking. The UK's Open Banking initiative required the UK's 9 leading retail banks to enable customers to access their own data and, with the customer's consent, share it with authorised third parties. The EU regulation, PSD2, introduced in 2018, imposed similar data sharing requirements.

We have since seen a wave of countries around the world adopting their own similar initiatives. Indeed, the concept has extended beyond the financial service sector. For example, later this year, Australia will introduce its much-anticipated Consumer Data Right, which will be rolled out on a sector basis, starting with financial services, but intended to enable data sharing across a range of sectors, including energy and telecoms. Singapore has also launched a Trusted Data Sharing Framework that is designed to encourage data sharing of both personal and business data and is sector-agnostic. France, keeping with its tradition of democratic transparency and of sharing information held by the public authorities, has launched an ambitious policy in 2016 relating to the openness of public data: open data becomes a synonym of open government, relying on taskforces such as "Etalab", which coordinates government action on open data, develops and administers an online portal relating to open data, and supports the re-use of public data. Back to the UK, in 2019 the UK government proposed a Smart Data initiative focused on the energy and telecoms sectors and the UK financial service regulator recently announced extending Open Banking to Open Finance.

Healthcare

Another sector increasingly focused on the benefits of data sharing is healthcare. Access to health data is key to developing data-driven healthcare technologies.

Hospitals and academic institutions around the world are increasingly willing to share health data with the private sector to aid the development of medical technology. In the UK, the National Health Service is a rich source of patient data – it holds millions of electronic medical records on the health of the UK population. If harnessed properly, this data could be used to develop technologies which improve patient care.

Research data is also a key area where sharing is promoted: public funding is directed at research projects on condition that the results are disseminated and shared with the public, as recently reported by the Preliminary Opinion of the European Data Protection Supervisor on data protection and scientific research published at the beginning of this year (see our article looking at this from a medical research perspective here).

However, as highlighted in our recent report, Outside the Comfort Zone: Building Consumer Trust in Digital Healthcare, although data sharing in the healthcare space offers great promise, it can seem a legal minefield. Legal frameworks for accessing and using patient data across the globe are evolving quickly. More obstacles are springing up as the pace of regulation tries to match the pace of innovation.

Undoubtedly, sharing health data may raise some thorny political and ethical issues. Once health data – to a large extent sensitive data – is shared with the private sector, how do you ensure patients feel in control of their health data? How do you address concerns around data security? How should such data be valued? These are just some of the issues that ethics committees, data protection authorities and healthcare regulatory bodies are beginning to grapple with.

BACK TO MAIN PAGE

Data Trusts

For more complex data sharing like the sharing of health data, data trusts may have a part to play. A data trust is defined by the Open Data Institute as "a legal structure that provides independent stewardship of data".

A key role of that independent steward is to ensure data is processed lawfully, addressing the power and information imbalance between data controllers and data subjects, and (hopefully) overcoming the possible mistrust that can be a barrier to data sharing. The involvement of an independent intermediary can facilitate the sharing of data between parties with competing interests.

In the current climate, the potential ability of data trusts to combine increased data sharing with greater trust and transparency protection is increasingly appealing. Although there are not currently many data trusts in operation, we expect to see broader use of these structures in 2020, as awareness grows.

Non-Personal Data

Understandably, personal data tends to get the most attention, but over recent years companies have also been focused on how to get value out of non-personal datasets. Although we have seen some regulatory activity in this area (the EU introduced a regulation on the free flow of non-personal data in 2019), the barriers tend not to be regulatory, but cultural or stem from concerns regarding IP protection, competition law or technical or commercial constraints. During 2020, we expect much of the activity in this area to continue to be the result of voluntary initiatives – whether bilateral, multi-party marketplaces, government initiated or industry led.

Ethics and Trust

In recent years, we have seen increased scrutiny on the responsible use of data which goes beyond privacy law and considers the broader impact on individuals and society. There is increased acceptance that you need to have both a top-down and bottom-up approach. Data ethics should be a board level issue, but also needs to be considered throughout the company's data lifecycle. In 2020, we expect companies to continue formulating data ethics principles and working on how to embed those values into their business, including in policies, procedures and training. As trust in tech continues to be a key theme, increasingly those companies that can demonstrate a commitment to the responsible use of data will be at a competitive advantage.

Magalie Dansac Le Clerk
Partner
Paris
magalie.dansacleclerc@bakermckenzie.com

Sue McLean
Partner
London
sue.mcLean@bakermckenzie.com

Jaspreet Takhar
Associate
London
jaspreet.takhar@bakermckenzie.com

BACK TO MAIN PAGE

Personal data regulation: What is on the horizon?

At the same time as companies, governments and individuals are increasingly recognizing the significance of data for innovation, governance, competition and market power (also see Data: Is it good to share? and Considerations in big data, digital platforms, and antitrust), politicians, data protection authorities and legislatures are ever-more rigidly regulating and restricting the processing of personal data. This contrast is bound to escalate in coming years with data processing regulation:

- restricting selling and other forms of sharing of personal information (as under the 2018 California Consumer Privacy Act – **CCPA**), potentially leading to market power concentration and reduced competition
- challenging advertising technologies and data monetization business models, resulting in less "free" online services (and information technology innovation slowdown, given the comparably slower pace of launching paid services)
- undermining the potential of cloud computing technologies due to international proliferation of restrictions on cross-border data sharing, data residency and record retention requirements
- tightening or abandoning exceptions for "de-identified," "anonymized" or "redacted" data, in light of re-identification threats.

Companies must prepare for increased enforcement activity and penalty sizes beyond the current record of a USD 5 Billion fine in the United States and threats of fines under the General Data Protection Regulation (**GDPR**) up to the greater of EUR 20M or 4% of annual turnover.

Further complicating the compliance challenge is that legislatures in many jurisdictions, particularly in U.S. states, constantly pile on additional privacy laws without repealing or consolidating existing privacy laws, overwhelming businesses and raising compliance costs to prohibitive levels.

These trends in personal data processing regulations bring several serious risks, which are illustrated particularly well in the healthcare sector. Modern medicine is evolving at a tremendous speed. On a daily basis, we learn about new treatments, drugs, medical devices and diagnoses. Both established technology companies and start-ups focus on health-related products and services in competition with traditional healthcare businesses. Telemedicine and electronic health records have the potential to improve the effectiveness of treatments significantly. Progress in the medical field depends above all on data, specifically, health information. Physicians, researchers and developers need health information to help patients by improving diagnoses, customizing treatments and finding new cures.

Yet, law and policymakers are increasingly focused on the fact that health information can also be used to harm individuals. Employers or insurance companies may disfavor individuals with pre-existing health conditions in the context of job offers, promotions as well as coverage and eligibility decisions. Some diseases carry a negative stigma in social circumstances. To reduce the risks of such harms and protect individual dignity, governments around the world regulate the collection, use, and sharing of health information with ever stricter laws.

European countries have generally prohibited the processing of personal data, subject to limited exceptions, which companies have to identify and document or apply for. The GDPR that took effect in 2018 confirms and amplifies a rigid regulatory regime that was first introduced in the German State Hessen in 1970 and demands that organizations minimize the amount of data they collect, use, share and retain. Healthcare and health-tech organizations have struggled to comply with this regime.

The United States, on the other hand, has traditionally relied on sector- and harm-specific laws to protect privacy, including data privacy and security rules under the federal Health Insurance Portability and Accountability Act (**HIPAA**) and numerous state laws including the Confidentiality of Medical Information Act (**CMIA**) in California, which specifically address the collection and use of health information. So long as organizations observe the specific restrictions and prohibitions in sector-specific privacy laws, they may collect, use and share health information. As a default rule in the United States, businesses are generally permitted to process personal information, including health information. Yet, recently, extremely broad and complex privacy laws have been proposed or enacted in some states, including the CCPA, which have a potential to render compliance with data privacy laws impractical for most businesses, including those in the healthcare and health tech sectors.

Meanwhile, the People's Republic of China is encouraging and incentivizing data-driven research and development by Chinese companies, including in the healthcare sector.

BACK TO MAIN PAGE

In Europe and the United States, the political pendulum has swung in the direction of ever more rigid data regulation and privacy laws, at the expense of potential benefits through medical progress. Governments, businesses and other organizations need to collect, use and share more personal health information, to advance the common good. The potential benefits of health data processing outweigh privacy risks, which can be better tackled by harm-specific laws. If discrimination by employers and insurance companies is a concern, then lawmakers and law enforcement agencies need to focus on anti-discrimination rules for employers and insurance companies – not prohibit or restrict the processing of personal data, which does not per se harm anyone.

The notion of only allowing data processing under specific conditions may hinder medical progress by slowing down treatments, referrals, research and development. It may also prevent the use of medical data as a tool for averting dangers for the public good. Data "anonymization" and requirements for specific consent based on overly detailed privacy notices may fail to protect patient privacy effectively and could unnecessarily complicate the processing of health data for medical purposes.

Property rights to personal data offer no solutions. Even if individuals – not companies creating databases – were granted property rights to their own data originally, this would not ultimately benefit individuals. Given that transfer and exclusion rights are at the core of property regimes, data property rights would threaten information freedom and privacy alike: after an individual sells their data, the buyer and new owner could exercise data property rights to enjoin the seller's friends and family from continued use of such personal data. Physicians, researchers and developers would not benefit either. They would have to deal with property rights in addition to privacy and medical confidentiality requirements.

Instead of overregulating data processing or creating new property rights in data, lawmakers should require and incentivize organizations to earn and maintain the trust of patients and other data subjects, and penalize organizations that use data in specifically prohibited ways to harm individuals. Electronic health records, improved notice and consent mechanisms and clear legal frameworks will promote medical progress, reduce risks of human error, lower costs and make data processing and sharing more reliable.

Laws like the GDPR or the CCPA could discourage organizations from collecting, using, retaining and sharing personal information. Physicians, researchers, developers, drug companies, medical device manufacturers and governments urgently need better and more access to personal health information.

Countries find themselves at a crossroads with respect to data privacy legislation. Data privacy law reform should focus on actual privacy harms and remain flexible to allow frequent updates and adjustments as technologies and threats or opportunities evolve. The future of medicine offers a great deal of such opportunities. It depends on trust and healthy data protection. Some degree of data regulation is necessary, but the dose makes the poison. For more details, see here and 26 Mich. Tech. L. Rev. (2020 – forthcoming).

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

Data in deals: Making sure our due diligence in M&A transactions covers data

Getting to grips with the issue of data when looking at an M&A target can feel daunting. However, the importance of data for many businesses, particularly in the tech space, combined with the high degree of public sensitivity around the use or perceived misuse of data and increasing regulatory scrutiny, means that grappling thoughtfully with the topic is a must. Trust in a tech platform or tech enabled business can be quickly and dramatically eroded if issues around data collection, storage or use emerge post-closing.

Data has become a critical asset for any business that seeks to compete in our data-driven economy. It is therefore no surprise that it is a key element of any M&A transaction. In any deal, buyer and seller will exchange a variety of data, including personal data, i.e., any information about an identified or identifiable individual. This triggers a number of compliance risks and issues that need to be taken into consideration, starting with the due diligence process.

Sensible and targeted data due diligence has the double benefit of:

- making sure you are acquiring a business with a data set you can use as intended and you are paying the right price for the business; and
- helping you get ahead of any data related issues that may be lurking in the target and which might otherwise blindside you post-closing with severe impacts on valuation and/or reputation.

What are the problems to look out for?

- Data that was unlawfully collected – i.e., without adequate legal ground. This might include data that was collected without valid consent where such consent was required for the particular use being made, or proposed to be made, or data that was collected without data subjects being properly informed in accordance with applicable data protection laws. Imagine a scenario where a prospect database has been built without appropriate legal basis and/or without informing the data subjects. The buyer will not be able to make any lawful use of the data in that database to contact prospects.
- Data that was lawfully collected for a specific purpose but cannot be lawfully transferred to buyer due to data protection restrictions. Imagine a scenario where data subjects consented to the processing of their data to receive marketing material from the target on specific products in a specific territory, but not to the sharing of their data with a potential buyer in another territory.
- Technology that cannot work in a data-compliant manner. Some technology platforms are simply too good to be true. Make sure you understand how the technology does what it does. Can it collect and use data in a way that is compliant with the law? Depending on applicable data protection laws, certain technologies may be regarded as too intrusive and disproportionate and, therefore, illegal. Think, for example, of very intrusive monitoring or surveillance technologies. Also see our chapter on facial recognition technologies.
- Absence of a data protection compliance framework or information governance within the target. This might evidence itself in the absence of appropriate privacy policies and notices, data flows chart, security controls, or privacy impact assessments.
- Targets with insufficient data security leading to an unacceptable risk of a data breach either through inadvertent error or third party hacking. Imagine the case of a data breach that occurred pre-closing, but that is detected post-closing and triggers an obligation to notify competent regulators and data subjects which then results in an investigation by the regulator, potentially significant fines and possible reputational risk. Regulators are increasingly willing to hold the acquirer accountable in these scenarios.

BACK TO MAIN PAGE

Scoping out the data due diligence

In scoping out a data due diligence exercise, we recommend asking these threshold questions:

- Is the target collecting/using personal data and is there a need for such personal data to be transferred to the buyer? Is it sufficient to share/transfer only aggregated or anonymized data (to facilitate compliance with data protection requirements)?
- Does the buyer want to re-use the data after the deal? Test whether the existing dataset is vital to the value of the deal. Sometimes the real value lies in the platform that was used to collect the data rather than in the data itself. This can be important to understand because if there are doubts about the legitimacy of the dataset, it may be more cost-effective to expunge the dataset and start fresh rather than incurring time and expense through a detailed analysis and remedial steps.
- How does the buyer want to use the data after the deal? Understanding this enables you to assess whether the data was collected in a manner that supports the type of use intended post-closing.

If a detailed review of data is required, this consists primarily in:

- Ensuring that the transfer of data to the buyer is justified on a valid legal ground (this could be the data subject's consent or, possibly, the legitimate interests of the target and/or the buyer, provided that such interests are not overridden by the data subjects' interests or fundamental rights and freedoms).
- Checking whether data subjects were notified that their data may transfer to a subsequent purchaser of the business (i.e., check the privacy terms provided at the point of data capture). If target's privacy terms permit this as a matter of course, that will make things easier. If the terms vary, it will require a more bespoke analysis per deal (or if that is unpalatable – excluding data). Bear in mind that targets are often start-ups who might not have prioritised data privacy compliance.
- Deciding how to notify data subjects if they had not been notified yet. In this situation, the target would need to inform them and likely offer them a choice regarding the transfer of the data to buyer. The safest method would be to obtain new consent for the transfer based on an 'opt-in' basis although, depending on applicable data protection laws, an 'opt-out' approach arguably could be relied on (albeit more risky).
- Understanding the flow of data through target's technology platform. Does the technology do what it promises, and can it do it in a compliant manner?
- Assessing general compliance with data protection principles, in particular accountability. Is the processing limited to what is necessary for the contemplated purpose (data minimization)? Does the technology/data use take into account data protection by design and by default principles? Is the data processing reflected in data maps and records of processing activities?
- Assessing data security measures. Buyer needs to carry out a proper due diligence of target's information security program. This includes checking security controls, documentation on physical and technical security measures, disaster recovery plan, procedure to deal with security incidents and data breaches and to report them to regulators where required. Bear in mind that certain regulators will not hesitate to hold the buyer liable, also for data breaches that occurred prior to the M&A transaction, if it appears that the buyer did not carry out a proper due diligence and failed to put in place the necessary remediation measures. Detecting data breaches during a transactional due diligence on the other hand, will allow the buyer to assess whether to go ahead with the transaction, and if so, significantly reduce the purchase price and allocate risk associated with the breach.

In today's digital world, data is frequently a core asset in a corporate transaction and we expect a further shift away from acquiring traditional assets like registered IP and brands towards acquiring novel assets like data and new technologies. It will be ever more important to reflect this in the due diligence process and throughout the acquisition to ensure you get what you pay for and you protect yourself against significant data privacy compliance risks that might result from the target's data practices preceding the deal. In 2020, we expect both commercial interests and increasing regulatory scrutiny to drive buyers to focus on data assets and related risks with the same rigor with which they analyze other business risks.

Michelle Blunt
Partner
London
michelle.blunt@bakermckenzie.com

Elisabeth Dehareng
Partner
Brussels
elisabeth.dehareng@bakermckenzie.com

2

NEW TECHNOLOGY: ARTIFICIAL INTELLIGENCE, 5G, TRUST AND BEYOND

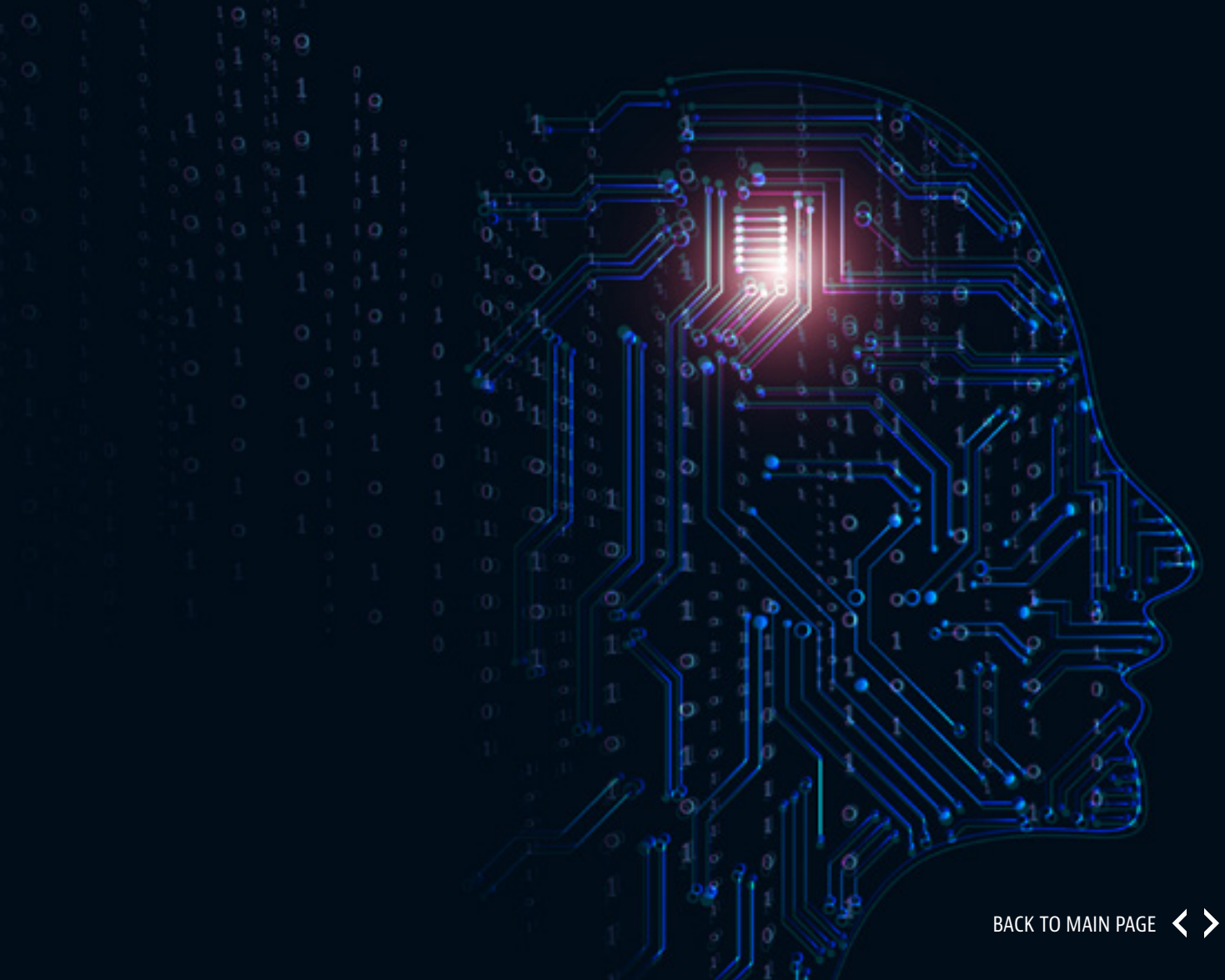
Advances in AI (and the machine learning technology underpinning it) bring into sharper focus the need for the right balance between regulation and innovation. Whilst AI strategies and principles are now in place in many countries, debate is shifting from high-level principles to more detailed regulation. But progress is slow due to the complexity of the task at hand. Collaboration between various stakeholders will be key in the year ahead not only to draft regulation that will adequately govern various known and unknown future use cases, but also to build further trust in new technologies increasingly perceived as potentially impactful on society and fundamental human rights.

At a glance:

- **AI regulation around the world -** If the past few years are any indicator, in 2020 we will see a further strong surge of activity on the AI policy and regulatory front. In 2019, we noted significant evolution of the global AI policy landscape as well as an uptick in regional and national policy-making with a number of countries across regions now having issued national AI strategies and/or sets of governance principles. In 2020, we expect more concrete regulatory proposals (in addition to AI strategies and governance principles) and these will likely greatly differ in approach. It will require multiple stakeholders to collaborate to ensure such regulation does not stifle innovation, effectively protects society against unwanted consequences, and adequately regulates a variety of future use cases across sectors.
- **Governing facial recognition technology -** This technology is receiving much attention by the media, governments, regulators and the general public as a result of new uses of the technology multiplying with sometimes limited oversight in various jurisdictions. While there is no shortage of socially beneficial use cases for this technology, it is also seen as posing certain possible risks to human rights and civil liberties which currently fuel a heated debate as to whether this technology should be permitted at all and, if so, how it should be governed. Interestingly, different regions are at different stages of the debate and social norms seem to heavily influence the direction of travel across continents.
- **Trust through tech leadership: Devising a proactive approach towards regulation -** Following a period of unprecedented acceleration of technological progress, enthusiasm for new technology is transforming into less euphoric sentiments with some questioning whether the benefits of modern technology still outweigh potential risks and whether maybe the impact of technology on society is more significant than anticipated. For 2020, we anticipate a vivid debate on the benefits and exposures of technology with four areas taking center-stage: (1) More regulation for the tech sector, (2) Technology and human rights, (3) Responsible use of data, and (4) Focus on sustainability, impact and purpose.

BACK TO MAIN PAGE

- **Coronavirus: Impact on the TMT sector and supply chain considerations -** The impact of the COVID-19 coronavirus on the TMT sector is multi-faceted. The supply chain is dealing with raw material, component and labour shortages leading to substantial business and operational disruptions. Many businesses see a sharp decline in demand for their products or services. On the flipside, parts of the TMT sector, such as telecommunication services, drones or technology enabling remote working, are core to enabling parts of the economy to still effectively function despite the impact of the coronavirus. The key is being nimble and ready to adapt. Immediate actions companies may wish to take include reviewing commercial terms with customers, suppliers and logistics providers (particularly force majeure and hardship provisions), understanding their health and safety obligations towards employees, and prioritizing supply chain re-organization.
- **Autonomous vehicles: A road map in 2020 -** With trials of autonomous vehicles on many public roads well advanced in several countries but with limited commercial deployments, governments and regulators worldwide are stepping up their law-making to help realize the benefits this new technology can bring to society. Detailed strategic frameworks setting out the shape of the necessary new laws are evolving, including those on type approvals and road safety. Autonomous vehicles, though, still have a number of years before large scale deployment will occur and important challenges to overcome in the interim – particularly gaining public trust and acceptance.
- **Mobile services for the connected era: Boosting 5G deployment in the EU and China -** With its ubiquitous, ultra-high bandwidth and low latency and ability to connect to a much wider range of connected devices, 5G promises to bring significant innovations. No wonder countries, including the EU and China, are racing to facilitate its roll out. In combination with technologies such as AI, IoT and M2M, 5G facilitates advances including industrial-class robots in homes, self-driving cars, smart cities and sophisticated telemedical devices. In the EU, the new European Electronic Communications Code (EECC) brings a number of significant legal changes aimed at meaningfully boosting deployment of 5G technology. Meanwhile, China has leveraged on its existing regulatory framework to allocate 5G frequencies to four carriers and encourages local provincial and municipal governments to release their own polices to foster development and promotion of 5G.
- **Protectionism: Foreign investment, trade wars and import tariffs -** Global trade wars (particularly between the US and China) continue to pose a challenge for TMT companies despite recent progress. Protectionist policies, including tighter foreign investment restrictions, limitations on technology transfers and the direction of travel on import tariffs are all key trends to watch in 2020.



BACK TO MAIN PAGE

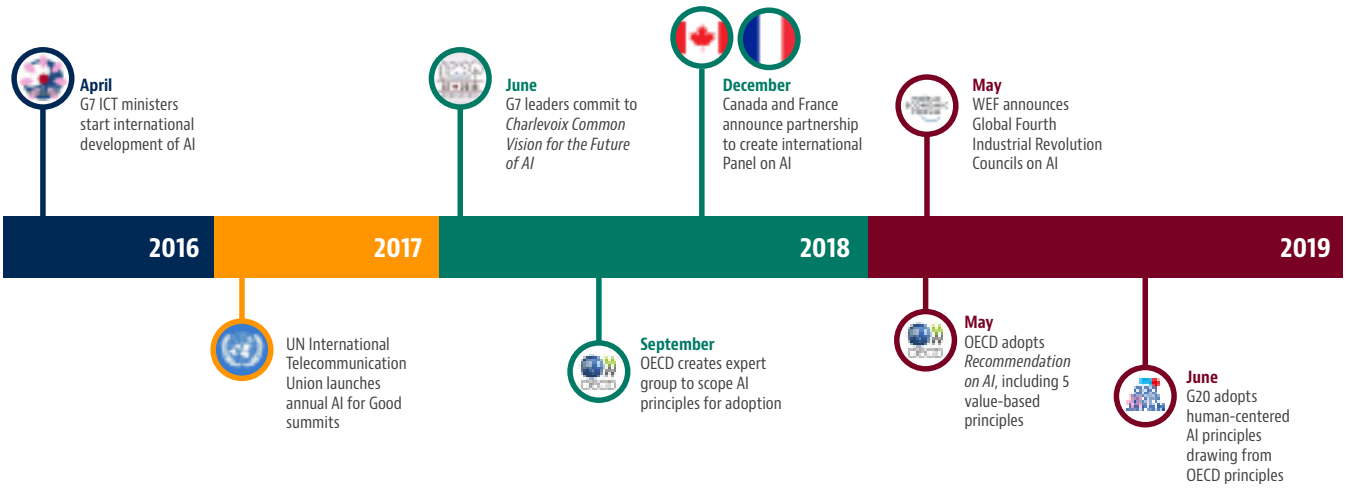
AI regulation around the world

If the past few years are any indicator, in 2020 we will see a further strong surge of activity on the Artificial Intelligence (AI) policy and regulatory front. In 2019, we saw significant evolution of the global AI policy landscape as in May 2019 more than 40 member countries signed on to the Organization for Economic Co-operation and Development's AI principles, the first inter-governmental standard on AI. Then, in June 2019, the G20 adopted human-centered AI principles that draw from the OECD principles. We also saw an uptick in regional and national policy-making, with a number of countries across the Americas, Asia-Pacific, Europe, and other parts of the world now having issued national AI strategies and/or sets of governance principles. Countries with some form of national AI strategy now include Australia, Canada, China, France, Germany, India, Japan, Russia, Singapore, South Korea, Sweden, United Arab Emirates, the United States, and the United Kingdom. Additionally, there has been a proliferation of AI principles and other policy guidelines issued by various non-governmental players, including multi-stakeholder organizations, industry and technical standards bodies, academic institutions, and civil society groups, as well as leading technology companies.

AI-specific laws and proposed legislation

At this stage, the United States, while in some respects lagging behind on the broader policy front, remains ahead of most other jurisdictions when it comes to AI-specific laws and proposed legislation. In particular, 2019 brought forth a number of high profile Federal draft bills directly aimed at regulating AI technologies, as well as new laws and legislative proposals at the State and local government levels. One notable example is the Federal Algorithmic Accountability Act (S. 1108, H.R. 2231), introduced in April 2019, which would require companies to conduct "impact assessments" of automated decision systems for accuracy, fairness, bias, discrimination, privacy, and security. While at the time of writing the Democrat-sponsored bill's future is uncertain, it is a significant regulatory milestone in that it is the first serious Congressional attempt at placing limits on the use of AI systems generally, rather than on specific applications (such as autonomous vehicles). Key 2019 developments at the US State level included California's Bolstering Online Transparency (B.O.T.) Act (SB-1001), which regulates against deceptive uses of "bots" in certain commercial and electoral contexts.

Evolving global AI policy landscape

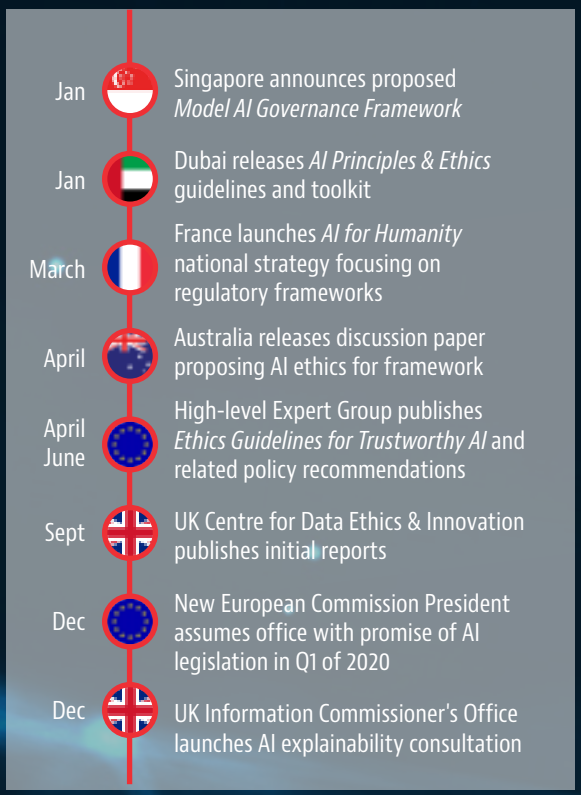


BACK TO MAIN PAGE

Other AI policy activity and developments

Outside the US, many players are following the increasing AI policy activity in Europe. European Commission President Ursula von der Leyen has promised AI-focused legislation during the first quarter of 2020, contemplating a General Data Protection Regulation-style "coordinated European approach on the human and ethical implications" of AI technologies, aimed at "balancing the flow and wide use of data" against "high privacy, security, safety and ethical standards." Any such legislation is expected to draw on the work of the Commission's independent High-Level Expert Group on AI, including its Ethics Guidelines for Trustworthy AI and related policy recommendations issued in 2019. These guidelines propose various requirements for AI systems based on core principles of: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination, and fairness; societal and environmental well-being; and accountability.

The United Kingdom is another jurisdiction of note, with various government and government-sponsored bodies advising on future regulation, including the House of Lords Select Committee, the Information Commissioner's Office (ICO), and the new Centre for Data Ethics and Innovation (CDEI). Beyond Europe, other 2019 rest of world policy highlights included Singapore's proposed Model AI Governance Framework and the Australian Government's AI Ethics Framework and Principles.



A complex and rapidly evolving regulatory environment

With a number of our clients engaged in ground-breaking AI research and leading advances in the field, and many others increasingly looking at leveraging machine intelligence in their businesses, we are closely following these and other AI policy and legal developments. We are also looking towards a machine learning-enabled future and already bake AI technologies into a number of services we deliver – giving us an appreciation of some of the challenges companies face in what is an already quite complex and rapidly evolving AI regulatory environment. One way we are tracking new law and policy is by analyzing and mapping different global, regional and national approaches to common regulatory themes, such as accountability, fairness, human oversight, safety/security, privacy, and transparency. We are also analyzing and helping clients understand how existing legal frameworks apply to AI products and services, one public-facing example being our multi-jurisdictional survey for the World Economic Forum's Generation AI project.

With the coming year set to be another active one for AI regulation and the field more broadly, we are committed to providing further meaningful insights in this space. In 2020, we expect more concrete regulatory proposals (in addition to AI strategies and governance principles) which will greatly differ in approach. This will require collaboration from stakeholders to ensure that new and existing laws do not stifle innovation, effectively protect society against unwanted consequences, and adequately regulate a variety of future use cases across sectors.

Key AI regulatory themes

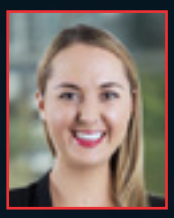
Global, regional and national

Overall focus level

More — Less

- Global
- Americas
- APAC
- EMEA

Raffaele Giarda
Partner
Rome
raffaele.giarda@bakermckenzie.com



Danielle Benecke
Associate
Palo Alto
danielle.benecke@bakermckenzie.com

BACK TO MAIN PAGE

Governing facial recognition technology

Facial recognition technology (FRT) is receiving increased attention by the media, governments, regulators and the general public as a result of new uses of the technology multiplying with sometimes limited oversight in various jurisdictions. While there are numerous socially beneficial use cases for this technology, such as enhanced security and convenient identification, it is also seen as posing certain possible risks to human rights and civil liberties, currently fueling a heated debate as to how to impose responsible limits on its use.

Like much of the other technologies underlying AI, different regions are at different stages of the debate and social norms seem to heavily influence the direction of travel across continents. In the following, we explore how FRT is being used, some of the associated tensions, and the emerging regulatory trends.

The technology and its use cases

FRT has numerous use cases that span both the public and private sectors. In the public sector, FRT is increasingly being used by law enforcement agencies to more effectively combat terrorism and identify potential criminals. Police are building comprehensive databases of facial and other biometric data against which suspects can be matched. Beyond spotting faces in a crowd, FRT is also used for efficiently identifying perpetrators of identity fraud, and is being considered for helping find missing persons, like children or victims of human trafficking, as well as for boarding pass screening.

FRT's civilian use cases are manifold and span all industries. To list a few, FRT can help identify rare genetic disorders, improve accessibility and communication for the blind, track attendance at school or work, control access to secure areas, improve targeted in-store advertising, validate identity at ATMs, or unlock your smartphone. The technology's versatility has led to an exponential growth in its adoption across many industries and use cases. Some use cases are directed at increasing convenience, whereas others are directly socially beneficial.

BACK TO MAIN PAGE

So, what's the problem?

As the use of this technology by the public and private sectors increases, concerns grow exponentially around the possible ethical profiles, and various stakeholders question whether it should be allowed at all in a democratic society or else allowed with certain safeguards in place. While many argue that FRT greatly improves public safety and assists in the fight against organized crime and terrorism, opponents highlight significant risk, including:

- **FRT's potential to enable indiscriminate and largely invisible mass surveillance.** Widespread use of FRT in public spaces for law enforcement purposes clearly may have an impact on privacy. Similarly, commercial applications of FRT enable corporate players to collect large amounts of sensitive data with individuals having limited control over how such data is used.
- **The inherent risk of inaccuracy and bias.** Studies have shown that FRT can greatly increase racial and gender bias if the AI is predominantly trained on images of people with certain characteristics, leaving others more vulnerable to incorrect identification.
- **Other possible threats to human rights and civil liberties including the freedom of expression and the freedom of assembly and association.** Using FRT in public spaces may prevent people from exercising their freedom of assembly and their freedom of speech. Others have also identified privacy and cybersecurity threats, such as corporate misuse of facial data or targeted hacking into government or corporate databases.

Governing the technology

So, how are governments, regulators, and legislators responding? There seems to be a consensus across stakeholders, including many government officials, technology companies, and civil societies that some form of governance is needed to ensure responsible use of FRT and protection of individual rights and fundamental freedoms. But there is no consensus in sight on what constitutes an adequate governance model that strikes a proper balance among the different factors.

The US perspective

The US recently saw a surge in laws and legislative proposals directed to FRT. There are city ordinances, such as those passed by San Francisco and Oakland in California, and Somerville, Massachusetts, in the summer of 2019, generally banning the use of FRT by city government agencies.

At the federal level, in March 2019, Congress introduced the Commercial Facial Recognition Privacy Act (S. 847) in an attempt to strengthen consumer protections and increase transparency. It would generally prohibit covered entities from using FRT "to collect facial recognition data" of end users without providing notice and obtaining their consent, where "covered entities" are broadly defined to include any non-governmental entity that "collects, stores, or processes facial recognition data." It would also prohibit the use of FRT to discriminate against consumers, as well as the repurposing of facial data or sharing such data with third parties without obtaining further consent from the end users.

Other federal bills (all introduced in July 2019) include H.R. 3875 to "prohibit Federal funding from being used for the purchase or use of" FRT and the Facial, Analysis, Comparison, and Evaluation (FACE) Protection Act (H.R. 4021) directed to prohibiting federal agencies from applying FRT to any government-issued photo ID without first obtaining a federal court order. Congress also introduced the No Biometric Barriers to Housing Act (H.R. 4008) in order to "prohibit the use of biometric recognition technology in certain federally assisted dwelling units."

State governments are undergoing similar trends. California introduced A.B. 1215 in February 2019, which would prohibit law enforcement agencies from using any "biometric surveillance system," including FRT, with an officer camera. It also introduced A.B. 1281, which would require California businesses that use FRT to disclose such usage on a physical sign that is "clear and conspicuous at the entrance of every location."

In Massachusetts, An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems (S.B. 1385) was introduced in January 2019 to establish a moratorium on the use of FRT by law enforcement. In New York, S.B. 5687 and A.B. 7790 were introduced in May 2019 to propose a temporary stop on the use of FRT in public schools, and in Washington, S.B. 5528 and H.B. 1654 were introduced in January 2019, concerning the procurement and use of FRT by government entities.

The above laws and bills share similarities with, and would supplement, existing privacy laws, particularly for biometric privacy laws. Illinois' Biometric Information Privacy Act (BIPA) and Texas' law on the Capture or Use of Biometric Identifier have actually been around since the late 2000s, defining "biometric identifier" to include a scan or record of face geometry. BIPA, for example, requires (i) informing a data subject on which biometric identifier is being captured, and about the purpose and length of the required use of the identifier, as well as (ii) obtaining written consent from each data subject. It contains statutory penalties for violations, which have served as the basis for a number of class action lawsuits recently.

Washington's bill on Biometric Identifiers was enacted in July 2017, and California Consumer Privacy Act was passed in June 2018 (effective in January 2020). Other bills were recently introduced in Massachusetts, Delaware, and Florida.

The increasing legislative trends on governing FRT and biometric privacy are viewed by many as government reflections of the public's increasing concerns.

What is going on in Asia Pacific?

With limited exceptions (see Australia below), there have not been laws introduced in the APAC region dedicated to regulating FRT. Use of personal data collected through deployment of FRT typically remains governed by data privacy laws, and some authorities have issued guidance that addresses it. For example, in Japan, the Ministry of Economy, Trade and Industry issued guidance on the use of cameras by businesses that track and perform analytics on customer activity.

We are starting to see an expansion in the use of FRT against this regulatory backdrop. While there has been private sector adoption, the primary focus of discussion has mainly been on public sector use of FRT. One common example of public sector use in the region is the deployment of FRT to speed up immigration clearance for travelers (e.g., in Australia and Singapore).

In India, there have reportedly been plans to expand on the existing national biometric identity database (Aadhaar) that presently collects facial photographs, fingerprints and iris scans. This may include enhancing police investigations through identification of criminals and missing persons and a proposed Automated Facial Recognition System (AFRS) that will include the ability to match facial images from CCTV feeds.

In an example of expansion towards private sector use, there are plans in Singapore to expand the use of its existing National Digital Identity database to permit private enterprises – such as hotels, banks and healthcare institutions – to use FRT to verify identities against the database.

In China, cameras and sensors with facial recognition technology have been rolled out to identify pedestrians and improve public security. China continues to be an important player in the region on this topic. A national working group was established in November 2019 to develop a Chinese national standard for facial recognition. On the international front, Chinese companies have reportedly been involved in shaping international standards on facial recognition through the International Telecommunication Union (ITU).

In Australia, biometric information used for the purpose of automated biometric verification or biometric identification is categorised as "sensitive information" under the Privacy Act 1988 (Cth). Subject to certain exceptions (e.g, if authorised under an Australian law), sensitive information may only be collected with the data-subject's consent and if reasonably necessary for the regulated organisation's functions or activities. There were recent moves in Australia to enact new federal laws that would have authorised expanded use of FRT. However, it seems the Australian Parliament is not yet prepared to accept such broad application of FRT (at least not without sufficient safeguards in place). In October 2019, the Parliamentary Joint Committee on Intelligence and Security recommended a re-draft of a bill which sought to facilitate the sharing of identification information, including facial images, for law enforcement and national security purposes. Recommendations included the need for the regime to be built around privacy, transparency and subject to robust safeguards and sufficient Parliamentary oversight.

Turning to Europe

In Europe, for the time being, data privacy laws - in particular the GDPR - govern the use of facial recognition technology. But the debate around whether to allow this technology, and if so, how to govern it, gained traction towards the end of 2019. In its White Paper on AI, published on 19 February 2020, the European Commission pushes for a clear European regulatory framework for AI, which would cover FRT as a high-risk AI application. As a result, if permitted, the use of FRT in public spaces would be subject to those mandatory legal requirements any future European AI regulatory framework would introduce. Examples of such requirements would include human oversight, adequate training data, record keeping requirements, transparency, robustness and accuracy. However, the European Commission takes the view that it is premature to propose specific rules at this stage and instead has recently foreshadowed a broad European debate on, firstly, the specific circumstances, if any, which might justify the technology's use in public spaces, and, secondly, common safeguards.

In the meantime, national data protection authorities (DPAs) have weighed in on the debate. France's CNIL in November 2019 issued a discussion paper on the technical, legal and ethical aspects of the technology. It calls for a proactive forward-looking debate, for political choices to be made to determine in which cases facial recognition is necessary in a democratic society, and the need to highlight the technological, ethical and societal risks associated with this technology.

The UK's ICO, which has made FRT a priority, has issued an opinion calling for statutory binding guidelines on the use of live facial recognition technology by law enforcement agencies. It is also investigating private sector use of the technology. However, in January 2020, London's Metropolitan police started using live facial recognition in the capital to search for people suspected of serious crimes. By way of contrast, the German government recently paused the technology's rollout for police use when it unexpectedly deleted its authorisation from a legislative package on the reform of police powers. This came in response to a warning by the federal data protection commissioner against FRT and is intended to enable further debate to establish public trust and acceptance in the technology before using it in public spaces.

In August 2019, Sweden's DPA issued a fine to a school that used facial recognition technology in a trial to monitor its students' attendance. At the same time, the Swedish DPA has given the Swedish police the green light to use facial recognition technology to help identify criminal suspects (e.g., comparing facial images from closed-circuit TV footage to biometric databases of known criminals).

BACK TO MAIN PAGE

Outlook

In the year ahead, it will be interesting to see if divergences across regions persist or if Europe and Asia Pacific will maybe follow the US approach and introduce more technology-specific regulation.

Adam Aft
Partner
Chicago
adam.aft@bakermckenzie.com

Anne Petterd
Partner
Sydney
anne.petterd@bakermckenzie.com

Alex Toh
Senior Associate
Singapore
alex.toh@bakermckenzie.com

Yoon Chae
Associate
Dallas
yoon.chae@bakermckenzie.com

Anna Von Dietze
Director of Knowledge, Global Industry Groups
Dusseldorf
anna.vondietze@bakermckenzie.com

Trust through tech leadership: Devising a proactive approach towards regulation

Technology has been a central element of society for centuries and brought positive change in various ways, such as humans travelling faster and further, machines taking over laborsome and dangerous tasks from human workers, improved medical diagnosis and treatment, new means of communication and connecting, and many more. On the other hand, technological progress has at times been associated to new risks for humans, the environment, and society in general. Think about cars hitting the roads for the first time in a world where people travelled on foot or by carriage only, heavy machinery being deployed in factories in the 18th century, or the first application of radiation technology for medical diagnosis.

Despite this period of unprecedented acceleration of technological progress in the last decade with no end in sight, enthusiasm for new technology for some has transformed into less euphoric sentiments that question whether the benefits of modern technology still outweigh risks. In part, this possible change in sentiment may be attributable to fear of the unknown. We are in a period of transitioning from long established paradigms to new models and the pace of change has been significant. Some of these new models are fundamentally different to what we are used to. But innovation and technological progress are here to stay. In the next few years, it will be key to devise approaches to assuage concerns about technological change. For the industry, this means continuing to take a proactive role in working with governments, policy makers, regulators, legislators, human rights experts and others in devising appropriate regulatory responses that continue to drive progress and maintain public trust. For 2020, we anticipate a vivid debate followed by action focused on the following areas.

BACK TO MAIN PAGE

Regulation for the tech sector

Regulators throughout the world have taken a proactive approach towards regulating the tech sector and already have many tools at their disposal to address public concerns. Additional regulation of the tech sector should therefore be carefully balanced so as not to hinder innovation and progress. We expect such regulation across legal disciplines from content governance, to tax and corporate governance. Balanced regulation devised with input from industry stakeholders can promote accountability and create legal certainty. Many jurisdictions are in the process of experimenting with new regulations governing technology. Proposals on the table vary greatly. Across the globe, regulators and governments are grappling with the task of creating additional rules that address public and stakeholder concerns without stifling innovation. Given they are tackling very similar issues, we are increasingly seeing regulators and governments in different parts of the world looking to collaborate, share experiences and seek guidance from each other. For tech companies this means that key developments in pioneer jurisdictions will provide a good sense of the general direction of travel. In addition, there is hope that this could lead to more consistent rules across jurisdictions (although we are a long way away from a harmonised regulatory framework).

Technology and human rights

Innovation and technology can have a significant and positive impact on the economy and overall standards of living. Nonetheless, artificial intelligence, facial recognition technology and automation have been cited as raising potential concerns with respect to issues of privacy, freedom of speech, and bias. In the years to come, the tech sector will be expected to help identify and manage these concerns, as well as develop and deploy technologies with appropriate safeguards. Some pioneers are already appointing chief trust or chief ethics officers or advisory boards to oversee efforts aimed at ensuring the responsible use and development of new technology.

Responsible use of data

Responsible use of data has emerged as a key theme and risk over the last couple of years and one that businesses are focused on. With tighter data privacy and security regulation developing across the world, regulators stepping up enforcement activity, security incidents damaging corporate reputation, and individuals expecting corporations to handle their data transparently and responsibly, it is of the essence that corporations continue to embrace data privacy as a core value and embed it into corporate culture and process.

At the same time, we are trending towards more data sharing and open data economies (see our chapter on "Data: Is it good to share?"). Europe, which has been focused on data privacy for the last few years with the introduction of enhanced rules embodied in the GDPR, has recently released a "European Strategy for Data" which could mark a turning point in how the EU approaches data more generally. The strategy aims to create a common European Data Space unlocking the value of unused personal and non-personal data by facilitating voluntary data sharing and giving the public and private sectors broad access to such data. The European Commission ambitiously foreshadows an enabling legislative framework for the governance of common European data spaces by Q4 2020. What will qualify as responsible use of data in a world in which business-to-business and business-to-government data sharing is encouraged may well be different compared to what qualifies today as responsible data use. For business, it will be important to find the right balance between protecting personal data and extracting value out of it.

Focus on sustainability, impact and purpose

Last year's Business Roundtable Statement on the Purpose of a Corporation signed by 181 US chief executives has marked a shift in corporate priorities towards not only shareholder primacy, but also employees, consumers, suppliers, local communities and the environment. Since then, we have seen other developments in this direction, including fund managers' pledge to put sustainability at the core of their investment decisions and to assess environmental, social and governance with the same rigor with which they analyse traditional risk. We expect this trend to accelerate in 2020. For the tech sector, it will be crucial to anticipate and be transparent about the ethical impact and social consequences of new technology. While this is a complex task, it also offers an opportunity to prove that technology has the potential to solve some of the most acute global challenges, support democratic processes and human rights, and bring about a positive transformation with enormous potential for people around the world. Tech companies are well suited to accelerate progress on many global issues: they are masters of solving big problems, they are not daunted by scale or complexity, they have a desire to innovate and drive change, and they are willing to experiment (and willing to risk on the way to success).

Outlook

The regulatory framework for new technologies is one that will continue to evolve and receive scrutiny. It will therefore be imperative for the tech sector to continue to embrace and progress the above themes and help technology play an even bigger role. While these frameworks may take time to develop, those tech companies that take a leadership role in addressing these concerns will be at a competitive advantage.

Sue McLean
Partner
London
sue.mcLean@bakermckenzie.com

Anna Von Dietze
Director of Knowledge, Global Industry Groups
Dusseldorf
anna.vondietze@bakermckenzie.com

Coronavirus: Impact on the TMT sector and supply chain considerations

Already beleaguered for over a year by the impacts of the US-China trade war, tech companies now face further disruption caused by the COVID-19 coronavirus outbreak.

For Baker McKenzie key resources on COVID-19 please visit our Coronavirus Resource Center.

The impact of coronavirus on people around the world is huge and shocking. The effects on the TMT sector are multi-faceted. Disruptions to factory workforces due to the coronavirus have already been identified. For some technology product companies this has meant they are not receiving inputs needed to complete their technology products. An immediate challenge these product companies face is whether the component can be quickly sourced elsewhere from a jurisdiction not subject to the same workforce limitations. This might not be easily done. Many technology product companies impacted by the US-China trade war were already facing challenges in sourcing alternate labour particularly for specialised skills from alternate jurisdictions. Before considering whether to restructure their supply chain, the product companies also need to consider if another impact of coronavirus will be a change in demand for the proposed end product.

For online businesses in the TMT sector, coronavirus might be anticipated to trigger an increase in demand. For example, previously the uptake of online shopping has differed greatly between jurisdictions (e.g., between those jurisdictions where in person shopping is seen as part of the fabric connecting the community compared to jurisdictions where online shopping is more seen as a necessary convenience). Restrictions on people's movements may disrupt attitudes to online shopping and result in greater take-up. However, the impact of coronavirus on an online business may very much depend on what the business is selling and how the product will be delivered. For example, online travel bookings are seeing a sharp decline as a result of the significant contraction of travelling activities due to coronavirus. Some online offerings (e.g., online banking) might be seen as involving activities that can be done almost totally in the online world. Other online offerings that still significantly depend on a human physical element (e.g., delivery of goods purchased online or preparation of food) due to people movement restrictions may face constraints in being able to support the anticipated increase in demand. One topic that will likely receive great attention is whether changes to regulations to allow greater use of drones could address some delivery constraints.

Parts of the TMT sector are core to enabling segments of the economy to still effectively function despite the impact of coronavirus. For example, telecommunications networks, particularly in residential areas, are certainly being stress tested as many businesses seek to have their personnel work from home. Products that support remote working will also see an increase in demand. The parts of IT support services contracts drafted for contingency planning are also likely to be heavily used at this time. There will no doubt be some learnings coming out of the need to quickly implement different working arrangements for the majority of personnel, including on matters that with hindsight could be set out differently in contract arrangements to support remote working (e.g., on the ability to quickly source sufficient quantities of laptops or tools that would be used to provide secure remote access to the corporate network).

BACK TO MAIN PAGE

Supply Chain Susceptibility

With many tech companies reliant on production and input from China and Southeast Asia for their consumer electronics, it's clear that the extended shutdown of parts of China's economy is now feeding through, and this may impact supply chains as existing stocks may become depleted. Worldwide, the full impact of the outbreak and the resulting emergency measures on international trade remain to be seen, but companies have reported substantial business and operational disruptions, including closures of workplaces and ports, bottlenecks to supply and distribution channels, shortage of labour and weakened regional demand.

Businesses will need to be nimble and ready to adapt. Companies should continue analysing their supply chains to understand at which point and where they might need to make changes or take proactive action to mitigate operational disruption. Considerations should include reviewing contractual obligations, assessing force majeure clauses, tax and employment implications of changes, relocation costs, entry and visa issues for staff, exit possibilities as well as the option of swiftly reversing changes if the situation stabilises.

Immediate actions to protect your businesses

With the rapidly expanding impact of the COVID-19 coronavirus outbreak companies will need to continue acting immediately to mitigate disruption to their supply chain and business operations. Key initial steps savvy companies will be undertaking in the coming months to support business continuity will include:

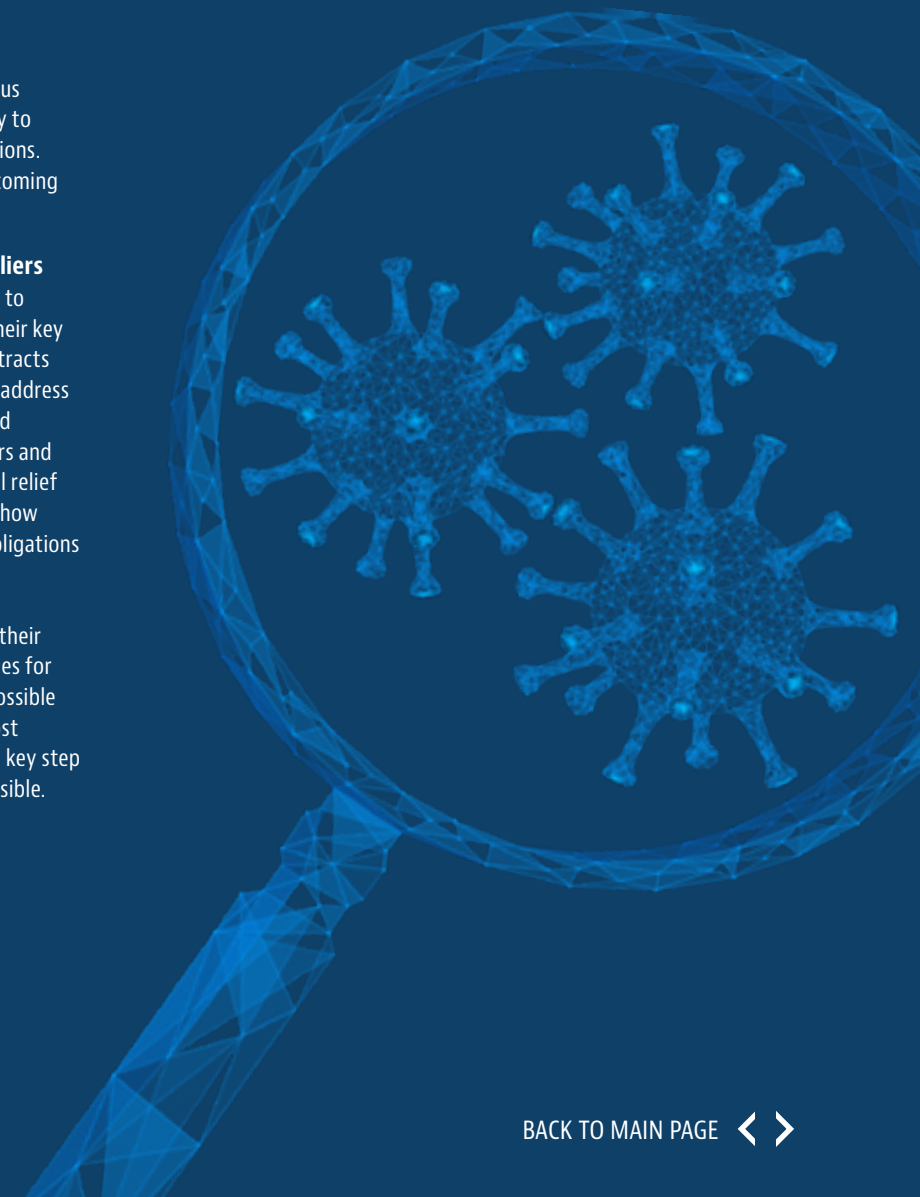
- **Review of commercial terms with customers, suppliers and logistics providers -** Tech companies will continue to review and analyse the contractual terms in place with their key suppliers and customers, as well as the national laws contracts are governed by with a view to identifying a strategy to address threats to supply chain operation. This, for example, could include a strategy to address the non-supply to customers and claims that may arise from this, as well as any contractual relief afforded to companies for their obligations. Strategy on how companies will need to shift to continue to meet their obligations will be central to the review.

  At the same time, companies should prioritize reviewing their logistical arrangements and in particular consider penalties for late deliveries, as well as hardship clauses to negotiate possible amendments. Closer communication with companies' most important suppliers as well as logistics providers is also a key step to mitigate disruption in the supply chain as much as possible.

- **Review and consider where force majeure provisions may be applicable -** Given the unexpected nature of the outbreak, attention has focused on the prospect that parties to affected commercial contracts may invoke force majeure provisions in order to excuse delay or non-performance. In that context, measures that could be taken in order to avoid or mitigate the effects of the delay or non-performance will also need to be assessed. All companies will consider force majeure, and force majeure claims involving a Chinese buyer or supplier have already been reported in the world media. It seems likely that claims with a wider ambit will follow as the ripple effects of the outbreak spread globally.

  Any contract with a specific force majeure clause may be the subject of a claim. Contracts governed by a civil law framework which grants force majeure remedies, whether or not they are written into the contract, may also be the subject of the claim.

  The effect of the outbreak on suppliers is perhaps most obvious. With emergency measures impacting on goods, workers and logistics, suppliers might be unable to fulfil their contracts within the prescribed time or at all. But invoking force majeure might also be considered by buyers, either because taking delivery under the contract has been impacted or due to disruptions in downstream markets.



BACK TO MAIN PAGE

- **Understand employee health and safety obligations as an employer -** Companies will also be faced with considering the implications around how travel restrictions, quarantine requirements and mobility hindrances coming from difficulty in obtaining work visas due to the coronavirus spread will disrupt labour output and impact businesses within their supply chain.

  At the same time, companies need also to consider whether they have a general obligation under national laws to ensure employees' health and safety as well as measures to prevent professional risks and should also provide sufficient training and information to employees to enable them to take care of their health.

- **Data privacy -** Companies that wish to collect personal data relating to the coronavirus, for example by requiring their employees, contractors or visitors to complete travel declaration forms or undergo temperature checks, need to adhere to applicable data protection laws. Where the processing is subject to the GDPR, companies need to decide and document what legal bases they rely on for the processing and provide proper information to the persons whose personal data are processed. Particularly in Europe, the processing of health data would be subject to stricter requirements and likely be lawful if there is a substantial public interest justifying such collection/processing of data. In Asia, on the other hand, the authorities seem to be more inclined to justify data processing by the private and public sector in order to contain the virus and safeguard public health.

- **Further emphasis on supply chain re-organization moving forward -** Electronics manufacturers moving production sites out of China to other (low-cost) jurisdictions such as Vietnam, Malaysia and Mexico has been a key priority for the tech industry over the past year as a result of the US-China trade war, and we have already seen many companies move their supply chains in that direction. With the COVID-19 coronavirus outbreak and particular uncertainty and disruption to China, we can expect prioritization of supply chain re-organization in the tech industry more than ever before. As a result, more and more manufacturers in the tech industry will be forced to rethink their entire supply chains considering adjustments to multi-layer contracts, force majeure clauses, hardship contractual provisions, cancellation and re-issuing rights, minimum volume requirements and clear processes for handling disputes and contingencies.

Conclusion

The concept of structuring supply chains to be able to quickly adapt to address sudden macro-trends is not novel, however the COVID-19 coronavirus outbreak has put a spotlight on a different situation as it is not within the control of companies or driven by commercial decisions. Thus, it is of high importance to focus on all aspects of disruptions for companies moving forward. An increased emphasis on prioritizing this adaptability may indeed shift the way companies contract with their suppliers, customers and logistics operators in the future.

Mattias Hedwall
Partner
Stockholm
mattias.hedwall@bakermckenzie.com

Anne Petterd
Partner
Sydney
anne.petterd@bakermckenzie.com

Autonomous vehicles: A road map in 2020

Automation in transportation will fundamentally transform the industry during the next few years, and many applications are already well underway. This applies particularly to autonomous vehicles (AVs) which have made significant progress towards reality on our roads with commercial trials in multiple jurisdictions worldwide.

The term "autonomous vehicle" describes a vehicle which "is able to plan its path and execute its plan without human intervention". As regards the development of AVs, five different levels of autonomous driving are generally defined: Level one is reached when the car contains assistance systems, such as a lane assistant or cruise control. On level two, different assistance systems are paired and enable the car to perform certain tasks without human intervention (for example advanced driver-assistance systems (ADAS)). The third level is reached when a vehicle can drive temporarily independently. On level four, the car can drive without a driver during defined use patterns such as in the event of traffic jams or on highways. A journey without a driver, or any passengers, is possible at level five (autonomous driving).

AVs bring social benefits including increased mobility and convenience and better managed traffic. They may also contribute to road safety through a better perception of complex situations and a lower error-rate. Finally, AVs create new business opportunities enabling new players to enter the relevant markets. On the flipside, they raise complex questions around liability, data, IP ownership regarding data and more.

Current AV Regulation

While the development of AVs progresses rapidly, the legal framework is far from being fully developed, let alone harmonized. Suppliers are faced with a mosaic of emerging AV regulations all over the world, which makes developing compliant AVs a complex challenge.

Countries worldwide are still grappling with issues such as whether to pass new regulations specifically for AVs or amend existing vehicle legislation (that typically approves and regulates vehicles that have a human driver, steering wheel and other traditional driving controls). Debate is also ongoing about whether the best approach is detailed top-down regulation or lighter touch principles-based regulation backed by voluntary or mandatory codes developed within the industry.

The US is currently continuing its longstanding efforts to pass a new federal law for AVs, meanwhile a mosaic of state and local laws exist which attempt to regulate how AVs are tested and deployed. Also, the Department of Transportation (DOT) released the latest version of its guidance on AVs on 8 January 2020. It establishes a voluntary standard approach for the regulatory integration of AV technologies and provides opportunities for AV stakeholders to collaborate with the US government in the areas of safety, mobility, fundamental research, security and cybersecurity, infrastructure, spectrum and connectivity, and workforce considerations.

In Europe, on 17 May 2018, the EU Commission published its EU strategy on connected and automated mobility, containing the "vision zero" – the EU goal of zero fatalities on European roads by 2050. Also, the EU strategy promotes testing and experience towards integration, addresses cybersecurity, data protection and data access and establishes guidelines to ensure harmonization with international partners, such as Japan, Russia, China and the US. In addition, on 4 September 2019, the EU Commission released its guidelines to help coordinate ad-hoc assessments of AVs and establish a process for EU exemptions under the EU vehicle approval framework.

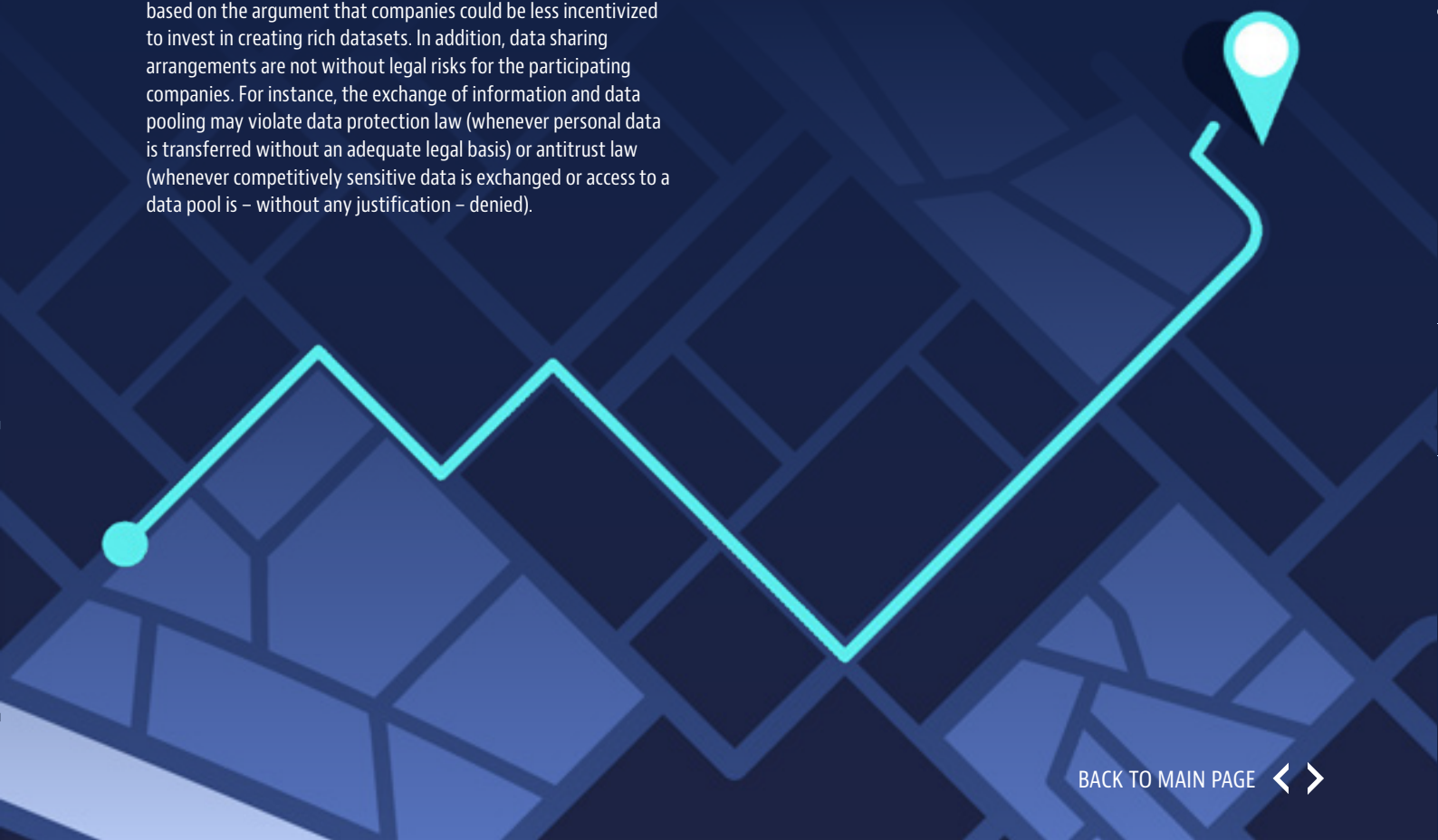
That said, AV regulations in the US and EU, along with similar initiatives and testing in China, Japan, Singapore, UK and many other jurisdictions all over the world are still nascent. AV stakeholders are well-advised to actively partner with governments worldwide to ensure commercial and regulatory viability at this critical juncture in the creation of AV technologies.

BACK TO MAIN PAGE

Major challenges

AVs still have to overcome different obstacles in order to unfold their full potential. Those obstacles include legal uncertainty, limited acceptance in society, lack of infrastructure, data privacy & security as well as ethical standards.

- Legal certainty is crucial to raising acceptance and trust levels in society. Product liability is a key issue that needs to be resolved. Product liability laws will need to evolve to clearly define where the line of non-fault legal liability gets drawn between the increasingly self-driving vehicle and the user/driver. Also if the vehicle is defective, which party within the supply chain is liable by law and how will the parties contractually allocate liability and risk across the supply chain. With fully autonomous AVs, there is little to no room for driver liability. However other levels of autonomy means a driver may well be liable for an accident, as they are usually required to decide when to engage as well as supervise even complex assisted driving systems. Making a driver liable for fully autonomous operation could only be justified by imposing the duty on the driver to intervene in risky situations. This could, however, lead to a significant obstacle to level 5 automation.
- Data lies at the core of AVs as data is needed to create and feed the AV algorithms. Numerous sensors present in AVs and integrated into mobility infrastructures continuously collect and exchange large volumes of data. Access to data is a key enabler for AV developers. Government and industry players are addressing data collection and data access in various cooperation projects such as the MUSICC Consortium in the UK, the PEGASUS Project in Germany, the SAKURA Project in Japan and most recently the European Strategy for Data. In Europe, some are calling for complete socialization of data access, in order to foster AVs (and other data driven) development. On the other hand, valid questions are raised on whether an open data approach would stifle innovation based on the argument that companies could be less incentivized to invest in creating rich datasets. In addition, data sharing arrangements are not without legal risks for the participating companies. For instance, the exchange of information and data pooling may violate data protection law (whenever personal data is transferred without an adequate legal basis) or antitrust law (whenever competitively sensitive data is exchanged or access to a data pool is – without any justification – denied).
- From a data privacy perspective recommendations were recently made by the European Data Protection Board (EDPB) in its guidelines on connected vehicles in the EU (Guidelines). They recommend a number of measures to mitigate the privacy risks that may arise in the context of data collection and processing by connected vehicles. Key risks include, for example, lack of information and control, insufficient data security, invalid consent and excessive collection. The EDPB makes a number of recommendations to address the key risks which we have summarized here.
- To enable autonomous driving throughout countries, and across borders, expanding the transport infrastructure and the mobile service coverage (5G) is another important challenge. This requires high investments and the use of SEPs (standard-essential patents) to enable communication between AVs from different OEMs. This, however, bears the risk of legal disputes about the appropriate fair, reasonable and non-discriminatory (FRAND) license fees for the use of SEPs. In addition, AV projects require multiple and complex partnerships for example between traditional OEMs and technology companies as well as with the relevant transport authorities in each country for the development of co-designed policy frameworks for AV deployment. The partnership between the San Francisco Municipal Transit Authority and the Israel Ministry of Transport is an example of this.



BACK TO MAIN PAGE

Navigating the challenges

The above-described challenges require a comprehensive risk mitigation plan whilst regulations develop and mature. OEMs and other technology companies developing AVs should closely monitor the changing legal frameworks and developments with regard to AV regulation and continue to pro-actively engage with the relevant regulators and industry bodies, including in the context of public consultations. Most companies developing AVs focus on a limited number of main jurisdictions in order to be able to mitigate their legal risks and to identify business opportunities, particularly concerning product liability issues and AV data access.

The promise of AVs remains exciting for future commercial and personal transportation. Whilst there are still many challenges to overcome, regular review and careful adjustment of the strategic plans of OEMs and other major players in the supply chain remains the route to success in 2020 and beyond.

Nicolas Kredel
Partner
Dusseldorf
nicolas.kredel@bakermckenzie.com

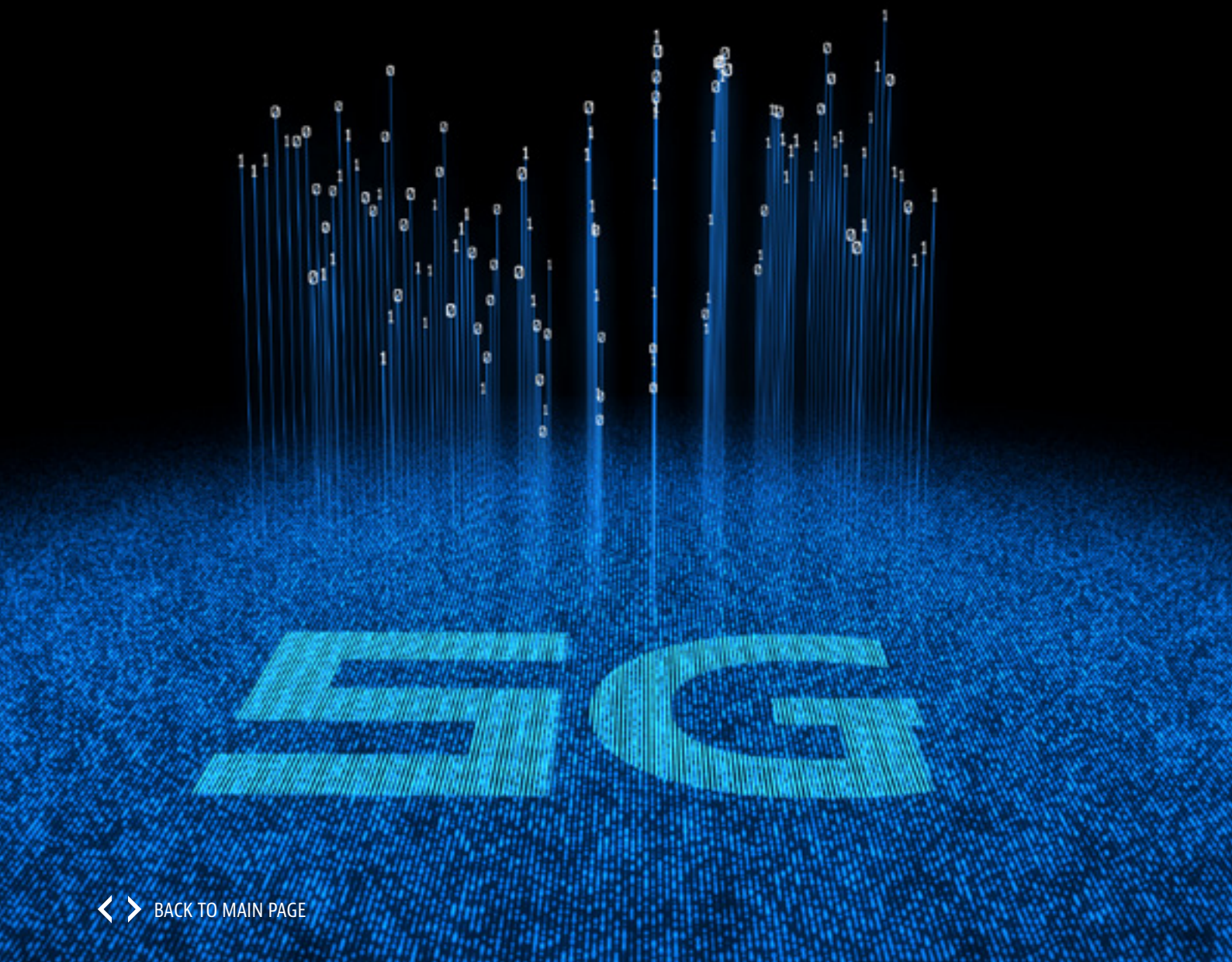
Jan Kresken
Associate
Dusseldorf
jan.kresken@bakermckenzie.com

BACK TO MAIN PAGE

Mobile Services for the connected era: Boosting 5G deployment in the EU and China

Compared to its 4G predecessor, 5G provides faster speeds (up to 1000 times faster), lower latency (1 millisecond under optimal conditions) and can support a larger number of devices (approximately 100 times more). 5G technology will also provide the infrastructure and data that are necessary to train and nurture AI technology.

With the potential of ubiquitous, ultra-high bandwidth and low latency connectivity to a much wider range of connected devices, 5G brings huge innovation potential including industrial-class robots, self-driving cars, smart cities and tele-medical devices. In combination with existing technologies including AI, M2M and IoT, 5G can bring Industry 4.0, also known as the "fourth industrial revolution", to a new level.



BACK TO MAIN PAGE

Current Status of 5G Frequency/Spectrum Allocation

Unlike other countries (e.g., Germany, UK, India) where spectrum auction models are adopted to allocate 5G frequency/spectrum, China authorizes its administrative body of the telecommunications sector (i.e., the Ministry of Industry and Information Technology (**MIIT**)) to allocate 5G frequency/spectrum without any auction. So far, MIIT has issued 5G licenses and the respective 5G frequency/spectrum to four Chinese telecommunication carriers (i.e., China Mobile, China Telecom, China Unicom and China Broadcasting Network).

In the EU, the European 5G Observatory, which monitors 5G developments on behalf of the European Commission, provides a comprehensive overview on national 5G spectrum assignments and current assignment proceedings within all Member States of the EU. The 5G frequencies covered by this overview include the ranges of 700 MHz, 3.4 – 3.6 GHz, 3.6 – 3.8 GHz as well as 24 GHz and above. Furthermore, the Observatory also provides information on global developments, among others, on the status of 5G-related matters for China.

Boosting 5G Roll-out

Simply providing a mechanism for and allocating 5G spectrum is not sufficient. Rather, the regulatory environment must be structured so that investment in 5G infrastructures and the expeditious roll-out of 5G networks is facilitated and incentivized.

China still follows its existing regulatory regime and framework to promote the development of 5G. No specific legislation has yet been drafted or passed for 5G deployment. Instead, from 2017 MIIT has issued a few administrative notices concerning 5G technology (including notices on spectrum/frequency and base stations) and has directed its local counterparts and provinces to encourage the promotion of 5G technology. Subsequently, some provincial and municipal governments have released their own policies regarding the promotion and development of 5G in their jurisdictions respectively.

The EU has taken a different approach and has used the occasion of the review of the former regulatory framework for electronic communications to implement a number of changes that promote the deployment of "very high capacity networks", among them mobile high-speed networks. Aiming at "an internal market in electronic communications networks and services that results in the deployment and take-up of very high capacity networks", and establishing a conducive regulatory environment in that regard, the European Electronic Communications Code of 11 December 2018 (**EECC**) – which replaces the previous telecommunications framework – certainly has the potential to boost 5G deployment.

The EECC establishes a harmonized legal framework for the regulation of electronic communications, including a variety of rules on electronic communications networks. The provisions of the EECC are not directly applicable in the European Member States, but need to be transposed into national law by each Member State by 21 December 2020.

The EECC contains a number of measures to promote the roll-out of very high capacity networks (among them certain high-speed mobile networks). These include:

- frequency assignments to be harmonized to a certain degree within the EU, inter alia, by strengthening the roles of the Radio Spectrum Policy Group (RPSG), a high-level advisory group assisting the European Commission, and the Body of European Regulators for Electronic Communications (BEREC). However, frequency assignment as such will remain within the competence of the Member States;
- when allocating individual rights of use for frequencies, Member States have to ensure regulatory predictability over a period of at least 20 years, whereas the individual assignment has to be granted for a minimum of 15 years, including an option for extension if specified conditions are met;
- frequency usage rights must be transferable and leasable. This flexibility is intended to support and enable new business models and cooperation, thus boosting 5G deployment;
- a regulatory framework for co-investments in new very high capacity network infrastructure. If certain conditions are met, such co-investors may be excluded from regulatory obligations on the basis of prior commitments made vis-à-vis the regulatory authority.

Conclusion

The EECC has the potential to meaningfully encourage and significantly boost 5G deployment in the EU, thus supporting the EU's aim in being the leading region in building trustworthy AI and relevant networks and in being at the forefront of the "fourth industrial revolution".

In China, with the commercial applications of 5G in 2019, the Chinese government will continue to promote and accelerate the implementation of 5G in a wide range of industrial and commercial activities in the coming years through various national plans and initiatives such as the ambitious "5G plus in Industrial Internet" program to be rolled out up to 2022.

.....

Zhenyu Ruan
Partner
Shanghai
zhenyu.ruan@bakermckenziefenxun.com

Caroline Heinickel
Counsel
Frankfurt
caroline.heinickel@bakermckenzie.com

Protectionism: Foreign investment, trade wars and import tariffs

Global trade wars (particularly between the US and China) continue to pose a challenge for TMT companies despite recent progress. Protectionist policies including tighter foreign investment restrictions, national security-driven procurement restrictions, limitations on technology transfers and the direction of travel on import tariffs are all key trends to watch in 2020.

Foreign Investment Regulations

Foreign investment review regimes across the globe pose a challenge in the coming years for the TMT sector. Protectionist sentiment worldwide has generated scrutiny of investments by foreign acquirers and has led to a number of jurisdictions updating their foreign investment rules that could impact TMT deal-making.

In January 2020, the United States Department of the Treasury (Treasury) released two final rules implementing the Foreign Investment Risk Review Modernization Act (FIRRMA). FIRRMA was enacted in 2018 and expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS), the US governmental inter-agency committee responsible for reviewing investments that might pose a threat to US national security. While CFIUS traditionally has had the authority to review transactions in which a foreign person takes "control" over a US business, FIRRMA expands CFIUS' role to review and potentially block certain non-controlling investments in businesses that handle "critical technology", "critical infrastructure" or "sensitive personal data." Proposed investments in "critical technology" businesses now require a mandatory declaration to CFIUS which will have an impact on deal strategy and timing. The expansion of CFIUS' jurisdiction could see even passive investors discouraged from investing in technology-related target companies in the coming years.

Similarly, other regimes around the world have expanded their scrutiny over foreign investments in technology and media companies. Germany, for example, widened its scope of foreign investment review to include review of acquisitions of media companies for national security concerns, as well as acquisitions of 10% of the voting rights by a non-European Union/European Free Trade Association acquirer of certain technology-related companies, such as cloud computing providers and companies that carry out measures for monitoring telecommunications. France also expanded its national security review to include acquisitions in a number of technology-related businesses and expanded its list of highly sensitive sectors to include "certain research and development activities relating to cybersecurity, artificial intelligence, robotics, additive manufacturing, semiconductors; and certain research and development activities relating to dual-use goods and technologies, when carried out as part of another listed activity."

5G Networks and National Security Restrictions

Another important trend relevant to the TMT sector is the application of additional security requirements to 5G telecoms networks and other essential/strategic public services affecting the end-to-end supply chain. Such national security requirements include:

- restrictions on the procurement or use of certain equipment and/or software, for example, restrictions in 5G networks on contracting with certain prescribed providers of equipment/software or on using equipment or software of prescribed providers in certain systems and networks;
- a requirement to notify government agencies and obtain their clearance for contracts falling within the foregoing restrictions.

For example, Italy recently enacted a law establishing a set of security-related provisions in relation to networks, information systems and IT services held by certain public administrations, public agencies and private companies. The law also amends foreign investment rules to require a wide range of parties in the supply chain to notify the Italian Government of any 5G related contracts with non-EU/non-EEA parties. Failure to comply with the new law results in pecuniary fines and may trigger even criminal penalties.

BACK TO MAIN PAGE

Technology Transfer Controls

The transfer of so called critical/emerging technologies, including notably 5G cellular and AI technologies, to specified countries or specific foreign entities is an ongoing focal point for national regulators. These efforts could see currently unrestricted newer technologies become subject to export licensing requirements and restrictions in the coming year. This could have a knock-on effect on global technological collaboration and the ability to hire talent. TMT companies should closely monitor such proposals and consider engaging proactively in the regulatory consultation process to help shape such controls.

Trade deals

Technology products have been a prominent target of import tariffs in the US/China trade war, forcing technology companies to rethink their supply chains and investment decisions. The first phase of the US/China trade deal (the Economic and Trade Agreement) was entered into on January 15, 2020. The deal has important provisions relating to technology and includes:

- commitments by China to increase the value of the US goods and services it imports by USD 200 billion in the next two years;
- a pledge by both parties to adhere to certain standards covering a range of issues, including intellectual property protection, technology transfer, financial services, and dispute resolution. The intellectual property provisions were front and centre of the deal and include, for example, an obligation for both parties to "ensure fair, adequate and effective protection and enforcement of intellectual property rights. Each party shall ensure fair and equitable access to persons of the other Party that rely upon intellectual property protection." The tech/IP commitments are targeted at bolstering IP protection including of trade marks and trade secrets, halting forced technology transfer to gain access to markets and enhanced enforcement procedures to curb the sale of counterfeit goods;
- indefinite suspension of US import tariffs that were scheduled to go into effect at the end of 2019 and a reduction in the tranche of existing tariffs on USD 120 billion of Chinese goods to 7.5%;
- a new bilateral dispute resolution mechanism for enforcement.

Whilst undoubtedly a positive move, the success of the phase one deal will depend on how quickly the promises are implemented and enforced. Also, a number of key areas were not covered in the deal, including Chinese state subsidies, cybersecurity and rules on cloud computing. These areas, as well as further movement on existing tariffs, may be addressed during phase 2, although uncertainties remain.

With the UK currently negotiating post-brexit trade deals with the EU, US and other major prospective trading partners we can expect further complications in international trade including potential import tariffs between the UK and EU especially if the EU and the UK do not manage to reach a deal; delays on the border due to customs formalities when goods move from the EU to the UK and vice versa (irrespective of whether a deal is reached); and the UK's potential divergence from a number of existing EU technical standards after it formally leaves the EU at the end of 2020.

Conclusion

2020 will continue to bring several developments that TMT companies will need to watch closely including:

- the continuing impact of foreign investment restrictions in the technology sector
- protectionism around technology supply chains
- potential new restrictions on transfers of key technology, including 5G and AI, affecting R&D
- progress on trade deals and, in particular:
  - how will phase one of the US/China trade deal get implemented and enforced in practice beyond the high level pledges
  - how will phase two play out, particularly with the US presidential election on the horizon
  - in the wake of Brexit , what will the UK's trade deals with Europe, the US and other countries mean for the sector, including in terms of mutual recognition of standards

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

Jason Irvine-Geddis
Knowledge Lawyer
Belfast
jason.irvinegeddis@bakermckenzie.com

3

DIGITAL CONTENT

The scale and pace of change in how digital content is developed, produced and consumed means we will continue to see significant regulatory evolutions for the key market players. From increasingly onerous obligations on all digital platforms to moderate user generated content, debates continue on how best to regulate global streaming companies with their significant content budgets in the wake of the so-called streaming wars. Also the regulatory hot topics, including in-game monetization models, game-related betting and player behavior remain in focus in 2020.

At a glance:

- **Content governance regulation: Where are we heading?** In 2019, we focused our attention on the Christchurch Call to Action, the "streaming wars", "fake news" and interference in elections and democratic processes. As 2019 closed, global developments continued to drive changes in content regulation with ripples of coordinated regulatory action moving around the globe. These changes in many ways represent a new direction for content governance. In 2020, governments are likely to continue to reassess protections previously granted and historical structures in light of global events, changing consumer behaviors and shifting competitive tensions.
- **Content distribution into 2020: The race for viewers, fans, subscribers and awards -** Content production practices, viewing habits and distribution models have changed over the last few years. Traditional episodic content and film, previously reserved for the movie studios, is a space now occupied by a vast range of companies, all competing for viewers and subscribers. At the same time, the battle for users' attention away from both the big and small screen is raging as viewers engage with short form entertainment. Budgets are larger than before, as are user expectations for the best and most engaging content. In TV and film the "arms race" continues. Key themes in 2020 will be: due diligence being more important than ever, defamation claims on the rise, increasing content regulation and consumer laws growing sharper teeth. Video sharing platforms are also coming to terms with a new legal and regulatory landscape.
- **Video gaming: Shall we play?** The global video games industry is projected to grow significantly in the next five years. Given the industry's size and importance, the worldwide trend of increased regulation is set to continue. Regulatory hot topics include microtransactions, loot boxes, game-related betting, and measures to combat toxic behavior of players. Recent changes in EU law focusing on working hours has implications for developer crunch, whilst new consumer protection laws on digital content should curtail hype in the pre-release cycle and give additional remedies in respect of bug laden games.

BACK TO MAIN PAGE

Content governance regulation: Where are we heading?

2019 brought us the Christchurch Call to Action, the "streaming wars", "fake news" and interference in elections and democratic processes. As 2019 closed, global developments continued to drive changes in content regulation with ripples of coordinated regulatory action moving around the globe. These changes in many ways represent a new direction for content governance, and are likely to become more keenly felt in 2020.

In the past, content regulatory inaction has been the status quo in many jurisdictions as changes in entertainment, news and content offerings, technology and viewing and reading outpaced changes in the law. Historically, governments have sometimes been reticent to take on significant media reform programs in the face of complex relationships with local media interests.

However, changes to address evolving media markets and viewing patterns are now gathering speed. For many reasons, both policy-based and historical, many digital content offerings have had the benefit of safe harbours and other protections with content obligations generally sitting more heavily with traditional media. Regulatory positions such as these have supported new and innovative market entrants, enabling the emergence of significant new voices and innovative platforms giving individuals the ability to create and share content like never before. However, public expectations and levels of trust surrounding news media and alternative news services, new risks, pressures on public interest journalism and market tensions have markedly altered in recent years, and the era of content regulatory inertia seems to be ending.

2020 is therefore framing as the year in which content regulatory change has the potential to significantly accelerate, as many initiatives started in 2019 are worked through, and a new appetite for regulatory change continues to emerge, as both the geopolitical and competitive media and content landscape shifts dramatically.

A few themes are likely to underpin accelerating content governance changes in 2020.

Event-driven regulatory responses

In recent years, global events have increasingly acted as one of the largest triggers for regulatory action – whether that be interference in elections and disinformation campaigns or coverage of terrorist or other significant events.

As a US election year, 2020 is likely to continue the recent trend of global event driven content regulatory change.

Global coordination

In parallel with this, 2020 is also likely to see a continuation of attempts at global cooperation. When considering online content governance in particular, the benefits of globally coordinated action are evident from both a government and industry perspective. However, local complexities surrounding content regulation (as outlined further below) can pose significant challenges to cooperative approaches.

Despite this, we are increasingly seeing attempts at coordinated action on content governance and this theme is likely to continue. In 2019, following the tragic events surrounding the terrorist attacks in Christchurch New Zealand, in addition to individual domestic legislative activity, coordinated action included work by:

- the "Christchurch Call to Action" initiated by New Zealand and France to involve both governments and online service providers voluntarily working together to address terrorist and violent extremist online content;
- the European Commission including initiatives such as the EU Internet Forum;
- the G20 and G7, including the G20 Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT) in June 2019;
- the Global Internet Forum to Counter Terrorism (GIFCT); and
- the United Nations, including the United Nations Counter Terrorism Executive Directorate (UN CTED) Tech Against Terrorism initiative.

In addition, communication and cooperation between government agencies in different jurisdictions on questions of how best to approach regulatory change is on the rise, and sometimes from novel directions. The role of global antitrust and competition regulators, in particular, has increased through 2019, with regulators such as the Australian Competition and Consumer Commission in its Digital Platforms Inquiry considering uneven content regulatory obligations as a potential competition issue.

BACK TO MAIN PAGE

Streaming

The so-called "streaming wars" including the launch of major new streaming services, and moves by other digital platforms into professional film and episodic television content, will likely continue to drive significant content regulatory change in 2020. As online platforms continue to rise, not only as distributors but also as key producers of film and episodic television content, and competitive tensions continue to shift as a result, historical legislative structures will continue to come under pressure.

This is likely to extend not only to content regulatory obligations (which historically have sat more heavily with traditional players), but requirements to support domestic content and production industries are also likely to be more widely felt.

Changing news media markets

Concerns about the credibility and accuracy of news sources will likely continue to be front and centre in 2020 as news sources and consumer behaviour continues to shift.

Tensions in relationships between traditional news media outlets and digital platforms including shifting advertising spend and use and monetisation of content will increasingly play out to some degree in the regulatory sphere, whilst public concerns over investment in public interest journalism, possible job losses within traditional news media, closures of rural/regional media outlets, concerns over bias and partisan reporting, and blurring distinctions between news reporting and commentary will continue to drive regulatory change.

BACK TO MAIN PAGE

Historical variation and complexity

Whilst many of these are global issues and global coordination is increasing, it is also true that global media and content regulatory approaches have historically varied significantly.

The reasons for these distinctions across jurisdictions have included widely differing approaches on issues such as freedom of speech, censorship and state involvement in the press, as well as significant structural differences in local media markets including the respective strength of public broadcasters, traditional free-to-air broadcasters and cable and subscription providers as well as speed of take-up of new services.

Whilst various countries have gradually moved to more platform neutral content regulatory approaches over the last twenty years in response to convergence pressures and the rise of online content providers and intermediaries, others continue to work from regulatory frameworks that are inherently tied to historical market structures. In addition, differing approaches to freedom of speech and state media control continue to underpin regulatory structures and changes in numerous jurisdictions. These variations will continue to influence how jurisdictions approach regulatory change to global issues in 2020.

Global variations are further complicated due to the wide variety of types of content harms that are increasingly sought to be addressed. Current regulatory focus areas include:

- restrictions, prohibitions and/or take-down requirements in relation to:
  - disinformation and "fake news";
  - hate speech;
  - spread of terrorism-related content and propaganda and other extreme violent content;
  - pornography;
  - cyberbullying, stalking and "trolling";
  - child abuse, exploitation and other predatory behaviour; and
  - other online harms including image-based abuse;
- content classification schemes for professional content (for example films and episodic television programs) to inform viewing decisions;
- promotion of local content industries including domestic production sectors; and
- support for public interest journalism.

Many jurisdictions conflate different content issues together when determining how best to address them, with differing results.

Whilst 2020 is increasingly likely to bring new examples of global coordination and alignment on some key issues, these variations will continue to lead to key differences in approach in 2020 and associated compliance challenges for content providers.

Conclusion

In 2020, governments are likely to continue to reassess protections previously granted and historical structures in light of global events, changing consumer behaviour and shifting competitive tensions.

However, through all the change, some content governance themes endure – with a desire on many fronts to ensure that the stories that we see on screen or otherwise read, watch or listen to, and the news that we rely on to hold power to account, continue to be facilitated, supported and enabled.

Adrian Lawrence
Partner
Sydney
adrian.lawrence@bakermckenzie.com

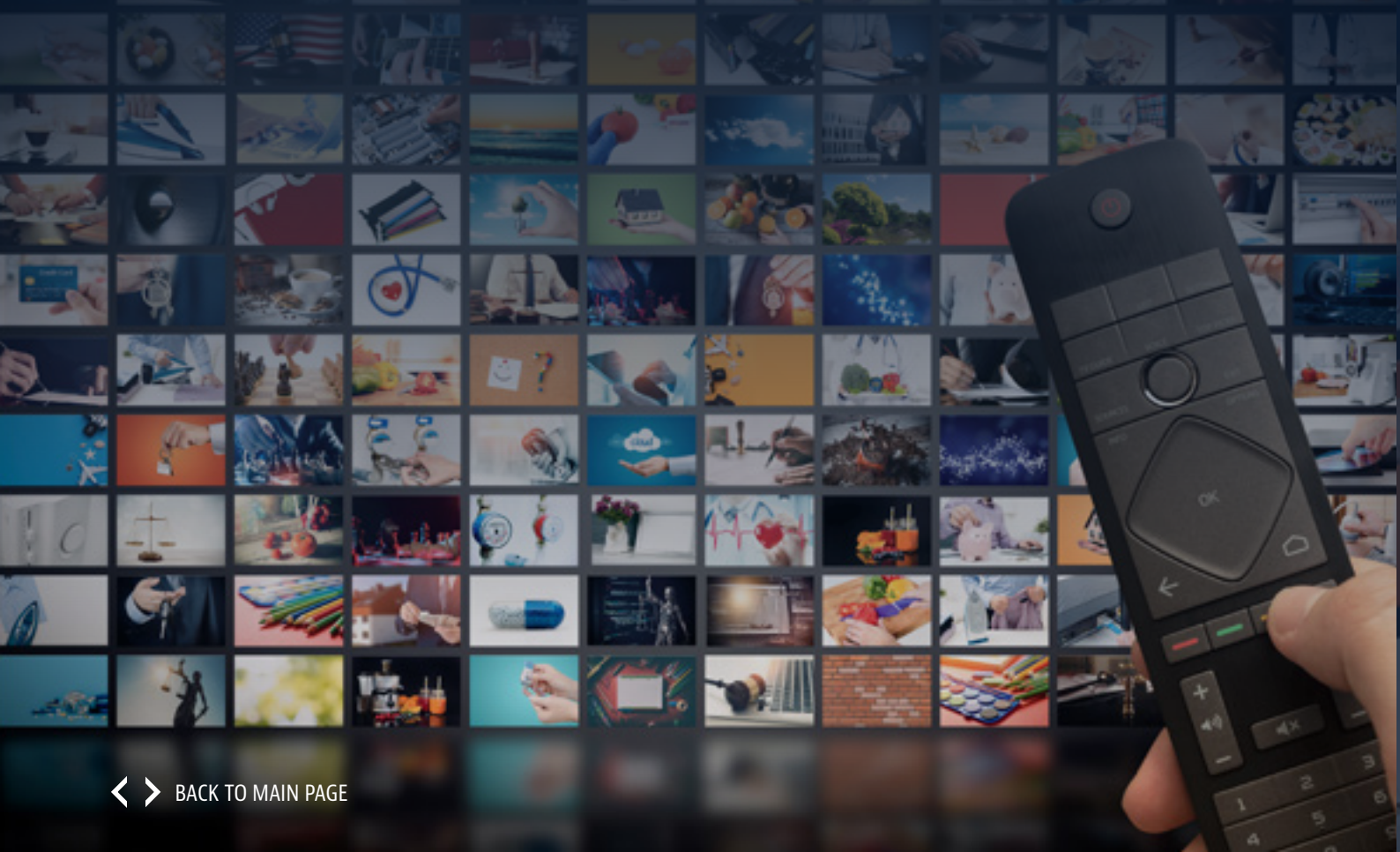
Allison Manvell
Special Counsel
Brisbane
allison.manvell@bakermckenzie.com

Content distribution into 2020: The race for viewers, fans, subscribers and awards

Content production practices, viewing habits and distribution models have been transformed over the last few years. Traditional episodic content and film, previously reserved for the movie studios, is a space now occupied by a vast range of companies, all competing for viewers, subscribers, and as we are seeing in this current award season, acclaim from the industry. At the same time, the battle for users' attention away from both the big and small screen is raging as viewers engage with short form entertainment. Budgets are larger than before, as are user expectations for the best and most engaging content.

With users devoting so much time engaging with content and having to confront issues like disinformation in a polarized political landscape, the need for trust in storytellers and media companies is of paramount importance. Law and policymakers around the world have made it clear that regulation of content and content providers' systems is essential in order to protect vulnerable viewers. Users themselves expect what and who they are watching to be trustworthy as well.

As a result, the demands on legal to identify and articulate risk are increasing and intensifying. The pressure to make the best content available as quickly as possible raises the stakes in terms of the speed at which effective legal guidance and compliance is needed. Potential claimants seem to believe that media companies' pockets are deep, so practical risk may be material. It seems clear that legal efforts and due diligence must scale appropriately to the increasing amounts of funds invested in content. For TV, Film, and short form content, there are certain legal risks to be particularly aware of in 2020, as well as wider political and societal concerns that should be considered. Below we sketch out a number of issues that media companies should consider.



BACK TO MAIN PAGE

TV and Film in 2020: The content "arms race" continues

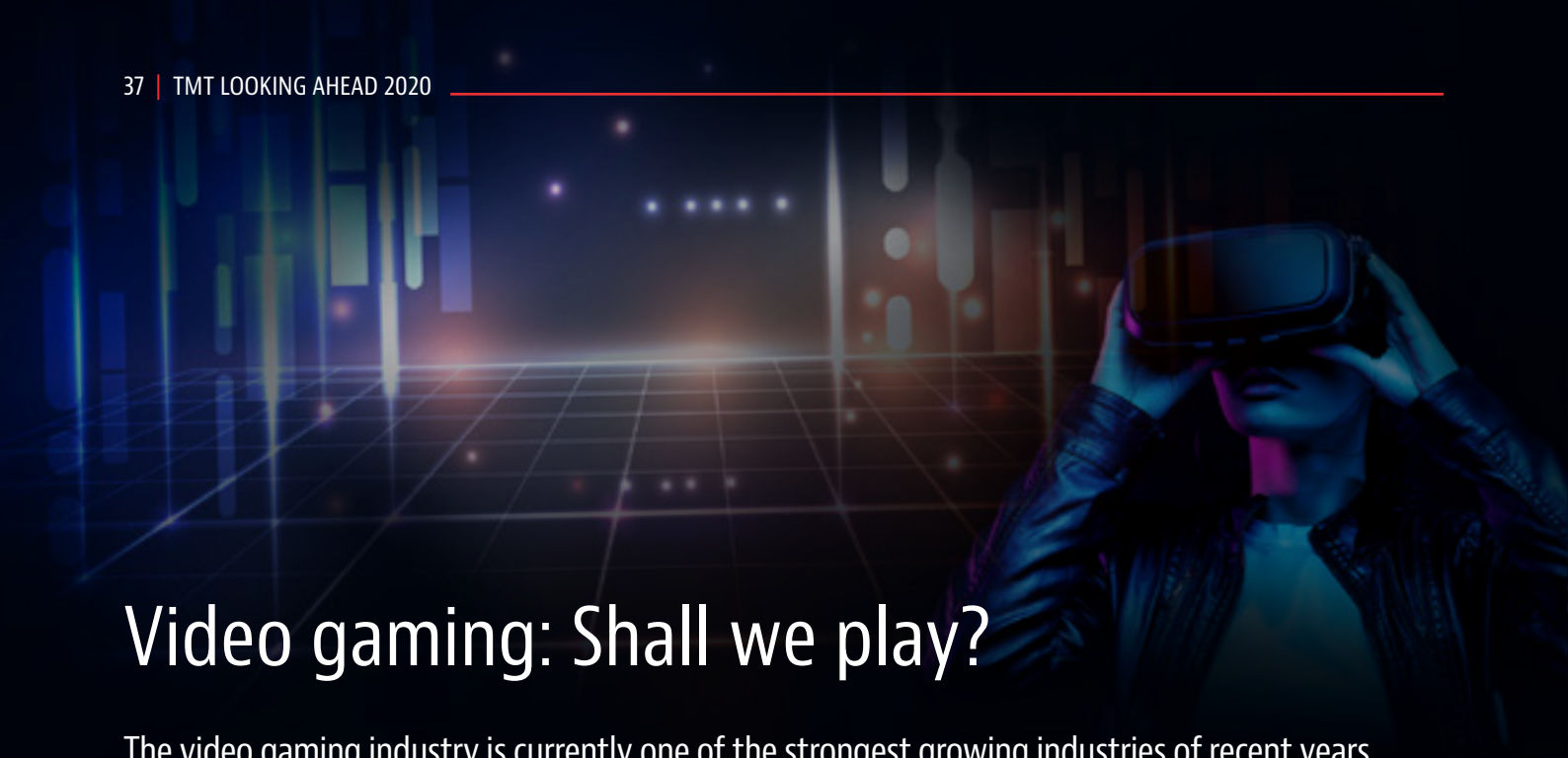
- **Due diligence is more important than ever.**
  - The pressure to release content as soon as possible is significant. However, the legal fundamentals are more important than ever: chain of title reviews should be cleared, script analysis should be carried out, and a robust rough-cut review should be completed. Different providers and different titles will be prepared to take differing levels of risk, but that should be a conscious decision rather than just passing over these steps.
  - The race to secure titles, actors, writers, directors or producers is occurring at breakneck speed. Yet, as we have seen, no name is more important than the company. Checks and analyses of the people involved should also be carried out, concerns should be addressed, and appropriate contractual protections should be built in and reviewed.
- **Defamation claims are on the rise.** There seems to be a pressing desire for real life documentaries and true crime series. As a result, we are seeing more defamation claims against creators, content providers and distributors. The emergence of documentaries examining old cases has led to renewed scrutiny, extensive discussion in the press and sometimes proceedings being reopened. Both of these patterns raise the stakes from a legal risk perspective.
- **Content regulation is increasing.** Rules and requirements around product placement, sponsorship, and advertising are getting tighter at a time when there is more pressure to pen deals securing these additional funding sources. The level and extent of all of these requirements vary around the world so a grasp of the requirements is certainly needed.
- **Consumer law is growing sharper teeth.** As content creators become services in their own right, they have to confront and comply with consumer law requirements at a time when they are being consolidated and strengthened around the world. As such, this may be a new realm for certain services.

Video sharing platforms in 2020: A new legal and regulatory landscape

- **A different liability regime?** Depending on the involvement with the content's creation, intermediary defences that are traditionally the platform's shield from claims might not be available.
- **New obligations in respect of UGC?** Laws and regulations relating to content are being expanded to place responsibilities on video sharing platforms in order to prevent harmful content being seen by children. That could mean profound changes for how platforms might structure their intake and moderation systems.
- **Engaging with less formal content creator structures carries risk.** Commissioned content on video sharing platforms rarely goes through the same production cycle as episodic content. Platforms generally may have less control over the schedule and content itself. That means that they may potentially also have weaker recourse when things go wrong. The competition for eyeballs should not mean that checks and reviews are not completed.
- **Freedom of speech laws vary.** Different countries protect freedom of speech and expression in different ways. For some, the right is extremely broad. For others, the right is balanced against freedom from harm rights. And in certain countries around the world, certain topics are completely excluded (for example criticism of a regime). This should be taken into account when considering the right personalities to engage with, particularly considering the company's values, ethos and political positioning.
- **Fans are loyal to the creator, not only the platform.** Creators garner significant, passionate, diehard fan bases. Remember that they are loyal to the creator, not just the platform. As a result, choices about which creators to onboard should be made carefully.
- **Creators may need additional support.** Many creators are young. They are under extreme pressure to deliver engaging content to millions of fans. The number and demands of fans can be overwhelming. At a time when platforms are under pressure to safeguard their own content moderators, they might also need to consider support for their creators as well.

John Groom
Senior Associate
London
john.groom@Bakermckenzie.com

BACK TO MAIN PAGE



Video gaming: Shall we play?

The video gaming industry is currently one of the strongest growing industries of recent years. In 2019, the global video games market is expected to generate around 152.1 billion USD (+9.6% on 2018) and is projected to reach up to USD 300 billion by the year 2025. With these numbers, not only have many of the big tech companies significantly invested in this sector with new technologies and business models emerging, but also public, political and regulatory scrutiny of the sector has significantly increased.

Video game streaming and subscription services

One of the most discussed trends in the video games sector is the potential of streaming. Two primary business models have been adopted in the market: cloud streaming services and subscription services. With cloud streaming services, the player who has purchased a game license does not have to download the video game or own expensive hardware (consoles or PCs), as the graphic and game processing is fully moved to the powerful cloud servers owned or rented by the service provider. On the other hand, the subscription service model requires the player to subscribe for a monthly fee to be granted access to a library of video games on a flat rate basis. Hybrid business models are also being implemented.

These new business models are facing a number of legal challenges. In a B2B context, the relationship between publishers and video game streaming service providers has become more complex and raises questions as to who owns the data on the gameplay patterns of platform users. Regarding B2C relations, one of the main concerns is whether a platform can offer a consistent level of service to players, given that user experience largely depends on third-party providers on the side of both the consumers (e.g., internet providers) and the platforms (e.g., third-party servers used to process the games).

Monetization, microtransactions and loot boxes

The monetization of video games through so-called microtransactions, i.e., smaller in-game purchases of digital content such as loot boxes, is a widely discussed trend. Microtransactions touch laws including consumer laws, youth protection laws, unfair competition laws, financial and even gambling laws.

Following the so called "skin betting scandal" from 2016 and the global "loot box debate" from 2017/2018, several countries such as the USA, France and Australia have started investigations of the monetization models of the video gaming industry and/or have regulated the subject. The Netherlands and Belgium have already banned certain forms of loot boxes under national gambling laws. As a result, several video game publishers had to make product changes or cease providing their services in different jurisdictions.

eSports

eSports remain one of the most discussed subjects in the industry and are considered as having the greatest potential for exponential growth. Some of the largest eSport tournaments already offer participants between USD 25–30 million in prize money and have more than 100 million viewers on internet live streams.

Since eSports is a new phenomenon, many legal aspects are novel and still in the early stages of analysis and discussion. eSports touch upon many areas of law including contracts and visa requirements for talent and youth protection, copyright and trademark issues, mandatory licensing requirements and resolving potentially conflicting interests between the publisher of the video game and the eSport tournament's organizer.

AR/VR

With *Pokémon Go* and *Snapchat*, augmented reality (**AR**) has become a mass phenomenon that is commercially successful. Improving AR technology often requires machine learning by taking pictures of the environment in order to have virtual reality (**VR**) items and things interact with the environment in a more fluent and convincing way to improve the player's immersion and experience. This typically raises data protection and copyright questions when photos also capture bystanders or copyright protected works.

BACK TO MAIN PAGE

Player toxicity

Player toxicity refers to gamers that behave in a toxic manner (e.g., making racist insults) within their respective gaming community and through a variety of different video game platforms (e.g., in-game chats). After the recent significant political, public and regulatory pressure on the social media industry and the passing of strict anti-hate speech laws in certain countries, the video gaming industry is increasingly focused on this area.

European Court of Justice – The end of Crunch?

"Crunch" refers to employees in the video gaming industry if they work significant overtime (overall between 60 and 120 hours per week) to meet development milestones and deadlines.

On May 14, 2019 the Court of Justice of the European Union (**CJEU**) issued a landmark decision (Case no. C-55/18) according to which employers are required to establish reliable mechanisms to track daily work hours of their workers, as without such a system in place workers would not be protected. As national legal frameworks are made consistent with this ruling in the coming months, video game companies with development studios or offices within the EU will have to comply with the relevant national laws and regulations. That might also require consideration of further legal obligations and requirements, in particular data protection laws and co-determination rights.

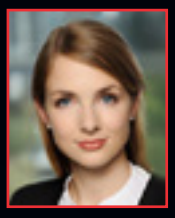
China – Increased regulatory scrutiny

Together with the USA, China remains by far the largest market for the video games industry. In 2019, China's State Administration of Press and Publication adopted a new game approval process, provided clarification on what is required to obtain a license, and issued new youth protection restrictions. The Online Games Ethics Committee was also formed to address and prevent what are perceived as addiction and monetization issues. In light of the above, video game companies active in China should closely monitor new developments and comply with these new regulations.

Digital Content Directive – The end of the day one patch?

Another game changer in the B2C landscape of the video games industry is the new EU Digital Content Directive applicable to most digital content and services offered to consumers for consideration, including video games. The Directive provides more stringent objective and subjective conformity requirements including that digital content or services (which includes games) must be (i) fit for the purposes for which digital content or services of that type would normally be used, and (ii) be of the quality and possess the performance features which a consumer may reasonably expect given the nature of the digital content or service and any public statements or advertising made on behalf of the supplier (objective requirements). Also, the subjective requirements include that digital content or services must be of the description, quantity and quality and possess the functionality, compatibility, interoperability and other features as required by the contract. Such requirements will likely affect different areas including the game development process, advertising and games-as-a-service. It is also expected to significantly impact all game streaming and subscription services. For instance, the release of broken, unfinished or heavily bug laden games, with the intention of fixing the issues at later stage may be subject to severe scrutiny once the Directive is adopted in Member States (by July 1, 2021). Should the game not fulfill the conformity requirements, consumers will have a number of remedies including having the game brought into conformity, receiving a proportionate reduction in the price or terminating the contract.

Holger Lutz
Partner
Frankfurt
holger.lutz@bakermckenzie.com



Monika Gebel
Senior Associate
Warsaw
monika.gebel@bakermckenzie.com

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

Gonzalo Santos
Associate
Madrid
gonzalo.santos@bakermckenzie.com

BACK TO MAIN PAGE

4

PLATFORM REGULATION

Platform regulation looks set to continue to make the headlines in technology news in 2020. The spotlight has recently centred on the ethical and other corporate social responsibility policies and means. Large digital platforms will continue to pro-actively engage with regulators and society on public policy issues. Meanwhile antitrust, privacy and consumer regulators will continue to look at the role of big data and market power in large tech platforms. Finally, the long running debate on how best to tax value derived from monetizing digital data will remain in the limelight this year.

At a glance:

- **Public policy: The new, tech, corporate social responsibility -** Tech platforms are increasingly alive to the reality that they will face accountability from users, media or regulators for possible adverse public outcomes associated with the economic activity they facilitate, including unforeseeable collateral outcomes. To prepare adequately for such scrutiny and related regulatory risk, these private sector platforms will engage with issues of public policy. Tracking and engaging on known areas of regulatory risk, shaping an equitable public understanding of the many societal benefits a platform accomplishes, and crafting meaningful solutions for the adverse consequences that could emerge, will be key.
- **Considerations in big data, digital platforms, and antitrust -** Technology platforms are on the radar of antitrust authorities around the globe. Indeed, some of these platforms have been the targets of intensive investigations on their alleged misuse of data. Beyond these investigations, it is questioned whether a platform's use of big data could enable the exercise of market power or whether a large firm could impact on market competition by acquiring a nascent competitor. Looking forward, antitrust law, and regulators around the world will continue to ask the question of how the collection and use of big data should be addressed without deterring innovation efforts.
- **Taxing the digital economy: Consensus or chaos?** Governments worldwide continue to grapple with how best to tax the value that large tech platforms derive from monetizing data. In response, the OECD has been driving international tax reform, focused on a new global regime for taxing profits from digital activities to achieve international consensus by the end of 2020. Despite recent endorsement by over 130 countries, challenges remain. The alternative to international consensus is a continued proliferation of unilateral digital services taxes. However, the imposition of unilateral taxes is being robustly challenged by the US under its trade laws, most recently felt by France. Whatever the outcome, the question of how to find a global tax system that is fit for the 21st century has been driven to the top of the agenda in 2020.

BACK TO MAIN PAGE

Public policy: The new, tech, corporate social responsibility

Tech platforms are increasingly alive to the reality that they will face accountability, whether from users, media, or regulators, for possible adverse public outcomes associated with the economic activity they facilitate. This may include unforeseeable collateral outcomes, ranging from third party misuse or abuse to mere unintended consequences. To prepare adequately for such scrutiny, these private sector platforms will engage with issues of public policy – a subject matter which has historically been the purview predominantly of governments and academics.

The idea of holding corporations accountable for collateral outcomes is not novel to the 21st century tech renaissance. Consumers, activists, press and governments have long endeavored to hold prominent corporations accountable for problematic outcomes whenever a causal link may be found. Footwear and apparel brands are expected to ensure that worker rights are respected at the base of the supply chain, half a globe and many commercial counterparties away. Purveyors of soap and ice cream are expected to guarantee that no orangutans were harmed by their suppliers of palm oil. The newest targets in the fight against climate change are similarly attenuated: banks, university endowments and retirement funds.

For activists and governments, the appeal of such accountability efforts is self-evident. Even though these targets are rarely the economic actors responsible for the collateral prejudice, their liability is often argued by activists and governments on the grounds that they are "prime movers" which manage the platform through which users interact and benefit from the overall economic arrangement. They are also typically the economic actors with the highest public profile and, therefore, the most likely to attract the attention of activists, regulators or the public at large.

Outside the tech world, the primary means by which businesses have aimed to ameliorate, or at least atone for, the adverse consequences that might be the result of certain behaviors in their industry or business model has been the attention to corporate social responsibility (**CSR**). There have been vigorous (and fascinating) debates, hearkening to Milton Friedman, and even Adam Smith, about whether the purpose of a corporation must be limited to the pursuit of profit alone (and by extension, shareholder value) or whether it is possible (or desirable) for a corporation to legally bind itself to additional ethically-defined outcomes. But for now, CSR remains – with few notable exceptions – mainly a voluntary undertaking.

Tech platforms' status as high profile, prime economic movers makes them a similar target not only for public pressure, but also for regulatory risk. But the economic success of tech platforms is simply too great, and the tumultuous changes they occasion too extensive for such regulatory risk to be parried off by commitments only to social responsibility helping hand projects.

BACK TO MAIN PAGE

Many tech platforms dream of disrupting an industry, but the disruption achieved could far outpace that goal. A tech platform might be designed to enable new types of transactions, and unintentionally facilitate unprecedented unlawful activity. A platform might seek consumers in a new jurisdiction by challenging entrenched market players, to later find out that doing so has disrupted a critical source of government revenue. Tech platforms could democratize a market, or destabilize a government. They could facilitate human connection, or disrupt the pattern of human behavior on a near-evolutionary scale. Collateral outcomes of this nature are too consequential for governments to ignore, though the issue is not around the means, but the users' utilization of such means.

Much of the ire leveled against tech platforms is premised on the unfair (and unjustified) notion that the disruptors don't understand one or more of these serious impacts from their economic activity. But in fact, the humanistic aspirations of Silicon Valley spring eternal. Yet such skepticism requires only a kernel of perceived truth to be felt with both passion and conviction.

So what's a tech platform to do? We submit: continue to consider seriously the challenges of public policy.

Governments are expected to look earnestly at the question of what impact their policies (i.e., actions and inactions) will have on all individuals subject to their jurisdiction, as well as on inter-jurisdictional (i.e., international) relations, the natural and social environment and future generations. Tech platforms are setting their sights on nothing less.

Emerging tech platforms should follow the lead of more established technology companies, which invest in and empower sophisticated public policy teams. The goal of such teams is not simply to respond to public pressure, although that is a welcome ancillary benefit. Rather, the most effective teams aim to: (1) track regulatory developments globally, as some threats and public reactions are prone to catch on across jurisdictions; (2) be proactive in helping shape an equitable public understanding of the many societal benefits the platform delivers, and (3) be empowered to create meaningful solutions for the unintended consequences that may emerge, both direct and collateral, by advising on product design, and establishing paradigms for self-regulation. The more a tech platform is oriented around these objectives, the better prepared it will be to meet the challenges of regulation.

John Foote
Partner
Washington, DC
john.foote@bakermckenzie.com

Carlos Vela-Trevino
Partner
Mexico City
carlos.vela-trevino@bakermckenzie.com

Considerations in big data, digital platforms, and antitrust

Recently, technology platforms have received more and more scrutiny from antitrust authorities around the globe. Indeed, some of these platforms have been the targets of intensive investigations on their alleged misuse of data. Some of these investigations have resulted in hefty fines, particularly in Europe.

Beyond these investigations, pundits and commentators have questioned whether a platform's use of big data could enable the exercise of market power and whether a large firm could impact competition by acquiring a nascent competitor.

Looking forward, antitrust law, and regulators around the world will continue to ask the question of how the collection and use of big data should be addressed without deterring innovation efforts.

The UK's antitrust authority, the Competition and Markets Authority (CMA), recently issued a report titled "Online platforms and digital advertising" (**Report**) which suggests that competition problems can arise in digital advertising markets created by these platforms and proposes a number of measures to address these issues. The Report is one example of commentary that is being produced by various antitrust regulators.

The Report contends that, when it comes to big data, an imbalance exists between larger established platforms and smaller nascent ones. Larger platforms can better target advertisements to specific users because of access to relevant personal data. Smaller platforms and potential entrants have difficulty competing because of a lack of access to such relevant data. In the view of the CMA, this imbalance is a barrier to entry that is not easily overcome and incentivizes vertical integration – possibly even entrenching the market power of established platforms.

The report recognizes that there may be operational efficiencies from the vertical integration of services within well-established platforms, but also argues that such integration could generate conflicts of interest with other firms that rely on the platforms to reach the same customers. For example, some platforms have been accused of demoting search results to incentivize the purchase of ancillary services where certain third parties have not purchased those services. The CMA believes that this result is more likely where vertically integrated platforms hold a predominant market position.

Of course, these platforms benefit from economies of scale and network effects, both related to the collection of personal data. Once a platform becomes the clear choice of certain end-users, they will return again and again providing the platform with increasingly detailed information. Under these circumstances, the platform may enjoy certain competitive advantages that its rivals cannot achieve.

The CMA proposed certain behavioral and structural measures to address these concerns including the implementation of enforceable codes of conduct embodying the principles of 'fair trade', 'open choice' and 'trust and transparency'. It also proposed more extreme measures such as requiring some platforms to share its "click-and-query" data with rival search engines and restricting the ability to enter into agreements with third parties to make its search engine the default.

Similarly, in other forums some platforms have been scrutinized for bundling the functionality of one market with a secondary target market. Once established, users of the platform in the first market are less likely to switch to the service of a competitor in the secondary target market (reducing what is known as "multi-homing"). The regulators warn that this type of bundling could disadvantage smaller platforms.

Clearly, the CMA – as well as other competition bodies and pundits around the world – has concerns about technology platforms and digital advertising. Whether these concerns will result in significant changes to the digital marketplace remains to be seen, but these platforms will clearly continue to be the focus of significant regulatory scrutiny.

Carolina Pardo
Partner
Bogota
carolina.pardo@bakermckenzie.com

Miguel de Quinto
Senior Associate
Bogota
miguel.dequinto@bakermckenzie.com

BACK TO MAIN PAGE

Taxing the digital economy: Consensus or chaos?

The OECD has been driving a programme of international tax reform, which is now focused on a new global regime for taxing profits from digital activities. Despite recent endorsement of the OECD's approach by over 130 countries, there are still challenges to reaching consensus by the end of the year. The alternative to consensus is a proliferation of unilateral digital services taxes, with some such taxes already in place and many other countries poised to introduce their own versions.

Digital Services Taxes: State of Play - Click to enlarge

The options on the table

In autumn 2019, the OECD Secretariat produced two public consultation documents setting out a two-part plan. These had not been approved by the Inclusive Framework (the 130+ member group that consists of OECD member states and a large number of other interested countries), but that group has recently given its endorsement to the OECD's proposed way forward, with some modifications.

The first document presented a "Unified Approach" under the so-called Pillar One. It includes (a): a new taxable nexus not based on physical presence, but on "sales" of digital services; (b) a new profit allocation rule going beyond the arm's length principle; and (c) a three-tier profit allocation mechanism, with residual (i.e., non-routine) profits allocated to market jurisdictions using a formula-based approach. Consumer-facing businesses as well as tech sector multinationals are in scope, but with carve-outs for certain categories such as extractive industries and other producers and sellers of raw materials and commodities, as well as most financial sector activities.

The second document (Pillar Two) put forward a Global Anti-Base Erosion (**GloBE**) proposal that would introduce a minimum tax rate. No level has yet been discussed although France at one point suggested 12.5%. Income of a foreign branch or controlled entity would, if taxed below that minimum rate, be attributed to the parent and related-party payments that were not taxed at or above that rate would not be deductible, or would be taxed at source (e.g., by a withholding tax).

BACK TO MAIN PAGE

What's been agreed and what remains to be done

The Inclusive Framework has committed to reaching a consensus-based solution by the end of 2020. It will work on the design for a new nexus rule. However, it recognises that challenges remain. For example, a reallocation of taxing rights under Pillar One requires improved tax certainty, including effective dispute prevention and resolution mechanisms and minimal complexity. A US proposal, made in December 2019, that Pillar One should operate on an optional or "safe harbour" basis was greeted with surprise and hostility on the grounds, among other things, that it would reduce tax certainty. In particular, countries will not want to commit to abandon their digital services taxes (as currently required) if multinationals have the choice of not electing into the safe harbour. A final decision on the issue will be taken at OECD level, once other elements of the solution have been agreed upon.

The GloBE proposals have been criticised as being too complex, with EU Member States in particular being divided over the need for a global minimum tax and some arguing for an exclusion for companies that have economic substance in a country. Others have said that the OECD's overall approach unfairly favours the US and Europe, with some developing countries concerned that the project is moving too quickly. However, the OECD has reported that good progress has been made on Pillar Two issues, although there is still work to do and several design options are under consideration.

We are now at a critical point, with the OECD team admitting that the timetable for finding a solution is "ambitious". Pascal Saint Amans, director of the OECD's Centre for Tax Policy and Administration, emphasised that "There is no Plan B". There is plan C, and C is for chaos if we don't reach agreement".

Next steps

The next Inclusive Framework meeting will be in early July, to try and agree on the main features of the Pillar One plus the architecture of both Pillars and the relationship between them. That will be followed by a G20 Finance Ministers' meeting later that month, with the final proposal to be put to the G20 leaders in November.

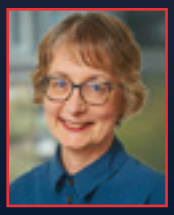
Unilateral digital service taxes

In the meantime, and with consensus not guaranteed, an increasing number of countries are going ahead with their own digital service taxes (**DSTs**). France's DST was the first, backdated to 1 January 2019, but Italian, Austrian and Malaysian DSTs apply from 1 January 2020. Turkey's DST enters into force in March 2020 and the UK and Canada's DSTs are due to take effect in April 2020. The French DST sparked a trade conflict with the US Government, with tariffs threatened on wine, cheese and cookware, among other things. France subsequently agreed to postpone collection of its tax until the end of the year when it would be known whether consensus had been achieved.

Tech forces the pace of change in tax law

Whatever the outcome, the question of how to find a global tax system that is fit for the 21st century has been driven to the top of the agenda by the urgent need to design rules to capture profits derived from sources that were not even in contemplation only a few years ago. So the pace of tax reform has been forced by the TMT sector, creating the need for a new approach to profit allocation and tax policies.

Kate Alexander
Partner
London
kate.alexander@bakermckenzie.com



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

Q&A with Sanjay Khanna

On hot topics occupying the tech sector

FUTURIST | TORONTO

sanjay.khanna@bakermckenzie.com

Q There is discussion about whether to increase regulation for the tech sector. As director and Futurist of Whitespace Legal Collab, how do you see that play out - do you think we will see a lot more heavy-handed tech regulation and, if so, in which areas? Or do you think we are going to see different approaches for governing technology?

A Depending on the particular issue driving a call for regulators to intervene, and depending on the potential social implications and impacts of any given tech company's activities, regulation will evolve differentially, likely influenced by social equity in any given jurisdiction. A high degree of social inequity might make strengthening regulations less likely, while a higher level of social equity might predispose any given jurisdiction to put into effect more stringent regulatory regimes. Furthermore, areas such as surveillance, facial recognition and autonomous vehicles generate new legal concerns that are complex and may necessitate stricter regulation.

Q In what ways do you envisage the tech sector to become further a force for good and help us tackle some of the most complex and pressing issues?

A A technology-focused economy introduces us to – and can protect us from – new and evolving risks, from cyberattacks to disinformation and increasingly complex and interdependent systems. Whether a given technology company becomes a force for good is about that company fostering a sense of interdependency among technologists and users, with the developers of new technologies embedding ethics into design, IP and internal oversight processes.

Q We are hearing a lot about concepts like the responsible organization, stakeholder governance and corporate priorities shifting away from equity holders towards employees, consumers, suppliers, local communities and the environment. Is this just a general discussion or do you envisage significant evolutions in the years ahead? If the latter, in what form?

A Urgent operational issues are at play for corporate leaders. Concepts such as purpose-led organizations, responsible business and stakeholder capitalism tend to improve strategy and behaviors in companies animated in practice by a responsible ethos or in companies that believe competitive advantage revolves around stakeholder relations. Promising examples where the stakeholder capitalism approach can move the dial include companies whose employees' expertise is hard to replace, consumer brands to which customers are symbiotically attached, suppliers whose components are a strategic element of finished goods, communities whose constituencies provide a social license to operate, and regions where a given brand is inextricably linked with the environment. To separate the best from the rest, close attention will need to be paid to organizations that on balance do more to be efficient, responsible and innovative in areas ranging from fair wages to human rights to carbon footprint.

Q Sustainability is predicted to become a competitive advantage. Do you have any practical tips for companies to get ahead in this respect?

A

- More efficient and effective business practices that reduce energy use, resource use, packaging, and so on are a proven competitive advantage. Today the world is facing considerable resource crises and during the past two decades those companies that have prepared for these crises, through greater efficiency, innovation in resource reuse from manufacturing to customer return and further reuse, are seen as being ahead of the game and are likely to remain so.
- For today's companies, the key is to hire leading experts in the field and move to implementation and expansion of programs that incorporate more efficient and respectful use of resources into business operations. Those companies whose chief sustainability officer is an operational leader are moving quickly around M&A due diligence, business process optimization, carbon and environmental footprint reduction, and the acquisition of innovative companies whose products and services align with business objectives around sustainability, from clean energy to food security to consumer-packaged goods.
- Once every company assesses the material risks they face from the aggregate pressures on resources from human activity, there will be a stampede for the right experts to help deliver sustainability results. I would recommend not to wait until the stampede happens as doing so would increase project execution risks.

BACK TO MAIN PAGE

Technology, Media and Telecommunications Industry Group

Key Contacts

Raffaele Giarda
Partner, Chair Global TMT
Rome
raffaele.giarda
@bakermckenzie.com

Kate Alexander
Partner, Tax
London
kate.alexander
@bakermckenzie.com

Lothar Determann
Partner, International Commercial
Palo Alto
lothar.determann
@bakermckenzie.com

Adrian Lawrence
Partner, Technology & Media
Sydney
adrian.lawrence
@bakermckenzie.com

Carolina Pardo
Partner, Antitrust & Competition
Bogotá
carolina.pardo
@bakermckenzie.com

Zhenyu Ruan
Partner, Mergers & Acquisitions
Shanghai
zhenyu.ruan
@bakermckenziefenxun.com

Editors

Anna Von Dietze
Director of Knowledge, Global Industry Groups
Dusseldorf
anna.vondietze
@bakermckenzie.com

Jason Irvine-Geddis
Knowledge Lawyer
Belfast
jason.irvineGeddis
@bakermckenzie.com

BACK TO MAIN PAGE